International Journal of Advanced Scientific Research and Engineering Trends

ISSN: 2456-0774

Volume 10 Issue 1s (2026) | Pages: 257-265

A Novel Federated Incremental Deep Learning Framework for Zero-Day Cyber Attack Detection

Amit Ratikant Uttarkar[1], Sandeep Vanjale[2]

[1,2]Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India

[1]uttarkar.amit@gmail.com, [2]sbvanjale@bvucoep.edu.in

Peer Review Information

Type: *Article*
Received: *02 April 2026*
Revised: *28 April 2026*
Accepted: *05 June 2026*
Published: *23 June 2026*

Abstract

Zero-day cyber-attacks pose a substantial hazard to modern networked systems due to their unknown signatures and ever-changing attack patterns. The centralized and static learning models that are the mainstay of traditional intrusion detection systems restrict their flexibility, scalability, and adherence to data privacy regulations. This research suggests a novel federated incremental deep learning framework for zero-day cyber-attack detection to overcome these difficulties. Without sharing raw data, the suggested architecture allows remote clients to cooperatively improve a global detection model using federated learning while performing incremental deep learning on locally generated network traffic. The framework successfully manages idea drift and instantly adjusts to new assault patterns by constantly changing model parameters. In comparison to centralized and static federated learning approaches, the suggested framework achieves higher detection accuracy, lower false positive rates, and improved adaptability while guaranteeing data privacy and scalability in distributed environments, according to extensive experiments carried out on benchmark intrusion detection datasets.

Keywords: Zero-Day Attacks; Federated Learning; Incremental Learning; Intrusion Detection Systems; Privacy-Preserving Learning

How to Cite This Article

Uttarkar, A. R., & Vanjale, S. (2026). A novel federated incremental deep learning framework for zero-day cyber attack detection. *International Journal of Advanced Scientific Research and Engineering Trends*, 10(1s), 257–265.

Introduction

Traditional security measures are no longer sufficient to safeguard contemporary networked systems due to the quick development and growing sophistication of cyberattacks. Zero-day attacks, which take advantage of previously undiscovered vulnerabilities for which there are no set rules or signatures, are one of these dangers that present a major difficulty. The capacity of traditional intrusion detection systems and machine learning-based security solutions to identify unknown attacks in real time and adjust to constantly changing threat patterns is constrained by their heavy reliance on centralized data collecting and offline training.[1]

In dispersed environments like cloud computing, the Internet of Things (IoT), edge networks, and large-scale enterprise systems, centralized learning methodologies also raise serious issues with data privacy, scalability, and communication overhead.[2] Due to privacy laws, data ownership concerns, and security dangers, it is frequently impracticable to share raw security data across enterprises or network nodes. Because of this, current centralized and static detection techniques are unable to respond to zero-day attacks in a timely and privacy-preserving manner.

A promising approach that allows distant nodes to collaborate on model training without exchanging raw data is federated learning. Nevertheless, the majority of federated learning-based intrusion detection systems currently in use are not able to gradually learn from continuously entering data streams because they are built for static learning contexts. When faced with concept drift, changing attack behaviors, and real-time zero-day assault scenarios, this weakness leads to model degradation.[3], [4] Furthermore, when exposed to new threats, federated models frequently have delayed adaptation, an increase in false positives, and inadequate detection accuracy.

Concept drift and the need for real-time learning are addressed by incremental learning techniques, which provide the capacity to update models continually without retraining from scratch. Nonetheless, a major research problem continues to be the unified and effective integration of incremental learning with federated infrastructures. A unique, scalable, and adaptive federated incremental learning approach that can guarantee privacy preservation, real-time responsiveness, and robust detection of zero-day assaults across distributed contexts has not been thoroughly investigated in previous research.

Consequently, there is a crucial research need in the design and development of a novel federated incremental learning framework that can identify zero-day attacks in real-time while also addressing issues with data privacy, scalability, flexibility, and detection accuracy. To improve proactive cyber defence mechanisms and provide robust security solutions for contemporary distributed systems, it is imperative to close this gap.[5]Here, this research's main goal is to create a revolutionary federated incremental learning architecture that can identify zero-day cyberattacks. It will be a single, federated incremental deep learning platform that facilitates ongoing, cooperative learning for dispersed environments' zero-day cyberattack detection.

The attack surface of contemporary networks has greatly expanded due to the exponential rise of cloud services, edge computing, Internet of Things (IoT), and networked devices. Zero-day attacks are one of the most hazardous types of cyberthreats because they take use of unidentified vulnerabilities for which there are no signatures or prior awareness.[6]Such attacks are not detectable by traditional signature-based intrusion detection systems (IDS), and anomaly-based systems frequently have high false positive rates. The performance of intrusion detection has been enhanced by recent developments in machine learning and deep learning; nonetheless, most current solutions are not appropriate for real-time zero-day detection since they rely on offline learning and centralized training. Serious issues with data privacy, scalability, and communication cost are also raised by centralized techniques, particularly in dispersed situations where security data exchange is prohibited.[3]

Federated learning (FL), which has lately gained interest in cyber security applications, allows remote clients to collaborate on model training without exchanging raw data. However, most FL-based IDS frameworks do not offer continuous model adaption and instead assume static learning settings.[7] As a result, their performance degrades when confronted with evolving attack patterns and concept drift. This study suggests a federated incremental learning approach for zero-day cyberattack detection in dispersed situations to overcome these drawbacks.

The following is a summary of this paper's primary contributions:

- Incremental Deep Learning for Zero-Day Detection: The detection model may adjust to changing and hitherto unforeseen attack behaviours without having to retrain from scratch thanks to the integration of an incremental deep learning mechanism at client nodes.
- Privacy-Preserving Distributed Learning: By limiting raw network traffic to local clients and distributing only model updates via federated aggregation, the framework protects data privacy.
- Real-Time Adaptability and Concept Drift Handling: In dynamic network situations, real-time detection of zero-day assaults is made possible by ongoing model updates that successfully address concept drift.

- Extensive Experimental Validation: The efficacy of the suggested framework is validated through extensive experiments on standard benchmark datasets, which show superior performance in terms of detection accuracy, false positive rate, and scalability when compared to current state-of-the-art intrusion detection techniques.

The subsequent sections of this article include more pertinent data and a thorough examination of zero-day vulnerability detection techniques. Section III provides a review of the literature on methods for detecting zero-day vulnerabilities. Section IV provides a thorough study and information about zero day attacks; Section V offers new preventative techniques; and Section VI includes a conclusion and future work.

Related work

Most of early intrusion detection systems relied on signatures, which are only useful for known assaults. To identify unexpected threats, anomaly-based intrusion detection systems (IDS) introduced machine learning techniques including Support Vector Machines, Random Forests, and k-Nearest Neighbours. Nevertheless, these models mostly rely on centralized data and offline training.

Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and hybrid architectures are examples of deep learning techniques that have further increased detection accuracy.[8] Nevertheless, their centralized nature limits scalability and violates privacy constraints.

In order to solve data privacy problems, federated learning has recently been investigated for intrusion detection. Current FL-based IDS systems are not appropriate for real-time zero-day detection since they primarily concentrate on static training and periodic aggregation. Although incremental learning approaches deal with concept drift and ongoing learning, they are devoid of collaborative intelligence across dispersed nodes.

To defend networked environments against hostile activity, intrusion detection systems (IDS) have been thoroughly investigated. Signature-based detection, which is only useful for known attack patterns and is unable to identify zero-day cyberattacks, was the mainstay of early intrusion detection systems. Anomaly-based detection methods, which concentrate on spotting departures from typical network behaviours, were developed to get around this restriction. Anomaly-based intrusion detection systems can identify unknown threats; however, they frequently have poor generalization and large false positive rates.

A number of supervised and unsupervised methods, such as Support Vector Machines, Decision Trees, k-Nearest Neighbours, and ensemble models, have been used for intrusion detection thanks to advancements in machine learning. These techniques showed better detection accuracy than conventional techniques, but they are not appropriate for real-time zero-day detection in distributed systems because they usually need offline training and centralized datasets.

