International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Smart Innovations in Computer Science and Applications
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Zero Day Hunter : AI-Based Detection of Zero-Day Attacks in Modern Network Environment

Aniket Mehar
Department of Science and Technology,
G. H. Raisoni Skill Tech University, Nagpur, India

Annotation

The rise of artificial intelligence (AI) revolutionized both cybersecurity defenses and cyber-criminals' methods to exploit vulnerabilities. Cybercriminals continue to exploit previously undiscovered vulnerabilities, known as zero-day attacks, posing severe threats to cyber security. These attacks are particularly challenging to detect, as they target unknown weaknesses in systems before security teams can respond or act. Traditional intrusion detection systems (IDS) rely heavily on pre-existing attack signatures, making them ineffective against zero-day threats. Machine learning (ML) algorithms have recently become a promising solution for enhancing IDS capabilities by identifying anomalies and predicting potential vulnerabilities in real time.

This review paper explores how cutting-edge AI techniques, specifically ML, DL, and federated learning (FL), are harnessed to counter zero-day attacks. AI is used to defend against cyberattacks that exploit vulnerabilities unknown to existing security software. This research explores different AI methods used in cybersecurity, analyzes the data used to train these AI models, and evaluates how well various algorithms perform in actual cyberattacks. Moreover, key challenges in deploying ML for zero-day detection are highlighted, including handling imbalanced data, generalization across diverse types of attacks, and the trade-offs between accuracy and computational cost. The paper outlines future research directions to enhance AI-based zero-day attack defenses and strengthen proactive cybersecurity strategies.

Problem Statement

Traditional cybersecurity systems rely heavily on signature-based detection methods, which fail to identify zero-day attacks—previously unknown vulnerabilities exploited by attackers. These attacks are highly dangerous because they bypass conventional defenses and remain undetected until damage is done.

Objective

The primary objective of this project is to design and develop an AI-based detection system capable of:

- Identifying anomalous network behavior in real time
- Detecting potential zero-day attacks without relying on predefined signatures
- Enhancing overall network security through adaptive and intelligent threat detection.

Introduction

In the recent digital era, mitigating cyber risks is crucial for organizations, governments, and individuals. The proliferation of digital systems has coincided with a rise in the volume and sophistication of cyber threats, making it imperative to implement advanced defense mechanisms. Cybercriminals continuously seek out vulnerabilities in systems and networks to execute malicious activities, ranging from stealing sensitive data to disrupting critical infrastructure. Zero-day attacks are among the most dangerous threats, which exploit previously unknown vulnerabilities, giving defenders no time to react before the attack begins. As a result, securing information systems has become a fundamental aspect of modern cybersecurity strategies.

Cybersecurity threats come in many forms, as shown in Fig. 1, each with varying complexity and potential damage. Malware attacks, including viruses, worms, and ransomware, can compromise millions of devices worldwide. Phishing tricks people into sharing personal data, while Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks overload networks, causing service disruptions. More sophisticated methods, such as Advanced Persistent Threats (APTs), involve prolonged infiltration into a target network, often for espionage or sabotage. Traditional security tools, such as firewalls and antivirus software, are becoming insufficient in the face of increasingly sophisticated and voluminous cyberattacks, especially zero-day threats that target unpatched flaws. Recent attacks utilize undiscovered vulnerabilities and advanced techniques to evade detection sys-terms.

Given the evolving nature of cyber threats, IDS and intrusion prevention systems (IPS) are crucial for detecting malicious activities within networks. An IDS monitors traffic, analyzing incoming and outgoing data to detect potential threats (malicious activities).

Conventional IDSs, which rely on predefined signatures of known attacks, are highly effective in catching familiar threats but struggle against novel or previously unseen attacks like zero-day exploits. The limitations of signature-based detection have driven the adoption of more sophisticated detection techniques, especially those that leverage ML.

