Iraqi Journal for Computers and Informatics
Available online: https://ijci.uoitc.edu.iq/index.php/ijci
Volume 52, issue 1. 2026

Print ISSN: 2313-190X, Online ISSN: 2520-4912

A Comprehensive Review of Machine Learning and Deep Learning Approaches for Zero-Day Attack Detection in Cybersecurity Systems

Maha Khalil Ibrahim

Mobile Communications and Computing Engineering Department, College of Engineering, University of Information Technology and Communications, Baghdad, Iraq

ARTICLEINFO

Keywords:

Machine Learning, Zero-Day Attack, Internet of Things, Deep Neural Network, vulnerabilities.

ABSTRACT

Over the past decade, the rapid digital transformation of infrastructures to digital forms, such as cloud computing, Internet of Things (IoT), and large-scale interconnected network systems, has made the threat of cybercrime much more pronounced. Of those, Zero-Day attacks are regarded as the most serious since they are previously unseen and so the traditional signature-based intrusion detection systems are useless. This paper presents an in-depth overview of machine learning (ML) and deep learning (DL) methods of detecting Zero-Day attacks. The methodology is based on reviewing, analyzing, and synthesizing recent literature, which is applied to ML, DL, and hybrid methods, threat intelligence integration, and real-time intrusion detection systems. The findings suggest that both ML and DL methods have high detection accuracy but have a number of weaknesses including high computational complexity, data imbalance, scarce availability of labeled data, and susceptibility to adversarial attacks. Moreover, this review shows some of the main gaps in research, especially in coping with the unknown attack patterns, the development of lightweight and real-time detection models, and the enhancement of the generalization abilities. Finally, the research paper shows that it is crucial to establish adaptive, scalable, and hybrid intelligent systems to improve the detection of Zero-Day attacks. To enhance actual cybersecurity applications in the future, future studies should focus on efficient learning mechanisms, strong adversarial defenses, and data-efficient models.

1. INTRODUCTION

Over the last few years, the speed of the development of digital infrastructures, such as cloud computing, Internet of Things (IoT), and large-scale networked systems, has intensified the threat of cyberattacks. The Zero-Day Vulnerability is one of the most serious and dangerous threats, as they are defined as unknown security vulnerabilities, which are used by malicious actors prior to the release of the patch or the fix by the developers [1]. Owing to the lack of previous information concerning such vulnerabilities, the traditional security measures find it hard to detect and stop such attacks [2].

Conventional intrusion detection systems rely heavily on signature-based models, where such are incapable of detecting unknown threats. Therefore, modern cybersecurity has assumed a different form of smart approaches with the advantages of Machine Learning-Based Detection to identify suspicious system activity [3]. The techniques enable the systems to learn according to the data and detect previously unknown attacks, this is why they are highly suitable in the scenario of Zero-Day [4].More recent developments in Deep Neural Networks have improved detection results by automatically deriving multi-faceted

E-mail address:
maha.ibrahim@ uoitc.edu.iq

Received 22 April 2026, Accepted 09 May 2026

DOI: 10.25195/ijci.v52i1807.

features on massive datasets without manually deriving features [5]. They are popular in Security Analytics, in which large amounts of network and system data are processed to detect suspicious behavior and possible threats[6] .

Intelligent Intrusion Detection has emerged as one of the most noticeable solutions in modern cybersecurity because it would be applicable to augment traditional systems of detecting threats with artificial intelligence to improve their accuracy and adaptability.[7,8]

Other important considerations are the Threat Intelligence which can be integrated with machine learning to assist in identifying and responding to Zero-Day Attacks in real time by integrating threat intelligence and machine learning [9-10]. In addition, Hybrid Machine Learning Models have performed well when it comes to the combination of various algorithms in order to enhance detection and minimize false positives [11]. Such hybrid models are particularly useful especially in the challenging environments that one model might not be helpful [12]. One of the most important needs in cybersecurity is Real-Time Detection because any delay in the detection of an attack can be catastrophic [13]. Machine learning models are also being optimized, in order to be able to work in real time conditions and with high precision [14]. Lastly, Network Traffic Analysis also plays an important role in detecting of Zero-Day Attacks as it is concerned with monitoring and investigation of data packet traversing the networks intrusion by comparing the trends and anomalies in traffic [15].