Deep learning-based intrusion detection systems have advanced significantly in recent years. To identify intricate attack patterns in network traffic data, models including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM) networks, and hybrid deep learning architectures have been used.[4], [8] Most current systems use centralized training methodologies and static learning procedures, which restrict scalability, adaptability, and compliance with data privacy requirements, even though deep learning approaches improve detection capability.

Federated learning, a decentralized learning paradigm that permits cooperative model training among dispersed nodes without sharing raw data, has emerged to solve privacy concerns. To achieve competitive detection performance while maintaining data confidentiality, several studies have investigated federated learning for intrusion detection. However, current federated intrusion detection frameworks are limited in their capacity to adapt to changing zero-day assault patterns and idea drift since they primarily rely on fixed data distributions and periodic batch training.

To allow models to learn continuously from streaming data, incremental and continuous learning strategies have been developed. These techniques work well for managing concept drift and adjusting to changing surroundings without requiring complete retraining. However, the majority of incremental learning strategies are created in isolated or centralized environments and do not take use of distributed systems' collaborative intelligence.[9]

Federated learning and incremental deep learning have mostly been investigated separately in the context of intrusion detection, according to a thorough analysis of the body of extant literature. Insufficient research has been done on integrating incremental deep learning into federated infrastructures for real-time zero-day cyberattack detection. Additionally, creating scalable, privacy-preserving frameworks that can continuously adjust to new attack behaviours has received less attention. In order to enable real-time zero-day cyber-attack detection while maintaining data privacy and scalability in distributed environments, this work suggests a novel federated incremental deep learning framework that combines decentralized training with ongoing model adaptation.

Literature Review

Zero-day attacks take advantage of undiscovered flaws in hardware, software, or network systems before security teams or developers can produce detection signatures or patches. The phrase "zero-day" describes how these attacks are more deadly and challenging to detect since defenders have zero days to prepare for them. Zero-day attacks have become a major issue for enterprises in many industries, from critical infrastructure to healthcare systems, as cyber threats continue to increase in sophistication and frequency.[1]Beyond technological difficulties, zero-day assault detection is important because it has significant social and economic ramifications. Long-term network compromise due to zero-day vulnerabilities can result in data breaches, service interruptions, and large financial losses.[10]

Detection Techniques: A Taxonomy

Signature-Based Detection:

By comparing observed patterns to databases of known attack signatures, signature-based detection embodies the conventional approach in intrusion detection. Signature-based techniques are essentially limited in their capacity to identify zero-day attacks, despite being quite successful in identifying known threats with low false positive rates. By definition, zero-day vulnerabilities lack the prior knowledge of attack patterns that these systems require.

Hybrid approaches that combine complimentary methodologies for detecting novel attacks with signature-based detection for known threats have been investigated recently. To achieve 98% detection accuracy while lowering false positive rates by roughly 70%, Kumar et al. suggested a hybrid framework that combined signature-based detection with anomaly-based techniques and LSTM models.[11]. This method uses machine learning-based anomaly detection to overcome the core vulnerability of signature-based detection against zero-day attacks while leveraging its advantages for known threats.

The literature has extensively documented the shortcomings of signature-based detection for zero-day attacks. According to Rafy et al., because signature-based detection algorithms require prior knowledge of established attack strategies, they are unable to find unexpected vulnerabilities. In a similar vein, Gowthami et al. stress that conventional intrusion prevention systems that depend on signature-based detection techniques typically fall short of identifying new attacks.[12] The research community has turned to alternate detection paradigms, including anomaly-based and machine learning techniques, because of these basic constraints.[13]

Anomaly-Based Detection:

A paradigm change from matching established patterns to spotting departures from typical behaviours is represented by anomaly-based detection. Because it may be able to detect new threats without prior knowledge of particular attack signatures, this method is especially well-suited for zero-day attack detection. Anomaly detection techniques simulate typical network or system behaviours and identify notable anomalies as possible threats.[14], [15]

Zoppi et al. reviewed clustering, density-based, classification (e.g., One-Class SVM), statistical, angle-based, neighbour-based, and neural network techniques in their thorough investigation of unsupervised algorithms for zero-day attack detection [24]. Their study showed that good detection performance can be attained by unsupervised anomaly detection algorithms, especially those that use meta-learning like Boosting (COF). Boosting (COF) greatly outperformed standard unsupervised algorithms using the SDN20 dataset, achieving precision of 0.997, recall of 0.994, F2-Score of 0.995, and Matthews Correlation Coefficient (MCC) of 0.986.

Machine Learning Approaches

Jonnalagadda et al. evaluated Support Vector Machines, Random Forest, K-Nearest Neighbours, Decision Trees, and Extreme Gradient Boosting in addition to deep learning models in a comparative study of machine learning and deep learning approaches for zero-day vulnerability identification.[16] They discovered that machine learning models often perform better than deep learning models in terms of detection accuracy and lowering false positive rates using the CIC-IDS-2017 and CIC-TON-IOT datasets. A hybrid strategy that combined the two paradigms reduced false positives and improved detection accuracy even more. Using a hybrid ensemble strategy that combined Random Forest with Gradient Boosting and SVM classifiers via weighted voting, Ahmed et al. achieved 97.8% detection accuracy on the UNSW-NB15 dataset.[17] For machine learning-based detection to be effective, feature engineering and selection are essential. The model's performance is greatly impacted by the characteristics selected, and redundant or unnecessary features may reduce detection accuracy. Packet length, inter-arrival time, flow duration, protocol metadata, and statistical aggregations are examples of network traffic characteristics that offer extensive information for differentiating benign from malevolent behaviours.[18] However, features like IP addresses may be redundant for detecting zero-day attacks and can negatively impact model performance. [19]

Deep Learning Techniques

With its capacity to autonomously build hierarchical feature representations from raw data without requiring significant manual feature engineering, deep learning has become a potent paradigm for zero-day attack detection. Convolutional neural networks (CNNs), recurrent

neural networks (RNNs), autoencoders, and other neural network architectures have shown remarkable performance in identifying new assaults [19]

Autoencoders:
One of the most popular deep learning architectures for detecting zero-day attacks is autoencoders. These neural networks are trained to reconstitute the original input after compressing it into a lower-dimensional latent representation. Autoencoders trained on normal data will reconstruct normal samples with little error, but they will create substantial reconstruction error for anomalous inputs, such as zero-day attacks. This is a crucial discovery for anomaly identification.[20].

In order to detect zero-day attacks, Hindy et al. suggested an autoencoder implementation that achieved detection accuracy of 89-99% on the NSL-KDD dataset and 75-98% on the CICIDS2017 dataset[20]. The study showed that autoencoders' encoding-decoding capabilities make them ideal for identifying sophisticated zero-day assaults. The autoencoder technique demonstrated better performance for complicated attack patterns while retaining acceptable false negative rates when compared to One-Class SVM.[21], [22]

Convolutional Neural Networks:
Originally created for image processing, Convolutional Neural Networks (CNNs) have been effectively modified for intrusion detection and network traffic analysis. When properly organized, CNNs are useful for analysing structured network traffic data because they are excellent at extracting spatial patterns and local features.[23] Using the UNSW-NB15 dataset, Nandiraju et al. showed how CNNs may be used to detect zero-day attacks in network traffic with 93.8% accuracy[24]. When it came to identifying intricate patterns in network traffic data, the CNN model fared better than the Random Forest and Support Vector Machine baselines. The model demonstrated its efficacy in learning, generalizing, and preserving robustness without overfitting with 95.1% precision, 93.8% accuracy, 96.5% recall, and 94.6% F1-score[6]

Recurrent Neural Networks:
For the analysis of sequential data, such as network traffic patterns, Recurrent Neural Networks (RNNs) and their sophisticated variations, Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU), are especially well-suited. By keeping an internal state that records temporal dependencies, these architectures make it possible to identify attack patterns that develop over time.[25].[26]

For zero-day exploit detection, Ahmed et al. created a hybrid AI-driven solution that combines ensemble techniques with CNNs and LSTM networks.[27], [28] On the UNSW-NB15 dataset, the combination of CNN for spatial feature extraction and LSTM for temporal pattern recognition produced a detection accuracy of 97.8% with a low false positive rate of 0.022.

Federated and Distributed Approaches:
Federated learning approaches enable collaborative threat detection across multiple networks while preserving privacy. Ohtani et al. proposed IDAC, a federated learning-based intrusion detection method using autonomously extracted anomalies in IoT environments[29]. The method autonomously extracts attack candidates from network traffic and aggregates similar candidates from multiple networks to determine attacks. IDAC demonstrated comparable detection performance against multiple attacks, including zero-day attacks, while successfully suppressing false positives during the extraction of attack candidates.[30]

Federated learning addresses several challenges in zero-day detection: data scarcity (by leveraging data from multiple sources), privacy concerns (by keeping data localized), and model generalization (by training on diverse network environments). However, challenges remain in autonomous labelling of attacks from traffic and sharing attack information between different device types[29].

Proposed Methodology

System Overview
To detect zero-day cyberattacks in dispersed network environments in real-time, the suggested methodology presents a Federated Incremental Deep Learning (FIDL) framework. The system is made up of a core federated server and several decentralized client nodes.[31] While the server manages global model aggregation without accessing raw data, each client individually keeps an eye on local network traffic and carries out incremental deep learning.

An incremental deep learning model based on locally observed network traffic is deployed by each client node.

The model may gradually update its parameters without having to retrain from scratch because incoming data streams are analysed in mini-batches.
Important traits:

- Constant adjustment to changing traffic patterns
- The ability to pick up attack behaviours that have never been observed before
- A decrease in computational overhead

This incremental learning strategy effectively addresses concept drift, which is common in real-world network environments.

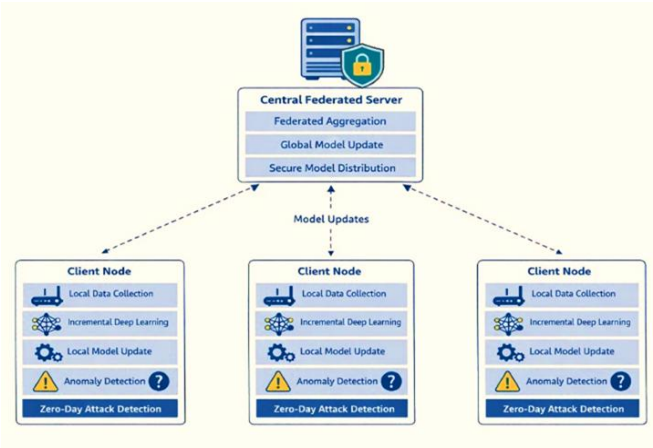

Fig. 1. *Proposed federated incremental deep learning framework*

The architecture is divided into the following sections:

1. Central Federated Server: This serves as the federated learning process's worldwide coordinator. Among its duties are:
2. Federated Aggregation: merging model updates from different client nodes.
3. Global Model Update: Using the combined data, a new, enhanced global model is created.
4. Secure Model Distribution: Returning the modified global model to the client nodes in a secure manner.
5. Client Nodes: These are local entities that store and process data locally while maintaining privacy, such as edge devices and local networks.

Each client node performs the following tasks:

1. Local Data Collection: Gathering raw information about network traffic or activity.
2. Incremental Deep Learning: Using fresh data as it becomes available, the local model is continuously trained.
3. Local Model Update: Using newly discovered patterns to improve the local model.
4. Anomaly Detection: Recognizing unusual network activity that departs from the established typical patterns.
5. Zero-Day Attack Detection: Specifically flagging the anomalies as potential novel (zero-day) attacks that were previously unknown.

Client nodes send updated model parameters to the federated server on a regular basis rather than exchanging raw data. To create a global model, the server uses secure federated aggregation, usually with weighted averaging.

To facilitate collaborative intelligence while maintaining data privacy, the aggregated global model is redistributed to clients. This procedure guarantees robustness across various data distributions while reducing communication overhead.

The process consists of an ongoing cycle:

1. Client nodes gather local data and identify anomalies using incremental deep learning.
2. The central server receives model updates—that is, learnt parameters rather than raw data—securely.
3. To improve the global model, the central server compiles these updates.
4. All client nodes receive the updated global model securely, enhancing each node's capacity to detect new threats in real time.

By centralizing raw data, this decentralized method protects user privacy while enabling the system to effectively respond to novel, unidentified (zero-day) threats. Finding abnormal behaviours that drastically depart from learned normal patterns is how zero-day detection is accomplished. Real-time detection of unknown assaults is made possible by the incremental deep learning model's constant updating of its decision limits. The framework reduces false positives while maintaining high detection accuracy by combining incremental adaptation with federated learning.

Let Us See How it works:
Input
Distributed client set: $C=\{C1,C2,\ldots,C_N\}$

- Streaming local network traffic data at each client
- Initial global model parameters: θ^0
- Learning rate: η

- Communication round index: t

Output

- Converged global model θ^*capable of detecting zero-day cyber attacks

Global Initialization: The federated server initializes the global deep learning model with parameters θ^0

Model Distribution: The server securely broadcasts the global model θ^t to all participating client nodes $C_i \in C$

Local Incremental Training (Client-Side):

For each client Ci (executed in parallel):

1. Receive the global model θ^t
2. Continuously collect local network traffic data streams.
3. Incrementally update local model parameters using mini-batch learning:

$$\theta it + 1 = \theta t - \eta \nabla L(\theta t, Di)$$

where Di denotes local data at client Ci.

Perform local anomaly and zero-day attack detection using the updated model. Transmit updated model parameters θ t+1 to the federated server.

Federated Aggregation (Server-Side): The server aggregates local updates received from all clients using weighted averaging:

$$\theta^{t+1} = \sum_{i=1}^{N} \frac{|D_i|}{\sum_{j=1}^{N} |D_j|} \theta_i^{t+1}$$

Global Model Update: The aggregated parameters θ^{t+1}form the updated global model.

Iteration: Steps second to five are repeated for multiple communication rounds until convergence criteria are satisfied (e.g., stabilization of detection accuracy or loss).

Termination: Output the final global model $\theta* = \theta^{t+1}$ for real-time zero-day attack detection.

Experimental Results and Discussion

Standard intrusion detection criteria, such as detection accuracy, precision, recall, F1-score, and false positive rate, are used to assess the effectiveness of the suggested framework. To evaluate scalability, convergence behavior and communication overhead are also examined. The suggested framework consistently outperforms static federated learning and centralized deep learning techniques, according on experimental data. Faster adaptability to new attack patterns is made possible by incremental learning, which improves recall and detection accuracy for zero-day attacks. Incremental learning considerably lessens idea drift-induced model degradation. In contrast to static models, which lose accuracy under changing attack circumstances, the framework sustains steady performance over time. The suggested architecture scales effectively as the number of participating clients rises, according to the results. Privacy hazards are reduced but competitive detection performance is maintained since raw data is never shared. Even though deep learning-based intrusion detection has been thoroughly studied, current methods mostly rely on centralized or static learning algorithms.

Although federated learning has been suggested as a solution to privacy issues, existing federated intrusion detection methods presume fixed data distributions and lack ongoing flexibility. Despite their effectiveness in managing concept drift, incremental learning approaches are rarely used into federated systems for cyber security applications. Their suitability for real-time zero-day attack detection in distributed environments is limited by this division.

Conclusion

By presenting a novel federated incremental deep learning architecture that combines decentralized learning, continuous adaptation, and privacy preservation, the proposed study fills this crucial gap. The suggested architecture is a major improvement over current state-of-the-art systems since, in contrast to earlier research, it simultaneously provides real-time responsiveness, scalability, and robustness against until undiscovered cyber-attacks.

References

1. A. R. Uttarkar, S. Vanjale, and P. Rajpoot, “A Comprehensive Review and Novel Approach for Detection of Zero Day Vulnerabilities,” in 2024 IEEE Pune Section International Conference, PuneCon 2024, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/PuneCon63413.2024.10894962.
2. J. Zhang, S. Liang, F. Ye, R. Q. Hu, and Y. Qian, “Towards Detection of Zero-Day Botnet Attack in IoT Networks Using Federated Learning,” in IEEE International Conference on Communications, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 7–12. doi: 10.1109/ICC45041.2023.10279423.

3. Abdelaziz Amara korba and Sidi Mohammed Senouci, “Federated Learning for Zero-Day Attack Detection in 5G and Beyond V2X Networks.”
4. R. Uttarkar and S. Vanjale, “A Novel Convolutional-Sequential XGB Neural Model for Zero-Day Attack Detection in Federated Learning,” in 2025 World Skills Conference on Universal Data Analytics and Sciences, WorldSUAS 2025, Institute of Electrical and Electronics Engineers Inc., 2025. doi: 10.1109/WorldSUAS66815.2025.11199174.
5. Y. Guo, “A Review of Machine Learning-Based Zero-Day Attack Detection: Challenges and Future Directions,” 2022. Available: https://www.sciencedirect.com/science/article/pii/S0140366422004248
6. U. Amit Ratikant, H. H. A, P. student JSCOE, P. Associate Professor, and J. Pune, “SNPDAC: Secure Network Protocol with Data Access Controlling in WSN,” 2012. Available: www.ijsr.net
7. R. Doriguzzi-Corin and D. Siracusa, “FLAD: Adaptive Federated Learning for DDoS attack detection,” Comput. Secur., vol. 137, Feb. 2024, doi: 10.1016/j.cose.2023.103597.
8. S. Thongsuwan, S. Jaiyen, A. Padcharoen, and P. Agarwal, “ConvXGB: A new deep learning model for classification problems based on CNN and XGBoost,” Nuclear Engineering and Technology, vol. 53, no. 2, pp. 522–531, Feb. 2021. doi: 10.1016/j.net.2020.04.008.
9. M. Sarhan, S. Layeghy, M. Gallagher, and M. Portmann, “From zero-shot machine learning to zero-day attack detection,” Int. J. Inf. Secur., vol. 22, no. 4, pp. 947–959, Aug. 2023. doi: 10.1007/s10207-023-00676-0.
10. Uttarkar, S. G. Pathak, A. Kamble, H. Lokhande, A. Dhore, and R. Patil, “AI Revolution in CAD: Pioneering the Future of Design,” in Lecture Notes in Networks and Systems, Springer Science and Business Media Deutschland GmbH, 2026, pp. 1–12. doi: 10.1007/978-3-032-06694-7_1.
11. Kumar et al., “Next-Generation Intrusion Detection Systems: A Hybrid Machine Learning Framework for Intelligent Cyber Threat Neutralization,” Jan. 08, 2025. doi: 10.21203/rs.3.rs-5762323/v1.
12. AL Rafy, Md Mashfiquer Rahman, Sharmin Nahar, Md. Najmul Gony, and MD Imranul Hoque Bhuiyan, “The role of machine learning in predicting zero-day vulnerabilities,” International Journal of Science and Research Archive, vol. 10, no. 1, pp. 1197–1208, Oct. 2023. doi: 10.30574/ijsra.2023.10.1.0838.
13. M. Sayduzzaman, J. T. Tamanna, and T. Rahman, “Interoperability and Explicable AI-based Zero-Day Attacks Detection Process in Smart Community Zero-Day Attacks Detection in Smart Community through Interoperability and Explainable AI.” Available: https://www.researchgate.net/publication/382913807
14. J. F. Cevallos M., A. Rizzardi, S. Sicari, and A. C. Porisini, “NERO: Neural algorithmic reasoning for zero-day attack detection in the IoT: A hybrid approach,” Comput. Secur., vol. 142, Jul. 2024. doi: 10.1016/j.cose.2024.103898.
15. P. Verma, N. Bharot, J. G. Breslin, D. O’shea, A. Vidyarthi, and D. Gupta, “Zero-Day Guardian: A Dual Model Enabled Federated Learning Framework for Handling Zero-Day Attacks in 5G Enabled IIoT,” IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 3856–3866, Feb. 2024. doi: 10.1109/TCE.2023.3335385.
16. M. Roopak, S. Parkinson, G. Y. Tian, Y. Ran, S. Khan, and B. Chandrasekaran, “An unsupervised approach for the detection of zero-day distributed denial of service attacks in Internet of Things networks,” IET Networks, vol. 13, no. 5–6, pp. 513–527, Sep. 2024. doi: 10.1049/ntw2.12134.
17. H. I. E. Tariq, M. B. I. E. Tariq, and S. Lu, “Hybrid AI-Driven Techniques for Enhancing Zero-Day Exploit Detection in Intrusion Detection System (IDS),” in 2024 3rd International Conference on Artificial Intelligence, Internet of Things and Cloud Computing Technology, AIoTC 2024, IEEE, 2024, pp. 156–160. doi: 10.1109/AIoTC63215.2024.10748333.
18. S. Sattar et al., “Anomaly detection in encrypted network traffic using self-supervised learning,” Sci. Rep., vol. 15, no. 1, Dec. 2025. doi: 10.1038/s41598-025-08568-0.
19. G. Kang, “Artificial Intelligence for Threat Detection: Leveraging Deep Learning to Identify Zero-Day Attacks in Real Time,” Universal Library of Engineering Technology, vol. 02, no. 04, pp. 74–79, Dec. 2025. doi: 10.70315/uloap.ulete.2025.0204013.
20. H. Hindy, R. Atkinson, C. Tachtatzis, J. N. Colin, E. Bayne, and X. Bellekens, “Utilising deep learning techniques for effective zero-day attack detection,” Electronics (Switzerland), vol. 9, no. 10, pp. 1–16, Oct. 2020. doi: 10.3390/electronics9101684.
21. N. Chowdhury and M. A. Kashem, “A comparative analysis of Feed-forward Neural network & Recurrent Neural network to detect intrusion,” in ICECE 2008, pp. 488–492. doi: 10.1109/ICECE.2008.4769258.
22. S. R. Wategaonkar et al., “Targeting Insider Threats and Zero-Day Vulnerabilities with Advanced Machine Learning and Behavioral Analytics,” ICIPTM 2024. doi: 10.1109/ICIPTM59628.2024.10563816.
23. T. T. Thein, Y. Shiraishi, and M. Morii, “Personalized federated learning-based intrusion detection system: Poisoning attack and defense,” Future Generation Computer Systems, vol. 153, pp. 182–192, 2024. doi: 10.1016/j.future.2023.10.005.
24. Z. Dai et al., “An intrusion detection model to detect zero-day attacks in unseen data using machine learning,” PLoS One, vol. 19, no. 9, 2024. doi: 10.1371/journal.pone.0308469.

25. P. R. Agbedanu et al., “A scalable approach to IoT and IIoT security using adaptive KNN for zero-day attack detection,” Sensors, vol. 25, no. 1, 2025. doi: 10.3390/s25010216.
26. Mbona and J. H. P. Eloff, “Detecting Zero-Day Intrusion Attacks Using Semi-Supervised Machine Learning Approaches,” IEEE Access, vol. 10, 2022. doi: 10.1109/ACCESS.2022.3187116.
27. A. Mohamed et al., “Zero-day exploit detection with adaptive WavePCA-Autoencoder (AWPA),” Sci. Rep., vol. 15, no. 1, 2025. doi: 10.1038/s41598-025-87615-2.
28. T. Ohtani, R. Yamamoto, and S. Ohzahata, “IDAC: Federated Learning-Based Intrusion Detection Using Autonomously Extracted Anomalies in IoT,” Sensors, vol. 24, no. 10, 2024. doi: 10.3390/s24103218.
29. Z. Mu, X. Shi, and S. Dogan, “Information System Security Reinforcement with WGAN-GP for Detection of Zero-Day Attacks,” ICAIBD 2024. doi: 10.1109/ICAIBD62003.2024.10604482.
30. M. Sayduzzaman, A. Rahman, J. T. Tamanna, D. Kundu, and T. Rahman, “Interoperability and Explicable AI-based Zero-Day Attacks Detection Process in Smart Community,” arXiv:2408.02921.