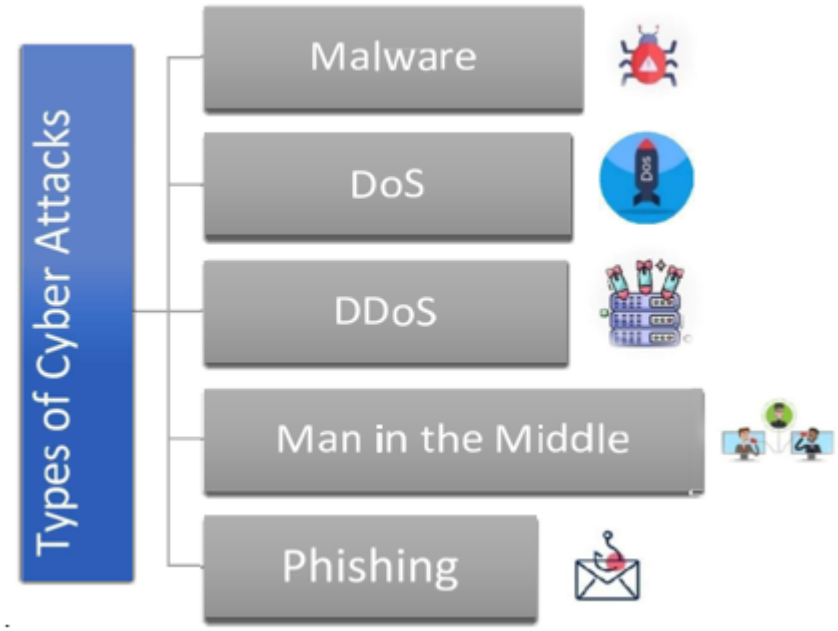

Fig. 1 Types of cyberattacks

The importance of ML in cybersecurity cannot be overstated. ML algorithms enhance the capabilities of IDS to identify and mitigate novel attacks. These models can detect even subtle anomalies of a

cyberattack by continuously analyzing vast amounts of network and system data. Moreover, ML models can adapt to changing attack patterns, making them more flexible and capable of detecting zero-day vulnerabilities that would go unnoticed by traditional IDS solutions. As cyberattacks evolve, the defenses and ML-based systems must be at the forefront of this battle. However, as cyber threats become more complex, challenges arise in scaling ML solutions across distributed networks with varied data sources. FL is a promising approach to overcome these challenges. FL is a decentralized ML approach that enables individual nodesto collaboratively train with a shared model without sharing raw data. FL, a collaborative ML technique, was introduced by Google in 2016. This is particularly important in cybersecurity, where privacy is concerned and the need for real-time threat detection makes traditional centralized learning impractical. FL keeps data localized to each device while sharing only the model updates, ensuring data privacy and collaboration.

The potential of FL to revolutionize cybersecurity is substantial, although challenges remain in its deployment. Enabling distributed learning, FL can enhance detection models, especially for zero-day attacks across different environments. With personalized federated learning (PFL), individual models can be fine-tuned to address the unique threat landscape of each client, making it a more robust solution in non-IID (independent and identically distributed) environments, where data distributions differ from one device or node to another.

This review paper comprehensively reviews ML, DL, and FL algorithms and their application in detecting zero-day attacks within cybersecurity. Various models and datasets that derive their performance are analyzed. The emerging role of FL in cybersecurity is also discussed. By examining advancements in ML-based IDS and addressing the remaining challenges, this review offers a foundation for future research to enhance defenses against evolving cyber threats.

The selection process for this survey relied on a comprehensive search of well-established academic databases, such as Google Scholar, IEEE Xplore, Science Direct, ResearchGate, Springer, ACM Digital Library, Scopus, Web of Science, Taylor and Francis, and Inder-science. Our scope was defined by objectives targeting zero-day attack detection using AI techniques, particularly ML, DL, and FL. The inclusion criteria required studies to focus on AI-driven methods for zero-day attacks relevant to our themes in peer-reviewed journals or reputable conferences.

The study was conducted using Google Scholar, IEEE Xplore, Science Direct, Research-Gate, Springer, ACM Digital Library, Scopus, Web of Science, Taylor and Francis, and Inder-science, with keywords like ‘zero-day attacks AND machine learning’, ‘deep learning in cybersecurity’, and ‘federated learning for zero-day threats. Results were screened by titles and abstracts to identify relevant studies, followed by a full-text review to ensure alignment with our research focus. Additionally, data points such as model types, datasets, and evaluation results were extracted and analyzed to identify trends and gaps in the literature review.

To the best of our knowledge, this literature review stands out by focusing on recent studies from 2024 and integrating various AI techniques: ML, DL, and FL. As a result, this review provides a robust comparison of cyberattack frameworks, offering valuable insights for researchers and serving as a research-based guide.

Additionally, it emphasizes the latest scientific papers and highlights cutting-edge advancements in the field.

The remainder of this survey is organized as follows: Sect. **2** introduces a background of zero-day attacks, IDS, and enhancing IDSs and Zero-day attack detection by AI techniques. Section **3** focuses on the benchmark datasets for IDS and zero-day attack detection.

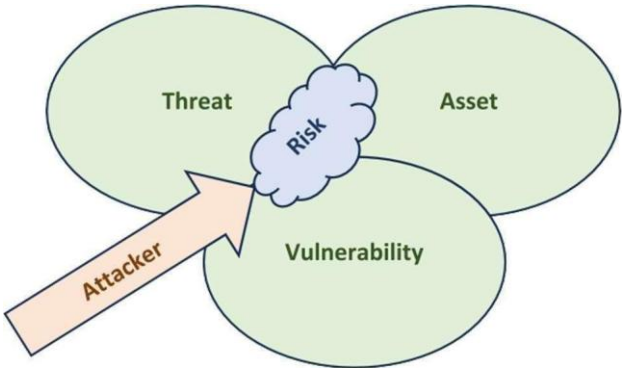

Fig. 2 How the attackers exploit the assets

increased every year. The CIA triad model sets the foundation for all security-based frameworks, which have been used for the past two decades to enforce security policies. It identifies possible threats and necessary solutions for those threats in the field of information security. The CIA triad model evolves around three major components, as shown in Fig. **3**.

Cyberattacks vary widely and can be classified according to the attackers' intentions and the information they need to gain access. Malware is malicious software that activates when the user clicks an unauthorized link or email attachment. Phishing is a common cyberattack where attackers send deceptive emails pretending to be legitimate sources to trick people into revealing sensitive information. Man-in-the-middle is another interesting

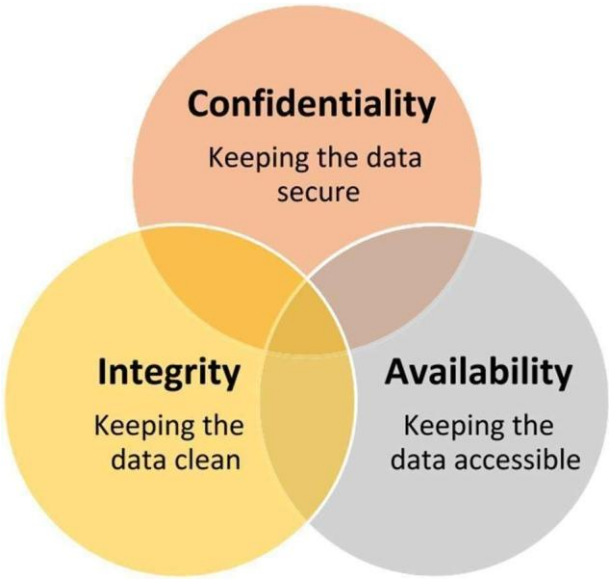

Fig. 3 The CIA triad model

attack where the intruders target the network itself. So, the sender will be sending the message without knowing that the hacker in the middle is receiving the information. One of the popular attacks, DoS, floods the system and the server with traffic to exploit the available resources and bandwidth. Unfortunately, the legitimate request cannot be addressed due to DoS attacks. Structured Query Language (SQL) attack inserts the malicious code into the server and forces the server to reveal sensitive information from the database. A Zero-day (0-day) attack is an unknown security threat in software applications for which the patch has not been released, or software developers are unaware of the attack. When such an attack occurs for the first time, defenders are given zero days of notice.

With the evolving digital era, cyberattacks have grown in volume and complexity not only against single systems but also against critical infrastructures.

DDoS attacks are among the most prevalent threats whose goal is to disrupt service availability by overwhelming systems with traffic. Volumetric DDoS attacks are type that engulfs networks with extremely large volumes of traffic, consuming all available bandwidth and rendering services inaccessible. These attacks have taken center stage due to the prevalence of Internet of Things (IoT) devices and the growth in botnet-fueled amplification tools, a major menace to current detection and countermeasures.

Worldwide DDoS attacks, both protocol and application-layer attacks, are becoming increasingly advanced through the utilization of high-level evasions. Their evading capabilities usually allow them to get beyond conventional security filters; therefore, precise and timely detection is increasingly necessary. Botnet attacks are one of the main drivers of such threats. A botnet consists of compromised systems owned by an attacker, used not only to launch DDoS attacks but also to deliver spam, credential stuffing, and spreading malware. Present studies emphasize the requirement of ML models for botnet detection with low false positives, and scalability.

Malware assaults are one of the most potent and versatile forms of cyberattacks. Variants like ransomware, spyware, and trojans can also steal sensitive information, encrypt files for ransom, or provide remote control to attackers. Malware's obfuscated and dynamic characteristics make its detection using traditional signature-based methods useless, hence the shift toward AI-based behavioral analysis methods. New, polymorphic, or zero-day malware variants must be caught by models that learn from previously observed patterns and do not overfit.

Another prevalent threat is phishing, which uses impersonating communication (typically websites or emails) to encourage users to give away credentials or install dangerous payloads. Phishing contributes toward a high success rate of successful data breaches and is typically used as a means of entry into broader intrusions. Phishing detection has recently explored the application of Natural Language Processing (NLP) and DL methods in detecting fine-grained signals in content, structure, and purpose. Fighting so many forms of cyberattacks, each with unique data characteristics and behavior traits refers to the need for adaptive and intelligent AI-powered systems, especially in handling unknown or zero-day variants.

1.1. Zero-day attacks

A zero-day attack is a new type of cyberattack that uses vulnerabilities that have not been publicly identified. These attacks are often undetected because they use new methods that avoid detection by existing security tools. This allows attackers to target specific systems without being noticed. Bilge and Dumitras studied how long these

Table 1. Zero-day terminologies

Zero-day Vulnerability	A zero-day vulnerability is one in which no fix is promptly available, and the seller could conceivably know. The non-attendance of a fix for multi-day helplessness introduces a zero-day risk to sellers and clients
Zero-day Exploit	A zero-day exploit is a type with a bit of programming, information, or a set of directions to exploit zero-day weakness
Zero-day Attack	A zero-day attack abuses zero-day helplessness

Fig. 4 Zero-day attack workflow

attacks last and how often they occur. Their findings show that a typical zero-day attack remains undetected for about 312 days on average. These attacks can rise significantly once vulnerabilities are made public. A zero-day vulnerability is a computer software vulnerability that is unknown to those who would be interested in mitigating the vulnerability. Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers, or a network. The security vulnerability in the software is susceptible to malware infection, remains unknown, and unfixed by the vendor, which is further exploited by malicious cyber criminals even before the vendor becomes aware of it. This type of exploit is called a zero-day attack. Table **1** defines the important terminologies related to zero-day, and Fig. **4** shows the workflow.

The primary difference between zero-day attacks and n-day attacks lies in the stage of vulnerability exploitation. Zero-day attacks target vulnerabilities are entirely unknown to the vendor and public, meaning no patch or fix exists when the attack occurs. This makes zero-day attacks particularly dangerous, as defenders have no prior knowledge or defense mechanisms, and the attack can go undetected for some time. N-day attacks are the exploitation of vulnerabilities that have already been disclosed and, in many cases, have been patched. However, attackers in n-day scenarios take advantage of systems that have not yet applied these patches, relying on delayed patch management. While n-day attacks can be mitigated by timely updates, zero-day attacks leave little room for immediate defense, requiring a more reactive approach.

In essence, zero-day attacks represent the exploitation of newly discovered weaknesses, whereas n-day attacks exploit known vulnerabilities that have not been adequately addressed. Table **2** summarizes these differences between 0-day attacks and n-day attacks.

1.2. Intrusion detection systems

The first IDS was proposed in 1980. For an IDS, an intrusion means an attempt to access information about computer systems or to damage the operation of the system in an illegal or unauthorized manner. An IDS is a computer security application that aims to detect various security violations, from attempted break-ins by outsiders to system.

Table 2 Zero-day attacks vs N-day attacks

Criteria	Zero-Day Attack	N-Day Attack
Definition	Exploits vulnerabilities unknown to the vendor or public, with no patch available	Exploits vulnerabilities that have been publicly disclosed, and a patch or mitigation is available
Discovery Stage made	It occurs before a vulnerability is public or patched	Occurs after the vulnerability is disclosed and possibly patched
Exploitation Window	Potentially high, as defenders are unaware of the vulnerability	Limited because patches or fixes are available; attackers exploit delayed patching by users
Risk Level	Very high due to no immediate defense mechanisms	Moderate to high, depending on how quickly patches are applied
Difficulty to Detect	It is difficult to detect since no known signatures exist in antivirus or security systems	It is easier to detect with known signatures and patches already available
Attacker Advantage	The attacker has a significant advantage defenses are typically non-existent	Attackers must exploit systems that have not yet applied the available patches
Mitigation	It is impossible to mitigate immediately; defense is often reactive	It can be mitigated by applying patches or updating systems regularly
Impact on Organizations	High impact, particularly on critical infrastructure or high-value targets	The impact varies; it can be high if patches are not applied promptly

Architecture Overview

The system follows a **multi-layered AI-driven pipeline**:

1. **Data Collection Layer**

- Network traffic data (packets, logs, flows)
- Sources: simulated datasets / real-time network capture

2. **Preprocessing Layer**

- Data cleaning and normalization
- Feature extraction (protocol, packet size, frequency, etc.)

3. **Feature Engineering**

- Selection of relevant features
- Dimensionality reduction (if needed)

4. **AI/ML Detection Engine**

- Algorithms used:
- Anomaly Detection (e.g., Isolation Forest, Autoencoders)
- Classification models (e.g., Random Forest, SVM)

- Detects deviations from normal behavior

5. Decision & Alert System

- Flags suspicious activities
- Generates alerts for potential zero-day attacks

6. Visualization Dashboard

- Displays attack insights
- Real-time monitoring graphs

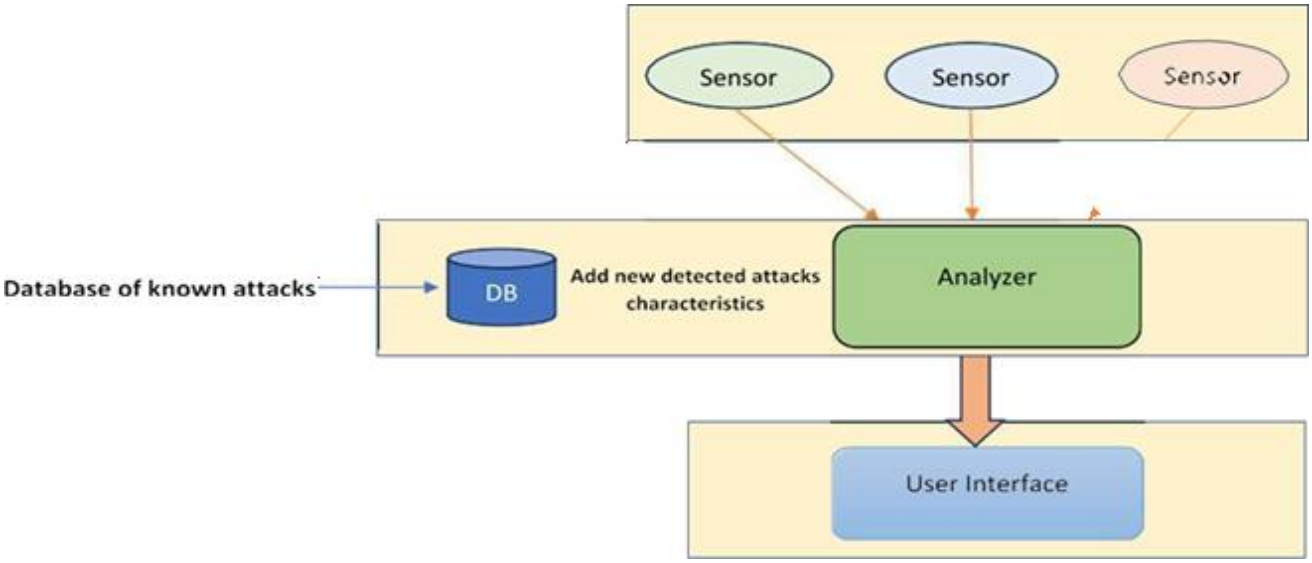

Fig.5 IDS general architecture

new attacks successfully due to their ability to identify deviations from normal profiles.

1.2. Enhancing IDSs and Zero-day attack detection by AI techniques

This section explores the enhancement of IDSs through advanced AI techniques, aiming to improve the detection of zero-day attacks and other sophisticated cyber threats. The discussion will cover how AI-based IDSs outperform traditional systems by leveraging ML, DL, and anomaly detection methods to recognize new and evolving attack patterns.

1.2.1. Machine learning

ML is the core field of AI that utilizes statistical techniques to enable systems to learn from data and make predictions or decisions without requiring explicit coding. The primary objective is to create autonomous systems that can learn from experience and adapt to changing environments.

Supervised ML is an ML paradigm that employs labeled examples to train models that can predict future occurrences. The learning algorithm learns a mapping function from input features to output labels by minimizing a loss function on the training data. This learned model can then be used to make predictions on new, unseen data.

Unsupervised ML is a ML paradigm that allows systems to identify hidden structures and relationships within unlabeled datasets. Unsupervised learning techniques, such as clustering and dimensionality reduction, can be used to explore and visualize large datasets.

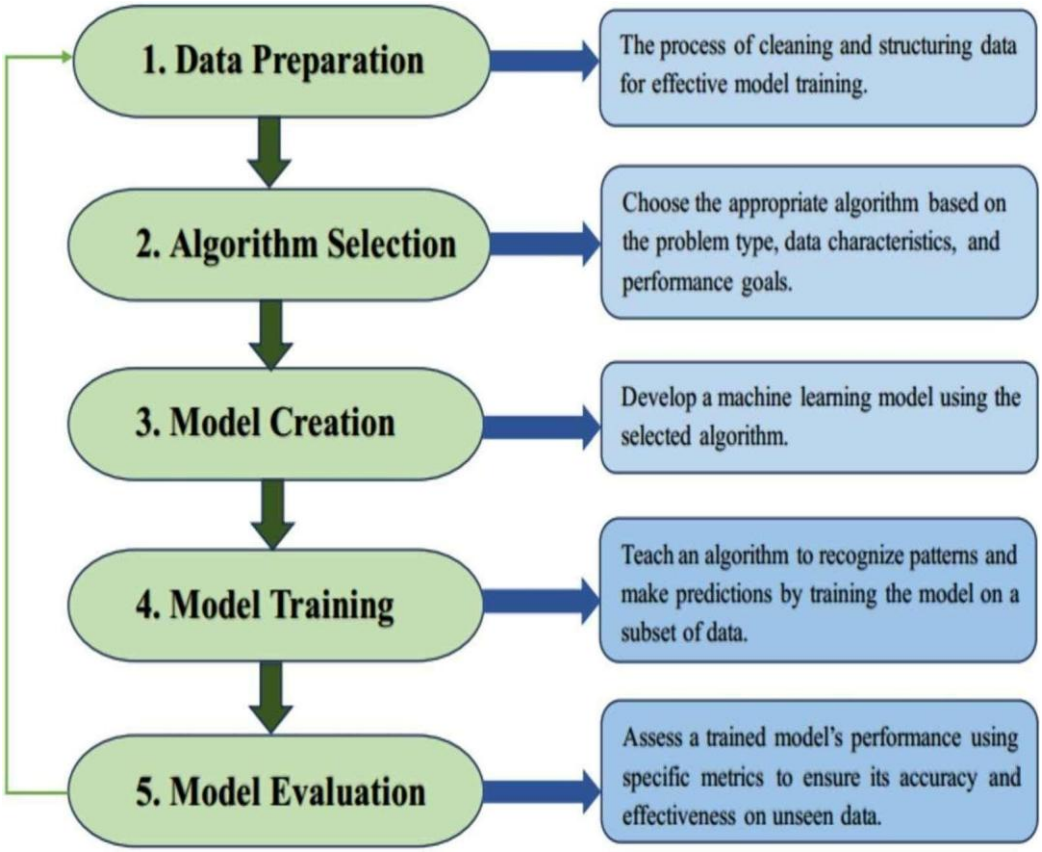

Fig. 6. The ML Process

To build an ML model, one must first gather and prepare relevant data, select an appropriate algorithm, partition the dataset into training and testing subsets, train the model on the former, and evaluate its performance on the rest. These steps are shown in Fig. **6**.

1.3.2. Deep learning

DL, a subset of AI, has emerged as a powerful tool for cybersecurity. Neural network (NN) architectures, such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs), have been employed to address challenges effectively, like intrusion detection and malware classification. These models have the potential to outperform traditional ML techniques in identifying APTs by analyzing temporal network traffic patterns.

ML techniques can significantly enhance the performance of cybersecurity systems by improving anomaly detection and threat classification. ML algorithms can process vast amounts of data to identify patterns indicative of malicious activities. ML models, lever-aging supervised, unsupervised, and DL techniques, can effectively classify and categorize various cyber threats, including malware, phishing attacks, and network intrusions.

These models can continuously learn from new data, improving their ability to detect and respond to emerging threats.

Integrating ML into cybersecurity significantly enhances both the accuracy and efficiency of threat detection by empowering systems to analyze vast quantities of data, identify intricate patterns, and minimize false positives. Furthermore, ML models, particularly DL techniques such as CNNs, facilitate the development of proactive defense mechanisms that can adapt to evolving threats, thereby providing a dynamic and robust approach to cyber security.

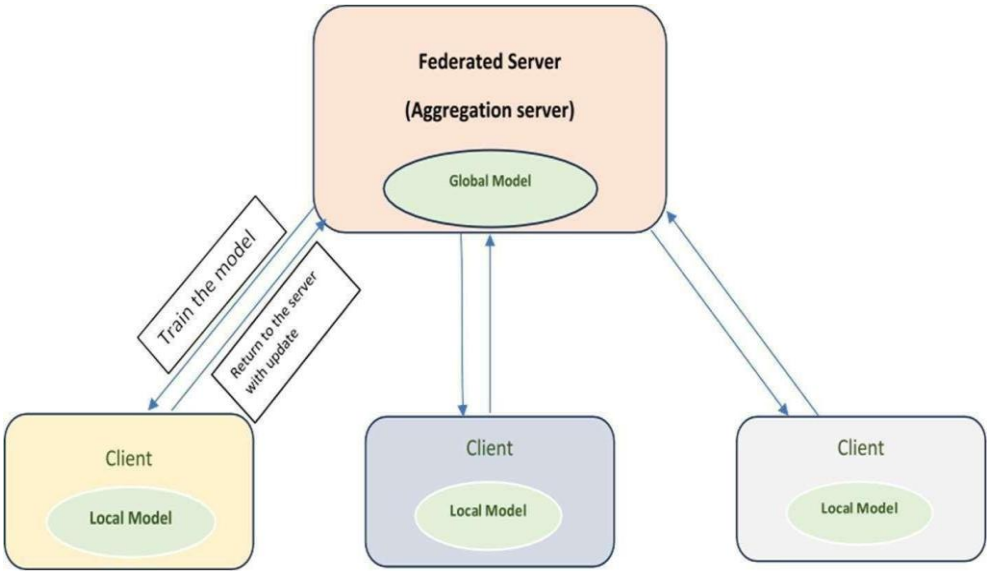

Fig. 7 The Concept of FL

1.2.1. Evaluation metrics

Multiple metrics are utilized to evaluate the performance of ML models in IDSs. These metrics are used to select optimal models. To comprehensively measure detection efficacy, a combination of metrics is often employed.

Accuracy is a suitable metric for balanced datasets, where the number of samples in each class is approximately equal. However, in imbalanced datasets, where one class significantly outnumbers the other, accuracy can be misleading, as the classifier may achieve

1. Accuracy

Accuracy measures the proportion of correctly classified instances among all instances.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

where:

- **TP** = True Positives
- **TN** = True Negatives
- **FP** = False Positives
- **FN** = False Negatives

2. Precision (P)

Precision is a key performance metric for imbalanced classification problems, as it measures the model's ability to identify positive instances accurately while minimizing false positive classifications.

$$P = \frac{TP}{TP + FP}$$

3. Recall (R)

Recall is a crucial metric for evaluating Intrusion Detection System (IDS) performance, as it measures the model's ability to identify attacks accurately and minimize false negatives.

$$R = \frac{TP}{TP + FN}$$

4. F-Measure (F1-Score)

The F-measure is a valuable metric for evaluating the performance of classification models, particularly in imbalanced datasets, as it considers both precision and recall.

$$F_1 = \frac{2 \times P \times R}{P + R}$$

5. False Negative Rate (FNR)

The False Negative Rate is a critical metric for evaluating IDS performance, as it measures the proportion of actual attacks that are incorrectly classified as normal.

$$FNR = \frac{FN}{TP + FN}$$

6. False Positive Rate (FPR)

The False Positive Rate is a critical metric for evaluating IDS performance, as it measures the proportion of normal instances that are incorrectly classified as attacks, thereby indicating the rate of false alarms.

$$FPR = \frac{FP}{FP + TN}$$

True positive (TP), false positive (FP), true negative (TN), and false negative (FN) are key performance metrics used to evaluate the performance of IDS. In attack detection, the positive class represents malicious activity, and the negative class represents benign activity. The selection of appropriate performance metrics depends on the specific goals of the IDS, such as maximizing detection accuracy, minimizing false alarms, or balancing both.

7. Matthews Correlation Coefficient (MCC)

The **Matthews Correlation Coefficient (MCC)** is a comprehensive metric for evaluating the performance of binary classification models. It incorporates all four components of the confusion matrix (**TP, TN, FP, and FN**) to provide a balanced assessment of model quality. MCC is particularly valuable for **imbalanced datasets** because it remains robust regardless of class distribution and does not favor the majority class.

MCC measures the correlation between the actual labels and the predicted labels. Its value ranges from **−1 to +1**, where:

- **+1** indicates perfect prediction,
- **0** indicates performance no better than random chance,
- **−1** indicates complete disagreement between predictions and actual outcomes.

Due to its balanced nature, many researchers consider MCC an important metric for evaluating the effectiveness of **Intrusion Detection Systems (IDSs)**.

$$MCC = \frac{(TP \times TN) - (FP \times FN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}$$

Challenges Faced

1. Lack of Real Zero-Day Attack Data

One of the biggest challenges was the absence of real-world zero-day datasets. Since zero-day attacks are unknown and rare, publicly available datasets often contain only known attack patterns.

2. Data Imbalance

One of the biggest challenges was the absence of real-world zero-day datasets. Since zero-day attacks are unknown and rare, publicly available datasets often contain only known attack patterns.

Network traffic datasets are usually highly imbalanced, where:

- Normal traffic = very high
- Malicious traffic = very low

3. Feature Selection Complexity

Selecting the right features from network traffic (e.g., packet size, protocol type, time intervals) was challenging.

4. Feature Selection Complexity

Selecting the right features from network traffic (e.g., packet size, protocol type, time intervals) was challenging.

5. High False Positive Rate

Anomaly detection models tend to flag many normal activities as suspicious. This led to:

- Alert fatigue
- Reduced trust in the system

1. Future directions

The detection of zero-day attacks using ML is rapidly evolving, but several challenges remain, offering promising avenues for future research. As the landscape of cybersecurity threats becomes more complex, the following directions hold significant potential for advancing the detection of zero-day attacks.

1.1. FL and privacy-preserving approaches

Centralized ML models can be vulnerable to data breaches and privacy violations, especially when dealing with sensitive data, such as medical records or financial information. FL enables multiple clients to participate in model training by sharing model updates, with a central server rather than raw data. This approach can help detect zero-day attacks in environments where privacy restricts data sharing. FL in cybersecurity research could focus on how FL can be applied across different organizations, each contributing to a global model while keeping their data private. Such models could be trained on attack data from multiple networks without exposing sensitive information, thereby improving the detection of previously unseen zero-day attacks across distributed systems.

Challenges in FL for zero-day detection: One major hurdle is the communication cost and latency in FL. Ensuring efficient and scalable deployment in real-time threat detection scenarios is crucial for future research.

Privacy-preserving ML combining FL with other privacy-preserving techniques like homomorphic encryption or differential privacy could offer additional layers of security. This approach enables security and privacy-preserving ML by training models on encrypted data, improving the detection of zero-day vulnerabilities.

Conclusion

The integration of ML into cybersecurity is revolutionizing threat detection by enabling proactive, intelligent, and adaptive responses to zero-day attacks. Key areas such as FL, XAI, and adversarial robustness are essential for improving the detection systems' accuracy, scalability, and security. These approaches allow real-time processing and learning from evolving threats, helping organizations stay ahead in an ever-changing cyber landscape. While the potential is vast, addressing the current limitations of ML and strengthening its

resilience against adversarial attacks remains critical for long-term effectiveness. The review also emphasizes the unique potential of FL in cybersecurity. FL, with its decentralized data learning approach, supports privacy-preserving and secure on-device AI, making it a suitable solution for sensitive data environments. By analyzing its application in various fields, such as finance and computer vision, the paper highlights the potential of FL and underscores the challenges that need to be overcome to realize its full potential in real-time cybersecurity scenarios. This review offers future directions to enhance FL's role in threat detection, paving the way for more resilient defenses against emerging cyber threats.

Author contributions S.A.A., S.M.A., F.M.T., and M.M.S. contributed to the methodology; S.A.A., S.M.A., F.M.T., and M.M.S. performed the validation; S.A.A., S.M.A., F.M.T., and M.M.S. curated the data; S.A.A. contributed to writing—original draft; S.M.A., F.M.T., and M.M.S. were involved in writing—review and editing; and S.A.A. and S.M.A. assisted in the visualization.

Funding Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB). The authors received no funding for this work.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval Not applicable.

Informed consent Not applicable.

References

1. Madou M (2022) Defence against the dark art of zero-day attacks. Netw Secur. https://doi.org/10.12968/ s1353-4858(22)70066-9
2. Vasani V, Bairwa AK, Joshi S, Pljonkin A, Kaur M, Amoon M (2023) Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion. Electronics 12(20):4299. https:// doi.org/10.3390/electronics12204299
3. Haija AAQ, Altamimi S, AlWadi M (2024) Analysis of extreme learning machines (ELMs) for intelligent intrusion detection systems: a survey. Expert Syst Appl 253:124317
4. Mijwil M, Aljanabi M (2023) Towards artificial intelligence-based cybersecurity: the practices and ChatGPT generated ways to combat cybercrime. Iraqi J Comput Sci Math 4(1):65–70
5. Tariq U, Ahmed I, Bashir AK, Shaukat K (2023) A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. Sensors 23(8):4117

6. Lopes A, Mamede HS, Reis L, Santos A (2024) Common techniques, success attack factors and obstacles to social engineering: a systematic literature review. Emerg Sci J 8(2):761–794
7. Ahmad R, Alsmadi I, Alhamdani W, Tawalbeh LA (2023) Zero-day attack detection: a systematic literature review. Artif Intell Rev 56(10):10733–10811
8. Rugina JM (2023) Through the eyes of attackers: a comprehensive analysis of cybersecurity strategies in international relations. Afro Eurasian Stud 12(1):40–57
9. Femi-Oyewole F, Osamor V, Okunbor D (2024) A systematic review of social engineering attacks & techniques: the past, present, and future. In: 2024 international conference on science, engineering and business for driving sustainable development goals (SEB4SDG) (pp. 1–12). IEEE
10. Emmah VT, Ejiofor CI, Onyejegbu LN (2017) Review of malware and techniques for combating zero-day attacks. Int J Eng Res Technol 6(11):267–275
11. Dobák I (2021) Thoughts on the evolution of national security in cyberspace. Secur
12. Def Q 33(1):75–85
13. Kopczewski M, Ciekanowski Z, Nowicka J, Bakalarczyk-Burakowska K (2022) Security threats in cyberspace. Sci J Mil Univ Land Forces 54:415
14. Sharma A, Gupta BB, Singh AK, Saraswat VK (2023) Advanced persistent threats (APT): evolution, anatomy, attribution and countermeasures. J Ambient Intell Humaniz Comput 14(7):9355–9381
15. Teichmann F, Boticiu SR, Sergi BS (2023) The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate? Int Cybersecur Law Rev 4(3):259–280
16. Zhou KQ (2022) Zero-day vulnerabilities: unveiling the threat landscape in network security. Mesop J CyberSecur 2022:57–64. https://doi.org/10.58496/mjcs/2022/007
17. Ekong AP, Etuk A, Inyang S, Ekere-obong M (2023) Securing against zero-day attacks: a machine learning approach for classification and organizations' perception of its impact. J Inf Syst Inform 5(3):1123–1140. https://doi.org/10.51519/journalisi.v5i3.546
18. Maynard P, McLaughlin K, Sezer S (2020) Decomposition and sequential-AND analysis of known cyber-attacks on critical infrastructure control systems. J Cybersecur 6(1):tyaa020. https://doi.org/10. 1093/cybsec/tyaa020
19. Armijos A and Cuenca E (2023) Zero-day attacks: review of the methods used based on intrusion detection and prevention systems. In: 2023 IEEE Colombian Caribbean conference (C3)