This paper systematically reviews the machine learning (ML) and deep learning (DL) solutions for identifying Zero-Day attacks. Critically reviews the existing methodologies based on their methods, strengths, weaknesses and applicability. The key contributions of this paper are:

(1)introducing a timely and systematic literature survey on ML and DL-based detection techniques,

(2)making a comparative analysis of the state-of-the-art approaches according to their advantages and disadvantages,

(3)discovering the critical research issues, including data imbalance, unlabeled datasets, and susceptibility to adversarial attacks, and

(4) suggesting future research directions for developing hybrid, adaptive, and real-time detection systems.

The paper is organized into six key parts: Introduction, Related Work, Methodology and Framework, Discussion, Challenges and Future Research Directions, and Conclusion. It also includes a literature summary and a comparison table of the state of the art concerning strengths and weaknesses of the currently in use zero-day attack detection measures.

2. RELATED WORK

The failure of conventional signature-based Network Intrusion Detection System (NIDS) to detect previously unseen threats has made detection of zero-day attacks a critical area of research. Recent research investigated machine learning (ML), deep learning (DL), reinforcement learning, and hybrid models to improve generalization and detection of unknown attacks.

Arun et al. (2025) suggested a deep learning system that uses Long Short-Term Memory (LSTM) networks to detect and simulate zero-day attacks. The model takes advantage of recurrent neural networks to estimate the temporal correlations of network traffic and to identify abnormal behavior. Their findings indicate that LSTM-based networks can greatly enhance the detection of anomalies because they learn sequential network flow patterns and thus identify a previously unknown attack patterns[16] .

Alam et al. (2024) proposed a Deep Reinforcement Learning (DRL)-based NIDS augmented with stacked LSTM architecture to enhance the ability to learn features and make decisions. The experiment was done using several benchmark datasets of various types of attacks including DoS, DDoS, injection, brute force and backdoor attacks. In order to replicate zero-day conditions, particular attack types (e.g., DoS and Backdoor) were not trained, but were used in testing.
Also, the authors covered the issue of class imbalance by employing oversampling methods like SMOTE, Borderline-SMOTE, ADASYN, and K-means SMOTE. Their results indicate that DRL along with LSTM significantly improves detection of known and unseen attacks [17].

Sarhan et al. (2023) proposed Zero-Shot Learning (ZSL) framework in the detection of zero-day attacks as a mapping of network traffic characteristics into semantic representations of familiar attack classes. The model makes inferences about visible and invisible attack types in the inference phase.

The paper proposed a novel evaluation metric the Zero-Day Detection Rate and used Wasserstein Distance to estimate the difference in the distributions across attack classes. The findings show that attacks whose feature distributions differ significantly are more difficult to detect by the traditional ML-based NIDS models[18] .

Ali et al. (2022) carried out a detailed comparative study of machine learning and deep learning approaches to detecting zero-day attacks. The work compared various models in terms of performance (accuracy, precision, recall and F1-score) with various datasets.
The findings indicate that there is no single model that was found to be superior to others in all cases, and hybrid and adaptive solutions are what would be needed to have a robust zero-day detection[19] .

The use of heavy-hitter analysis and graph-based techniques led to a strong model of zero-day attack detection proposed by Kumar and Sinha. Their approach consists of two stages: generation of signatures and evaluation. The model recorded good results in benchmark datasets like CICIDS18, with an accuracy of more than 91 percent in binary classification problems. It shows the usefulness of combining statistical analysis and graph based modelling in the recognition of low frequency attack patterns [20].

The Al-Rushdan et al. (2019) suggested a zero-day attack detection and prevention framework of Software-Defined Networks (SDN) based on a modified Cuckoo Sandbox environment. The system seals infected clients to avoid the spread of malware in the network laterally.
Their experimental results show that the proposed approach is able to detect and contain zero day malware and to prevent its propagation to network nodes [21]. See Table 1.

