2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence) | 979-8-3503-4483-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/CONFLUENCE60223.2024.10463429

Zero Day Attack Detection and Simulation through Deep Learning Techniques

Aalap Arun
Department of Computer Science and Engineering
Amrita School of Computing
Amrita Vishwa Vidhyapeetam,
Chennai,India
aalap.arun@gmail.com

Anjaly S Nair
Department of Computer Science and Engineering
Amrita School of Computing
Amrita Vishwa Vidhyapeetam,
Chennai, India
sn.anjaly@gmail.com

Sreedevi A. G.*
Department of Computer Science and Engineering
Amrita School of Computing
Amrita Vishwa Vidhyapeetam,
Chennai,India
ag_sreedevi@gmail.com

***Abstract*— Combating zero-day attacks is essential in the age of ongoing cyber threats. For simulating and identifying these dangers, our research uses Long Short-Term Memory (LSTM) algorithms, which are skilled at collecting temporal data correlations. This novel method signals a paradigm shift in cybersecurity. The project begins by developing a complex framework to model intricate zero-day attacks that imitate previously undiscovered vulnerabilities. Our detection method uses recurrent neural networks and sophisticated gating techniques, and it is LSTM-based. Its capacity to recognize novel assault patterns and pinpoint minute departures from the usual is demonstrated by rigorous testing. The result is a powerful zero-day attack detection system that improves accuracy and responsiveness. This reduces the potential damage that unknown vulnerabilities could inflict.**

Keywords*— Deep Learning, Zero Day Attacks, Long Short-Term Memory, Anomaly Detection, Vulnerability Detection.

I. INTRODUCTION

An era marked by the development of interconnected systems and networks has been ushered in by the modern digital landscape, offering an ideal environment for both innovation and exploitation. Cyber dangers and vulnerabilities have also increased exponentially in this time period, highlighting the urgent need for effective cybersecurity solutions. Zero-day attacks stand out among these dangers as a particularly cunning threat that presents a significant threat to the safety of both software and hardware systems. The idea that there are "zero days" of protection available to potential targets at the time of the attack gives zero day attacks its name. Zero-day vulnerabilities are still unknown, in contrast to known vulnerabilities, which have been found and may be handled by security patches or mitigations. Due to these stealthy attacks, conventional signature-based detection techniques that depend on identifying well-known patterns and behaviors become useless. Zero-day vulnerabilities are hidden from developers, security professionals, and even the companies managing the impacted systems. Without the usual defences and precautions in place, this hidden nature enables malevolent actors to plan stealthy and potentially destructive strikes. Such attacks can have devastating effects, resulting in everything from financial losses and data breaches to the compromise of vital infrastructure and, in some situations, even risks to national security. Therefore, it is critically important to strengthen our cybersecurity defences against the elusive and unpredictable threat of zero-day attacks in this dynamic digital environment where innovation and connectivity are in abundance.

Traditional security systems are very good at identifying previously observed patterns and behaviours. The work done by Mbona et.al[1] provides information about identifying zero-day attacks with a focus on machine learning techniques that are semi-supervised. However, these systems fail when exposed to zero-day attacks, which by definition operates in the uncharted territory.

A best analogy for explaining the scenario is finding a needle in a haystack. This is an accurate analogy for how difficult it is to detect zero-day attacks in real-time. By design, these attacks show no previous patterns or recognized signatures, making conventional security systems unaware of their existence. The paper by Saher et. al. [2] focuses on addressing access control challenges within the Internet of Things (IoT). The attackers can get access to such networks, carry out malicious operations, and exfiltrate data without being detected or setting off alarms. The enormous volume of digital activity and the intricacy of these attacks make it more challenging to make a timely identification. It is like to trying to find a minuscule thing in a vast, exponentially expanding digital haystack.

Sotani et. al.[3] have proposed an adaptable deep learning based intrusion detection system to detect zero day attack. Alok Kumar Shukla[4] in his work proposed a hybrid evolutionary approach for identification of zero day attacks on wired/wireless network system. LSTM techniques must be able to identify harmful actions that depart from well-established patterns and behaviours, displaying a degree of adaptability and foresight unequalled by traditional security systems.

This research tries to address the critical issue of zero-day attack detection by exploiting the capabilities of Long-Short Term Memory (LSTM) algorithms, a subset of deep learning approaches. We want to develop a proactive security system that can spot these sneaky attacks in real-time by teaching LSTM models to spot departures from accepted norms and behavioural patterns. A study by Asifullah Khan et. al.[5] explores the effectiveness of Zero-shot Learning (ZSL) strategies using a novel Deep Contractive Autoencoder-based Attribute Learning (DCAE-ZSL) approach to counteract zero-day ransomware attacks.

This study seeks to create a novel approach to counter these risks by simulating and detecting zero-day attacks through the use of deep learning, specifically Long Short-Term Memory (LSTM) algorithms. By allowing systems to adapt and learn from data, this strategy aims to go beyond reactive responses and provide a proactive defense against these constantly changing threats.

Fig[1] shows the changing environment of cyber threats and vulnerabilities in the digital realm throughout the selected time. The timeline shown in fig[1], which runs through 2023, shows a clear increase trend in the number of cyberthreats and vulnerabilities. Each data point on the graph represents a situation, weakness, or threat identified over the time, with the points increasing in value over time.

Fig[1] also shows an evident increase in the complexity and variety of threats as the timeframe goes on. The various sizes, colors, and forms of the data points serve as a representation of this complexity. The expanding tactics and strategies used by cyber adversaries are reflected in the growing complexity of threats, making it even harder to identify zero-day attacks using conventional methods. The performance of conventional security systems is either largely stagnant or grows more slowly while the threat trendline climbs sharply. The inherent limitations of reactive security strategies are highlighted by this disparity, especially when faced with zero-day attacks, which thrive on taking advantage of the unknowable Fig.[1] offers important context for the study concerned with LSTM-based zero-day attack detection. It underlines the need for a change to proactive and flexible security measures due to the current threat scenario. The use of deep learning methods, as illustrated by the LSTM algorithm, is a direct reaction to the growing demand for better ways to recognize and defend against zero-day attacks, as seen by the upward trend in the graph.

The rest of the paper is organized as follows: Section II discusses related previous studies. Section III contains descriptions of all datasets used in this study. Section IV contains description about the proposed model that has the dynamic architecture description and further details on the ML model. Section V describes the algorithm used for the model and explains all the steps performed for the study. Section VI contains the results and discussion of this study. Section VII concludes the study.

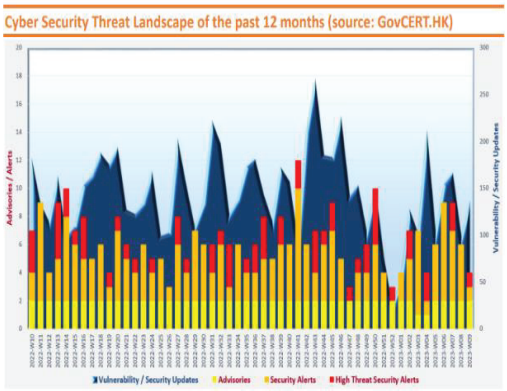

Fig.1. Cyber Security Threat landscape of the past 12 months

II. Related Works

A thorough analysis of various approaches to zero-day attack detection demonstrates the effectiveness of different machine learning strategies and their unique approaches to tackling this pressing cybersecurity issue. The study[6] examines several machine learning algorithms for intrusion detection, with a focus on deep learning, autoencoders, and support vector machines (SVMs). It presents a sophisticated methodology created especially for modeling and identifying these elusive threats and provides insights into zero-day vulnerabilities. In contrast, the LSTM-based study focuses on zero-day threats and demonstrates how LSTM algorithms can detect and mitigate these intricate vulnerabilities through rigorous testing. By proactively detecting anomalies and unidentified attacks, both strategies aim to strengthen cybersecurity defenses against dynamic threats.

In the meantime, Sameera and Shashi[7] present Deep Transductive Transfer Learning (DTTL), which creates soft labels for target instances by using cluster correspondence. This technique transfers knowledge from labeled source domains to unlabeled target domains by using a DNN classifier and taking advantage of domain correlation. By aligning domains and taking advantage of correlations, this strategy transfers knowledge to detect zero-day attacks, whereas LSTM-based techniques are superior at identifying temporal patterns in network traffic data.

Zafer et al.[8] suggest a novel approach for anomaly detection in Software-Defined Networks (SDNs) that combines Long Short-Term Memory (LSTM) algorithms with Convolutional Neural Networks (CNN). Their hybrid model shows enhanced ability to detect zero-day attacks by extracting both temporal and spatial features from network traffic data. The research highlights the benefits of merging CNN and LSTM architectures, demonstrating notable enhancements in SDN anomaly detection[9].

Guo et al. [10]also highlight the capacity of LSTM networks to process sequential data for more complex detection while comparing different ML models for zero-day detection. Zhang et al.[11], in contrast, concentrate on creating a formal metric to evaluate the resilience and attack surface of networks. LSTM-based techniques focus on historical data to forecast future attacks, prioritizing the use of deep learning to find patterns in network traffic. By merging behavioral anomalies and structural weaknesses, the combination of the two strategies could strengthen network security.

In order to overcome the lack of labeled data, the PlausMal-GAN[12]framework concentrates on realistically generating zero-day malware instances, whereas LSTM-based strategies prioritize sequential learning and historical pattern analysis. In contrast to LSTM-based techniques that use recurrent neural networks—more specifically, LSTM models—for anomaly detection in network traffic data, Zoppi et al. [13]investigate unsupervised algorithms for zero-day attack detection.

Agathe Blaise et al.[9] use real-time traffic analysis and unsupervised learning techniques to focus on feature evolution and joint analysis for attack detection. By using recurrent neural networks, LSTM-based models, on the other hand, place more emphasis on learning temporal dependencies within sequential data to detect zero-day attacks. The work done by Vaishnavi Konde et al.[14] aligns with efforts to enhance the effectiveness of intrusion detection systems (IDSs) against hitherto unknown threats,

particularly zero-day attacks, while also focusing on mitigating false positives.

Ashok Kumar Mohan et al.[15] has studied in detail about the vulnerability assessment and penetration testing method for wireless security auditing to find and fix known vulnerabilities in a network's defenses. Another study by Akarsh et al.[16] introduces a malware classification framework that utilizes CNN and LSTM architectures with hyperparameter tuning and a 70-30% train-test split to handle imbalanced datasets.

The study by Zhou et al.[17] explores the machine learning models for zero-day attack detection while Fahd Alhaidari et al.[18] introduces the ZeVigilante system uses machine learning techniques like Random Forest, Neural Networks, Decision Tree, k-Nearest Neighbor, Naïve Bayes, and Support Vector Machine in a sandbox setting.

When taken as a whole, these studies highlight the complex terrain of zero-day attack detection, highlighting the potential of hybrid architectures, LSTM-based models, unsupervised algorithms, and creative approaches to strengthen cybersecurity defenses against new threats.

III. DATASETS

For the evaluation of the suggested models, two popular IDS datasets are used. The CICIDS2017[19] dataset, created by the Canadian Institute for Cybersecurity (CIC), is the first. A wide variety of current insider and outer attacks are covered by the CICIDS2017 dataset. Finally, it is offered in a raw format, giving researchers the freedom to process the dataset anyway they see fit. It includes a diverse coverage of protocols and attacking variations. The CICIDS2017 dataset is therefore a good choice for testing the suggested models.

The five consecutive days of traffic from benign, insider, and external attacks are captured in the CICIDS2017 dataset. The PCAP recordings are made available. The NSL-KDD is the second dataset. The CIC released NSL-KDD in order to fix the issues with the KDD Cup'99 dataset. The dataset of choice for evaluating more than 50% of IDS from the last ten years was the KDD Cup'99 dataset, which was followed by the NSL-KDD dataset, which was utilized for evaluating more than 17% of IDS. These issues include redundant records and a disparity in class sizes.

The NSL-KDD dataset includes both normal/harmless traffic as well as four types of cyberattacks: DoS, probing, Remote to Local (R2L), and User to Root (U2R). 'KDDTrain+.csv' and 'KDDTest+.csv' are two files that include the NSL-KDD dataset. The NSL-KDD dataset is offered in comma separated value (csv) feature files, just like the KDD Cup'99. The class label and each instance's feature values are displayed together. To be suitable for ML usage, the feature files go through categorical features encoding.

IV. PROPOSED MODEL

The paper proposes a model called Dynamic LSTM-based Anomaly Detection (DLAD) for Zero-Day Attack Detection. DLAD is intended to address the shortcomings of conventional intrusion detection systems (IDS) by integrating dynamic long short-term memory networks (LSTM networks) to analyze network traffic in real-time. The primary innovation is the dynamic adaptation of LSTM states to changing network behaviors, which enables more accurate zero-day attack detection[20].

Dynamic LSTM Architecture: Our DLAD model uses a dynamic LSTM architecture, as opposed to static LSTM networks. Because of this design, the model can dynamically modify its internal states and parameters in response to the stream of input data. DLAD can detect minute variations and adjust to shifting network traffic patterns thanks to the dynamic nature of LSTM neurons.

A. Feature Selection and Extraction: To select the most pertinent network traffic attributes, such as packet size, inter-arrival times, and protocol details, DLAD uses feature selection algorithms. Sequences of these features are fed into the dynamic LSTM network.

B. Unsupervised Learning: Because DLAD functions in an unsupervised learning mode, it is especially useful for detecting zero-day attacks. It becomes skilled at recognizing new attacks because it learns the network's typical behavior without having any prior knowledge of attack patterns.

C. Dynamic State Update Mechanism: The dynamic state update mechanism is the main innovation of DLAD. The internal states of DLAD are constantly updated in response to incoming data, in contrast to traditional LSTM models that have fixed internal states. As a result, it can recognize long-term dependencies and adjust to changing network conditions.

V. ALGORITHM

The complex process of identifying zero-day and real-time attacks is depicted in the diagram. Before training the model, the raw data is first sent to a data preprocessing module for extensive cleaning and preparation. The model is generated and trained during the training phase in the training module. The model is used to predict attacks in real time after it has been trained. