Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 4, Issue 3, 2026

MACHINE LEARNING-BASED FRAMEWORK FOR DETECTING ZERO-DAY ATTACKS IN NETWORK INTRUSION DETECTION SYSTEM

Naila Anwar

PhD Scholar, Dept. of Information Technology, University of Gujrat,

naila.anwwar@uog.edu.pk

DOI: https://doi.org/10.5281/zenodo.24027775

Keywords
Zero day attack, cyber-attacks, Cyber threats, artificial intelligence, ZSL

Article History
Received: 07 January 2026
Accepted: 17 March 2026
Published: 31 March 2026

Copyright@Author
Corresponding Author: *
Naila Anwar

Abstract
Zero-day attacks are most critical cybersecurity threats, exploiting unknown software vulnerabilities before developers can release appropriate security patches. These attacks are a major threat to governments, organizations, individuals and critical infrastructure of networks by illegal access, data theft and malware deployment. This research paper examines nature, types, detection techniques, and mitigation strategies associated of zero-day attacks. It also discusses using artificial intelligence and machine learning and for early threat detection. Furthermore, the paper discusses existing challenges and research gaps in developing effective defense mechanisms to prevent zero day attacks. Finally, it highlights future research directions for strengthening cybersecurity and reducing the impact of zero-day threats.

IEER
Institute for Excellence in Education & Research

INTRODUCTION:

The exceptional development of internet and usage of internet of things and devices have changed the ways of our lives. Internet and IOT devices play an important role in governments, industries and daily routine lives of people. Moreover big amount of data released by devices and offices enable companies and individuals to execute critical tasks and resolve data complications, enhance productivity and increase the amount of output [1].

Large amount of data creation and passage of data on internet create an attack surface for cyber community. The data creation and internet traffic has made it very easy for cyber attackers to get control of devices, resources and internet to launch attacks. These attacks destroy infrastructure, misuses critical data and crash websites by using advanced mechanisms, tools and techniques [1].

Cyber-criminals use advanced tools and technologies to access critical infrastructure of networks so that they can install virus for malicious software in public and private areas. Cisco pointed in their annual report that increase in internet breaks and attacks has increased to 776% by the year 2025 and number of distributed denial of service attacks increased up to 15.4 million by the start of 2026. System Security weakness is a problem in system structure, design and processes which exposes network to threats and make system vulnerable and exploitable. Elimination of security weakness typically requires system and process updation [12].

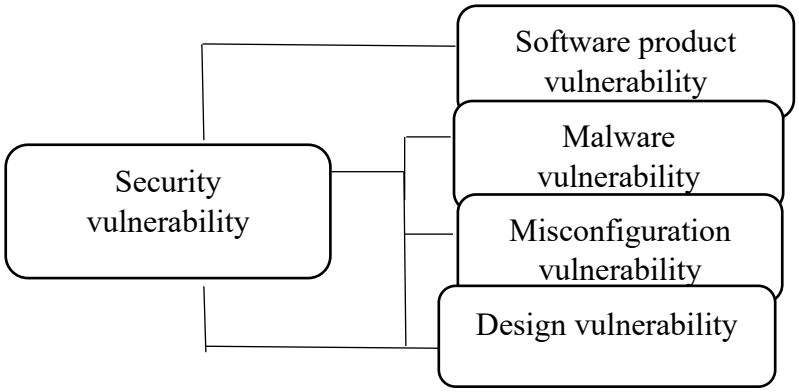


Figure 1 : Security vulnerability

The critical term cybersecurity include practices, processes and technologies which are used to protect computers professionals, networks, security mechanism and digital information from malicious acts like unauthorized access, attacks and data theft. With advancement of latest technologies and increased dependence on internet, cybersecurity has become an important design factor for individuals, organizations and governments. This critical security feature includes combating phishing, malware, infections and denial-of-service attacks which harms confidentiality, integrity and availability [13].

Zero-day attack is an unknown category of cyber-attack that public and security experts are not aware of. Zero day attack uses vulnerabilities and weaknesses which have not been discussed previously by using new techniques to escape detection from existing devices and techniques. Cyber hackers and attackers choose targets of their interest while their identity remains hidden [2].

A zero-day attack normally lasts for 312 days on average until they are detected and volume of attacks continues to increase with magnitude of five until system weaknesses and discrepancies are discussed [2]. Zero-day attacks have become one of the most widely discussed cyber-attack which is particularly new and uncommon to cyber society. The word Zero-day means that developers have had zero days to address the discrepancies before being misused by attackers. Zero day attack targets operating systems, web applications and network infrastructure causing unauthorized access, data theft, privilege escalation and disruption of critical services [2].

Traditionally, cyber-attack detection systems is classified in two groups: signature-based and anomaly-based detection systems. The signature-based detection system consists of a fixed collection of signatures, finger prints which is called known attacks. The detection in this class is done by comparing incoming signature with already present signature in repository [2].

The recent methods for classifying the malware depends on dynamic or static analysis in order to extract the representative features. Such techniques include examining byte codes of malware, file headers, assembly code structure, or execution behavior and dynamic actions by utilizing the Machine learning algorithms for classification [3].

There are various AI methods for zero-day attack. It can be categorized in four types.

- Machine learning,
- Deep learning,
- Hybrid models
- Anomaly-based.

The techniques for combating cyber-attacks can be grouped in two classes [8].

- known attack
- Zero-day attack

Moreover AI also plays a pivotal role in mitigating attack spread across networks. The success rate of Artificial intelligence in recognizing and combating zero-day attacks and vulnerabilities is exceptional. This strength of AI in dealing cyber terrorism point towards solutions which make AI based solutions more common. Anomaly-driven IDS are the more prevalent solutions for

recognition and prevention from zero-day attacks. Usually Artificial Neural Networks (ANN) are used for combating zero-day attack. This is due to the fact that ANN based solutions once successful can be trained with data, and attacks can be named and recognized [3].

The secure design solution is one practical and common solution in preventing both known and unknown attacks. Secure design solution can be categorized in following categories.

- Secure software design
- Secure hardware design

Secure software design is also called as secure coding. Secure Software Development Framework report issued by NIST [54] is an example study that adopted this solution. Implementing secure coding is one of the best solutions to stop security vulnerabilities [14].

Related Work:

Assuring robust cybersecurity means discussing and combating security vulnerabilities and security gaps. Both these terms are almost interrelated but it needs to be learnt and discussed separately, because approaches and solutions for both these two are different [8]. Security issues and cyber-attacks can be divided into two classes. i.e.

- Known attacks
- Unknown attacks

Researchers report that almost 15 percent of total cyber-attacks are zero-day attacks. These attacks can be virus, phishing attack or a zero-day attack. The most common example of zero day attack is WannaCry. This attack infected approximately 300,000 computers around the world in the year 2017. Scientists and researchers report that the attack damaged hundreds of millions to almost 4 billion dollars. In 2024, another ransom ware attacked a server without multifactor authentication. This attack destroyed data of 190 million persons and caused a $ 22 million payoff [9].

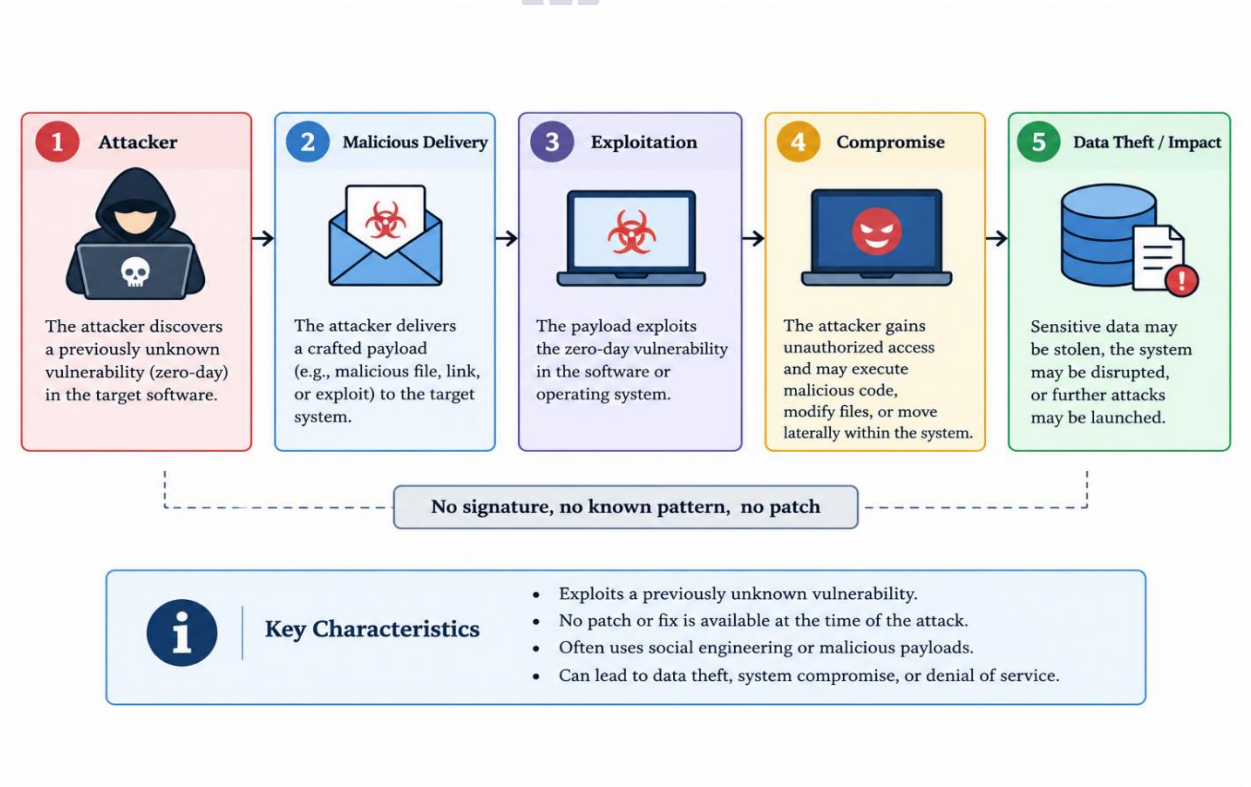


Figure 2: Zero day attack life cycle

The sudden surge in use of information technology and cyber world has increased the significance of cybersecurity. To guarantee safe and secure flow of operations and safe deployment of technical devices like IOT devices, cloud and critical designs networks must be secured from threats. A deep knowledge of security issues and exposure is essential to achieve secure and reliable safety. A cyber-attack becomes successful only when there is a gap in system security. These vulnerabilities encourage attackers to take advantage and steal sensitive information [11].

There are various AI methods for zero day attack detection. We can group these into four classes: i.e. machine learning, deep learning, hybrid and anomaly-based models. Machine learning models have the capability of detecting complex and modern attacks requiring latest tools and techniques. By using latest tools and technology and security elements to organization's framework adds sophisticated layers of defense which limits internal and external threats [7].

Machine learning has gained importance as an auspicious technique for cyber-threat detection. Machine learning generates models consisting of sample data called as training data. These models can detect confusing patterns to find similar attacks and changing behavior of attacks. Machine learning is an effective technology for zero day attack detection. Deep learning employs neural network to explain complex features and patterns from raw data. Common methods for attack detection in CNN are auto encoders, generative AI and cloud [2]

In Supervised learning the input data is usually labeled so that models can be trained to find specific patterns in data. In supervised learning, every sample is considered as a vector which consists of input items like traffic data and projected outcome. This is called as supervisory signal [3]. Unsupervised learning does not uses labeled data and most often used for outliers, to discover anomalous behaviors and new attacks [3]. Machine learning is a powerful technique but adoption of ML faces several challenges. Training data availability is a basics requirement for ML technique. Zero-day attacks are unknown until they are discovered. Availability of data sets for zero day attacks is a tough procedure. So it is generally assumed that zero-day attacks are similar to existing attacks. The model used for existing data can also be used for zero-day attacks detection [6].

Installing Network Intrusion Detection Systems is an important security mechanism which helps in detecting zero day attacks before they breach organization's network. Signature based intrusion detection system works by scanning network traffic for threats, attacks and malware. One of the major challenges in scanning incoming traffic with intrusion detection system is scanning traffic for zero day attacks. A zero-day attack is designed to disrupt network traffic, and it is a new and unseen [6].

Organizations using signature-based intrusion detection system are more susceptible to attacks. So instead of using traditional intrusion detection system, ML based intrusion detection systems are more preferred, which turns out to be more advanced than traditional intrusion detection system. The analysis is performed by matching behavior of input traffic with safe traffic [8].

Research Questions:

Main objective of research is to investigate challenges and problems for examining the attacks.

- Which methods are used for investigating zero-day attacks by using artificial intelligence?
- What difficulties are faced in identifying zero-day attacks?
- What is extent for artificial intelligence usage in combatting zero day attacks?

Research Objectives:

- What are current methods to identify zero day attacks by using artificial intelligence?
- What are the major challenges in identifying and combating zero-day attacks

Techniques of attack detection:

Fuzz testing is a technique in which raw or random data is passed through software systems to find vulnerability in data and weak patch of security. This testing finds how software reacts to diverse and different data. This technique is especially effective in discovering security status and vulnerabilities like errors, overflow and data

Fuzzing is particularly effective in finding security vulnerabilities like buffer overflows, web crashes and code errors [9].

In Cyber-attacks detection a particularly new method combines the concepts of **heavy hitters and graph technique**. In this method unknown high volume data, unknown low volume data and attacks like DOS/DDOS attacks, data theft, scanning are investigated. Signatures and details of such attacks are unknown. Heavy hitters is a frequency estimation problem where we find samples of input traffic which fulfills strategy of cut off frequency stream.

Anomaly-based malware detection investigates threats and particularly zero day attacks through behavioral analysis. Behavioral analysis refers to investigating deviation from normal behavior in software or process form. But anomaly based detection has limitations because attackers can develop techniques to show malware safe, moreover anomaly based detection have high false positive rate. So it is required that malware detection mechanism must be updated to combat threats and have effective protection from zero day attacks [5].

Penetration testing is a simulated cyber-attack mechanism to find security gaps in system, application or network. This testing can be done to find whether these vulnerabilities can be exploited. Pen testing aims to determine vulnerability of a system by mimicking mindset of a cyber-attacker [5].

Outlier-based zero-day attack method trains detection models by considering normal data sent in past. This model discovers zero-day attacks by assuming zero-day attack has major differences from normal behavior. One-class Supportive Vector Machine (SVM) and auto-encoder are the two examples of machine learning models for attack detection. Secondly, how to process data and derive feature vector, an n-dimensional vector for numerical features is challenging. The process of designing feature vectors requires knowledge of cybersecurity which is especially valuable in designing zero-day attack machine learning model [11].

Zero Shot Learning (ZSL) is a methodology designed to solve the problem of data sets. it is a methodology used for managing the issue of not having data sets. Unlike outdated approaches, the aim of this approach is to help the issue of not having seen classes of data by generalizing that learning model data samples and not derived from pre-observed classes. This technique overcomes drawback of assessing ML centered IDS for detecting zero-day attacks because collection of data for zero-day attacks is a challenging task [7].

Conclusion:

This attack is one of the most significant challenges in modern digital world. This attack can exploit unknown weaknesses before developer implements effective defenses. This research highlights evolving nature of zero-day threats, their impact on individuals, organizations and the limitations of traditional security mechanisms in detecting and preventing such attacks. Addressing zero day attacks require active and multilayered security mechanism to combine AI, machine learning, behavioral analysis and continuous vulnerability assessment. Furthermore collaboration between researchers, software developers, security professionals, and policymakers is essential for cyber resilience. Although completely eliminating zero-day attacks is challenging but continuous improvement in detection techniques, automated security systems and proactive strategies can reduce their risks and consequences. In future research will be focused on building accurate and efficient security mechanisms, capable of identifying emerging zero-day threats while reducin false positives and computational overhead.

REFERENCES:

[1] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, "Zero-day attack detection: A systematic literature review," *Artificial Intelligence Review*, vol. 56, pp. 10733–10811, 2023, doi: 10.1007/s10462-023-10437-z.

[2] Y. Guo, "A Survey of Machine Learning-Based Zero-Day Attack Detection: Challenges and Future Directions," *Computer Communications*, 2023.

[3] L. Y. Por, Z. Dai, S. J. Leem, Y. Chen, J. Yang, F. Binbeshr, K. Y. Phan, and C. S. Ku, "A systematic literature review on AI-based methods and challenges in detecting zero-day attacks," *IEEE Access*, vol. 12, pp. 144150–144163, 2024, doi: 10.1109/ACCESS.2024.3455410

[4] V. Kumar and D. Sinha, "A robust intelligent zero-day cyber-attack detection technique," *Complex & Intelligent Systems*, vol. 7, pp. 2211–2234, 2021, doi: 10.1007/s40747-021-00396-9.

[5] H. Ishfaq, J. H. Shah, R. Saleem, and M. Afzal, "A distributed framework for zero-day malware detection using federated ensemble models," *PLOS ONE*, vol. 21, no. 1, Art. no. e0339907, Jan. 2026, doi: 10.1371/journal.pone.0339907

[6] M. Sarhan, S. Layeghy, M. Gallagher, and M. Portmann, "From zero-shot machine learning to zero-day attack detection," *International Journal of Information Security*, vol. 22, no. 4, pp. 947–959, 2023, doi: 10.1007/s10207-023-00676-0.

[7] Zhang, Z., Liu, Q., Qiu, S., Zhou, S., Zhang, C.: Unknown attack detection based on zero-shot learning. IEEE Access 8, 193981–193991 (2020) Sommer, R., Paxson,

[8] L. Yee Por *et al.*, "A systematic literature review on AI-based methods and challenges in detecting zero-day attacks," *IEEE Access*, vol. 12, pp. 144150–144163, 2024

[9] I. Mbona and J. H. P. Eloff, "Detecting zero-day intrusion attacks using semi-supervised machine learning approaches," *IEEE Access*, vol. 10, pp. 69822–69838, 2022, doi: 10.1109/ACCESS.2022.3187116.

[10] I. Mbona and J. H. P. Eloff, "Detecting zero-day intrusion attacks using semi-supervised machine learning approaches," *IEEE Access*, vol. 10, pp. 69822–69838, 2022, doi: 10.1109/ACCESS.2022.3187116.

[11] "Systematic review of current approaches and innovative solutions for combating zero-day vulnerabilities and zero-day attacks," *IEEE Access*, vol. 13, pp. 102071–102091, 2025, doi: 10.1109/ACCESS.2025.3577941.

[12] Li, Z. and X. Xu, "L2-BiTCN-CNN: Spatio-temporal features fusion-based multi-classification model for various internet applications identification," *Computer Networks*, vol. 243, Art. no. 110298, Apr. 2024, doi: 10.1016/j.comnet.2024.110298.

[13] I. Bojanova and C. E. Cardoso Galhardo, "Bug, fault, error, or weakness: Demystifying software security vulnerabilities," IT Professional, vol. 25, no. 1, 2023, doi: 10.1109/MITP.2023.3238631

[14] M. Souppaya, K. Scarfone, and D. Dodson, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities," NIST Special Publication 800-218, National Institute of Standards and Technology, Feb. 2022. DOI: 10.6028/NIST.SP.800-218

[15] J. F. Cevallos M., A. Rizzardi, S. Sicari, and A. Coen-Porisini, "HERO: From high-dimensional network traffic to zERO-day attack detection," *Computer Networks*, vol. 265, Art. no. 111264, 2025, doi: 10.1016/j.comnet.2025.111264.

IEEE Center for Excellence in Education & Research