Table 1 Comparison Table of Recent Studies

Ref.	Approach	Model Type	Zero-Day Strategy	Strengths	Limitations
[16]	LSTM-based DL	Deep Learning	Detects anomalies via temporal patterns	Strong sequential learning	Limited generalization to highly novel attacks
[17]	DRL + Stacked LSTM	Hybrid DRL	Excludes attack types during training	High adaptability + imbalance handling	Depends on dataset quality
[18]	Zero-Shot Learning	Semantic ML	Maps known → unseen attack relations	Good generalization ability	Sensitive to distribution shift
[19]	Comparative ML/DL Study	Benchmark Analysis	Evaluates multiple models	Comprehensive evaluation	No novel detection model
[20]	Graph + Heavy-Hitter	Hybrid Statistical	Signature + graph analysis	High accuracy (~91%)	Computational complexity
[21]	SDN + Sandbox	Prevention System	Isolation-based mitigation	Strong containment ability	Limited to SDN environments

3. METHODOLOGY AND FRAMEWORK FOR ZERO-DAY ATTACK DETECTION

To be able to provide an overview of the methods that have been employed in this work a distinction can be made between three main types of Zero-Day attack detection methods: Machine Learning (ML) based methods, Deep Learning (DL) based methods and Hybrid methods. ML-based approaches rely on the classical algorithms such as Support Vector Machines (SVM), Random Forest (RF), Decision Trees (DT) which are effective for detecting known attack patterns but less effective for unknown attacks Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN) are DL-based methods that can extract more complex features and identify unknown attack patterns with a greater accuracy. Hybrid methods integrate several ML and DL methods to improve detection performance, reduce false positives, and increase generalization ability. Figure 1 shows how these approaches can be classified.

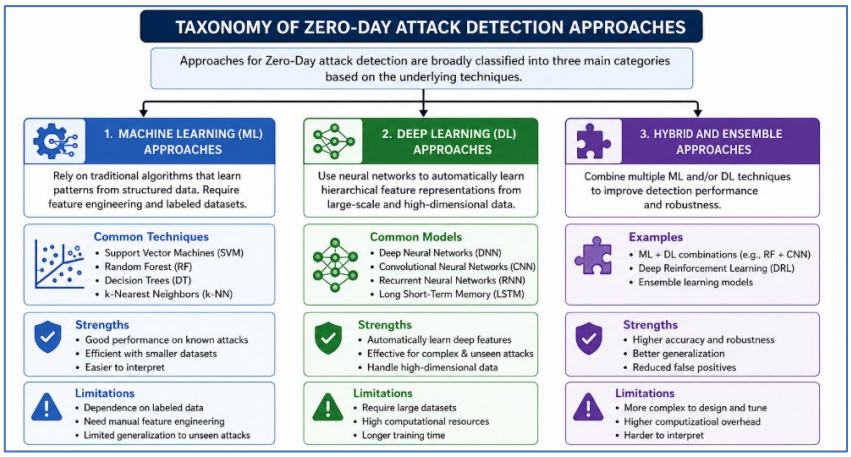

Figure 1 *: Taxonomy of Zero-Day Attack Detection Approaches (Machine Learning, Deep Learning, and Hybrid Methods)*

3.1 Proposed Detection Framework

The detection systems of Zero-Day attacks developed nowadays use a complex and multi-step system that allows identifying new and previously unknown threats. It starts with the collection of data of heterogeneous sources, including network traffic, system logs, Internet of Things (IoT) devices, and security monitoring tools. These diverse sources of data provide useful behavioral data which is mandatory in detecting abnormalities associated with Zero-Day attacks. Unlike the out-of-date signature-based systems, this framework pays attention to the analysis of behavior rather than fixed attack patterns.
Preprocessing is crucial after gathering the data to enhance the quality of the data and suitability to be used in machine learning models. The procedures involved in this step are the removal of noise, missing data, standardization of the numeric data and coding of nominal variables. Effective preprocessing does not only make the computationally costly aspect of cybersecurity cheaper, but also increases the detection accuracy.

The second step is concerned with the feature engineering, which is possible by means of manual or automatic learning. Traditional techniques rely on domain knowledge to reveal any meaningful property such as the size of the packets, the length of the connection and frequency of traffic. Deep learning approaches on the other hand enable automatic learning of features, which entails deriving hidden representations without having to be aware of any data beforehand. This feature improves greatly the ability to detect intricate and subtle attack patterns linked to Zero-Day threats.
The main element of the framework is model training in which various learning paradigms are used based on the type of data and the objectives of the detection. It is possible to employ supervised learning techniques, when the labeled data are at hand, and the unsupervised and semi-supervised techniques can be implemented in the Zero-Day scenario, as the labeled attack data are nonexistent. Deep learning models including Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are also able to detect complex to identify intricate patterns in high dimensional data, thereby improving detection performance. Another type of multi-algorithm model is the hybrid and ensemble models which are employed to enhance potency and reduce false positive.

After the training of the detection engine, the detection engine continuously scans incoming data in real time, and tag it as either normal or suspicious behavior. This aspect is essential in identifying any potential Zero-Day attacks by observing anomalies of learned patterns. Output of the detection engine is then passed to the response module which generates alerts and may lead to automated remedies such as blocking malicious traffic or updating threat intelligence systems.

Finally, the framework performance is compared to standard performance metrics, e.g., accuracy, precision, recall, F1-score and false positive rate. These metrics are the general quantification of efficiency of the system in the capability to detect attacks and reduction of the false alarm required in the real-life application of cybersecurity.

3.2 Framework Visualization

The model depicted above can be depicted as a pipeline, which is implemented in an order in which data acquisition, preprocessing, feature engineering, model training, and real-time detection are integrated. This sequential flow will offer round

the clock monitoring and analysis of the network activities in such a way that the system will be able to adapt dynamically to new threats. Scaling and intelligent detection, provided by the combination of machine learning and deep learning strategies in this pipeline, is appropriate in the environment of the contemporary cybersecurity such as cloud computing and IoT systems.

3.3 Detection Model Representation

Mathematically, the process of detection could be represented as a mathematical function, which takes as input data and outputs a classification result. Given an input feature vector X, the trained model, The output of (X) is given . Y, with the output being either normal or abnormal. The model is frequently trained in the context of the Zero-Day detection, where anomaly scoring systems are used instead of explicit labels of classes because unknown attacks are not presented in the training data. Thus, those cases that are considerably different in comparison to having learned normal patterns are reported as possible threats.

3.4 Key Insights of the Framework

The framework analysis shows a number of significant insights. To begin with, anomaly-based detection is more efficient than signature-based systems to detect Zero-Day attacks because it can detect unfamiliar patterns. Second, deep learning methods improve the detection performance by a large margin because it automatically extracts high-level features using large amounts of data. Third, hybrid and ensemble models are more robust and generalize better than single-model approaches. Nevertheless, real-time detection and high accuracy is a significant problem that must be overcome especially in high-speed network settings.

3.5 Advantages and Limitations

The proposed framework has a number of benefits, such as the ability to identify unknown attacks, the potential to scale to large datasets, and the ability to adapt to different environments, such as cloud and IoT systems. Additionally, intelligent models are integrated so that real-time monitoring and proactive threat detection can be performed.

General proposed farmwork of Zero-day attack detection using deep and machine learning is illustrated in Figure 2.

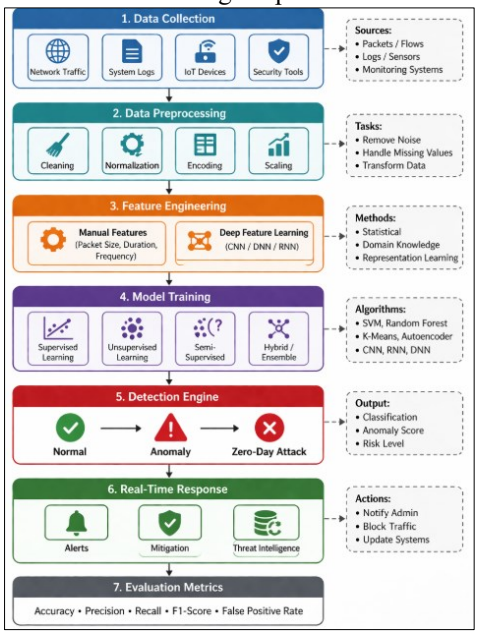

Figure 2 *: General Framework for Zero-Day Attack Detection Using Machine Learning and Deep Learning*

4. DISCUSSION

This part has critically reviewed the studies reviewed and has discussed the significant findings, the emerging trends, and the existing challenges to the machine learning-based Zero-Day attack detection

4.1 Comparative study of detection methods.

The reviewed literature indicates that machine learning (ML) algorithms have significantly increased the ability to detect cyber threats compared to the traditional signature-based algorithms. Among the ML methods that demonstrate high performance in identifying familiar patterns of attack, there are supervised learning models, such as Random Forest and Support Vector Machines. Their usability in the situation of Zero-Days is however limited since they are based on labeled datasets.

Deep learning (DL) models, especially Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs) demonstrate a higher performance in identifying complex and previously unseen attack patterns. These models have the ability to automatically derive hierarchical features on raw data and these features are very applicable in detecting Zero-Day attacks. However, their excessive computational rate and the complexity of training is a major hindrance.

Hybrid and ensemble models have become the most viable solutions, which are a combination of the advantages of various algorithms. These models are more accurate, better generalize and have lower false positives than single model methods. However, their implementation complexity and resource demands make them challenging to be implemented in real life.

4.2 Future Trend in Zero-Day Attack Detection

According to recent research, there are a number of significant trends in cybersecurity research. To start with, it is evident that there is a growing trend toward hybrid machine learning models that combine several models to improve on detection. Second, threat intelligence and machine learning models have enhanced both the real-time detection of emerging and unknown threats.

The usage of lightweight and real-time detection models is another trend that is important. Researchers have been paying a lot of attention to the optimization of deep learning structures so that they can minimize the number of computations and still be able to detect objects with high precision. Moreover, big data analytics and cloud-based solutions have facilitated the processing of large amounts of data on network traffic in a scalable and efficient manner.

Moreover, more than ever before there is interest in the use of more advanced methods like adversarial machine learning, explainable AI (XAI), and federated learning to enhance the robustness, transparency, and privacy of models.

4.3 Major Problems of current solutions.

Even with the progress made, there are still a number of challenges that are critical in detecting Zero-Day attacks. The unavailability of high-quality labeled datasets is one of the problems, and it restricts the performance of supervised learning methods. Zero-Day attacks are both unrepresentative and unknown, which makes it hard to gain representative training data.

Tradeoff between computational efficiency and detection accuracy is another challenge. Deep learning models are accurate, but not always suitable in real-life applications as they consume a lot of resources.

Model complexity also poses the issue, especially in hybrid systems, where the complexity of system design is raised, as well as interpretability, through the addition of many algorithms into the system. Also, adversarial attacks can be a significant threat, since the attackers could interfere with input data to avoid detection mechanisms.

Lastly, the use of third-party threat intelligence sources presents the possibility of risks associated with data availability, reliability, and complexities in integrating the data.

4.4 Essential Insights and Research Implications.

Resting on the review of the available literature, there are some valuable conclusions that may be made. To begin with, there is no one machine learning model that can be used to counter the complexity and variability of Zero-Day attacks. Rather, it is more efficient to have hybrid and adaptive solutions, utilizing the advantages of various techniques.

Second, there is a strong need to develop lightweight and efficient models, which are capable of working in real-time scenarios without affecting the detection performance. Third, to increase the likelihood of reliable cybersecurity systems, it is necessary to make models resistant to adversarial attacks.

In addition, the limitation of the labeled datasets should be addressed by future research on data-efficient learning algorithms, including semi-supervised and unsupervised learning, to avoid the need to label the datasets. Another important aspect of enhancing transparency and trust in machine learning-based security systems is the need to integrate explainable AI techniques.

In general, the results emphasize the need to develop smart, dynamic and scalable structures to fight successfully Zero-Day attacks in contemporary digital space.

5. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Although machine learning (ML) and deep learning (DL) methods have achieved significant progress in detecting Zero-Day attacks in cybersecurity systems, a range of critical issues continues to hinder their application to the real world[22].

Some of the issues that need to be addressed are: Lack of labelled Zero-Day attack data sets. Zero-Day attacks are inherently unknown and hence it is extremely difficult to come up with representative training data. The majority of the existing models are historical models and have limited generalizability to new patterns of attacks [23]. In addition, cybersecurity data sets have a very skewed distribution of benign traffic that vastly outnumber malicious samples. It causes skewed learning and sub-optimal performance of rarely-used classes of attack detection [23.[24][

The other notable disadvantage is that deep learning models are extremely complex to compute. Advanced architectures like Deep Neural Networks (DNNs) and Convolutional Neural Networks (CNNs) are extremely accurate but due to the complexity of the calculations cannot be practically implemented in real-time and resource-limited environments [25]. This creates a trade-off between detection accuracy and system efficiency particularly in large scale network location .[26]

The other significant challenge is the generalization ability. The majority of ML-based intrusion detectors tend to overfit during the training process such that when shown to new kinds of attacks, their performance reduces. This is especially an issue in the Zero-Day cases where the attack patterns are not known and need to be discovered without having been previously experienced [24, 26]. Future research should focus on more adaptive solutions such as transfer learning, zero-shot learning and open-set recognition [27].Moreover, adversarial attacks are also a significant threat to ML-based cybersecurity systems. Attackers can manipulate input data to lie to detection models, compromising their reliability and the trustworthiness of detection models in the real world. So, to counter such manipulations, there is a need to design a robust model and train adversarial systems that are more resilient to them.

Limitations on feature representation is another problem. Conventional feature engineering algorithms use extensive domain knowledge and might not be able to reveal the complicated and high-dimensional relationships in network traffic data. They can be overcome by using deep representation learning, which automatically learns meaningful features of raw data [28].

In addition, modern intrusion detection systems are in need of real-time detection ability. Most of the current methods are not designed to be used in low-latency systems and might not be able to effectively handle fast network traffic [28]. This explains why there is a necessity in lightweight, streaming-based, and online learning models, which can be fast and which do not compromise accuracy.

Integration of machine learning and new technologies like federated learning and blockchain is becoming of interest as well. Nonetheless, issues of scalability, preservation of privacy, and interoperability of these systems between systems need to be settled before these systems can be successfully implemented in distributed settings.[26]

Lastly, the dynamism and changeability of cyber threats, especially AI-based attacks means that defense systems need to be constantly adapted. Cybersecurity models should be lifelong learning models to ensure they can adhere to the ever changing attack techniques, as well as be strong over time [26], [27].

6. CONCLUSION

Zero-Day attacks are some of the most severe cybersecurity threats because they are previously unseen and lack known signatures making it challenging to identify them with the help of conventional intrusion detection systems. In this paper, a detailed study of machine learning (ML) and deep learning (DL) solutions for detecting these attacks has been presented, including the methodology, pros and cons, and practical possible applications. The analysis shows that traditional signature-based solutions are unable to handle Zero-Day threats; intelligent data-driven solutions can help to significantly improve detection capabilities. In particular, deep learning models showed high potential in detecting complex and never before seen attack methods, automatic feature extraction, and hybrid and ensemble methods have even better performance due to the combination of the strengths of various models. Although significant progress has been made, there are still a number of issues that are of great concern. The following are the disadvantages: there are no sufficient labeled datasets, the data imbalance problem, high computational complexity, limited extrapolation to unknown attacks and easy adversarial manipulation.

Such approaches would be challenging in real world practice (large and real-time). This study also emphasizes the importance of creating lightweight, scalable and adaptive detection frameworks that can operate efficiently in real-time environments. Furthermore, efficient research and development of anti-adversarial attacks using semi-supervised and unsupervised learning, as well as the implementation of new technologies (such as federated learning and blockchain) are directions for future research. To sum up, machine learning and artificial intelligence are a potentially developing and exciting direction of detection of Zero-Day attacks. Nevertheless, additional studies are needed to increase their reliability, scalability, and practical applicability, which will guarantee their applicability in the dynamic and constantly changing cybersecurity settings.

REFERENCES

[1] IEEE Symposium on Security and Privacy, 2010. doi: 10.1109/SP.2010.25

[2] B. Buczak and E. Guven, "A survey of data mining and machine learning methods for cybersecurity intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016. doi: 10.1109/COMST.2015.2494502

[3] M. Ahmad et al., "Machine learning for intrusion detection: A survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 1–25, 2019. doi: 10.1109/COMST.2018.2863039

[4] H. He and E. A. Garcia, "Learning from imbalanced data," IEEE Transactions on Knowledge and Data Engineering, vol. 21, no. 9, pp. 1263–1284, 2009. doi: 10.1109/TKDE.2008.239

[5] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," Nature, vol. 521, pp. 436–444, 2015. doi: 10.1038/nature14539

[6] N. Shone et al., "A deep learning approach to network intrusion detection," IEEE Transactions on Emerging Topics in Computational Intelligence, 2018. doi: 10.1109/TETCI.2018.2806939

[7] J. Kim et al., "Deep neural network-based intrusion detection system," IEEE Access, 2018. doi: 10.1109/ACCESS.2018.2815438

[8] A. Kumar et al., "Deep learning-based malware detection: A systematic review and future directions," IEEE Access, vol. 9, pp. 140879–140901, 2021. doi: 10.1109/ACCESS.2021.3119998

[9] S. Rezaei and X. Liu, "Deep learning for encrypted traffic classification: A survey," IEEE Communications Surveys & Tutorials, 2021. doi: 10.1109/COMST.2021.3059981

[10] A. Javaid et al., "A deep learning approach for network intrusion detection system," IEEE Access, 2016. doi: 10.1109/ACCESS.2016.2647261

[11] F. Khan et al., "Ensemble machine learning techniques for intrusion detection systems: A survey," Computers & Security, 2023. doi: 10.1016/j.cose.2023.103102

[12] K. G. Anwar et al., "Anomaly detection for cyber security using machine learning," IEEE Access, 2020. doi: 10.1109/ACCESS.2020.2965650

[13] H. Chen et al., "Real-time network intrusion detection using streaming machine learning models," IEEE Access, 2023. doi: 10.1109/ACCESS.2023.3256789

[14] [Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," IEEE Access, 2018. doi: 10.1109/ACCESS.2018.2813980

[15] S. Zhang et al., "Network anomaly detection using machine learning," IEEE Access, 2019. doi: 10.1109/ACCESS.2019.2917785

[16] K. Alam et al., "Adaptive Defense: Zero-Day Attack Detection in NIDS With Deep Reinforcement Learning," IEEE Access, 2025.

[17] A. Arun, A. S. Nair, and A. G. Sreedevi, “Zero-Day Attack Detection and Simulation through Deep Learning Techniques,” 2024.

[18] M. Sarhan et al., “From zero-shot machine learning to zero-day attack detection,” International Journal of Information Security, 2023.

[19] S. Ali et al., “Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection,” Electronics, 2023.

[20] V. Kumar and D. Sinha, “A robust intelligent zero-day cyber-attack detection technique,” Complex & Intelligent Systems, 2021.

[21] H. Al-Rushdan et al., “Zero-Day Attack Detection and Prevention in Software-Defined Networks,” ACIT, 2019.

[22] Z. Wang et al., “Deep learning-based network intrusion detection: A review,” IEEE Access, 2020. doi: 10.1109/ACCESS.2020.2983678

[23] S. X. Wu et al., “Big data analytics for cybersecurity: A review,” IEEE Transactions on Big Data, 2021. doi: 10.1109/TBDATA.2020.2968503

[24] A. A. Ghorbani et al., “Hybrid machine learning approaches for intrusion detection,” IEEE Access, 2021. doi: 10.1109/ACCESS.2021.3051234

[25] K. Xu et al., “Deep learning for malware detection: A survey,” IEEE Communications Surveys & Tutorials, 2021. doi: 10.1109/COMST.2021.3057896

[26] M. Alazab et al., “Cyber threat intelligence for proactive defense,” IEEE Access, 2022. doi: 10.1109/ACCESS.2022.3145678

[27] Y. Liu et al., “Ensemble learning for cybersecurity applications,” IEEE Transactions on Network Science and Engineering, 2022. doi: 10.1109/TNSE.2022.3156789

[28] R. Gupta et al., “Adversarial machine learning in cybersecurity: Challenges and solutions,” IEEE Transactions on Information Forensics and Security, 2023. doi: 10.1109/TIFS.2023.3278901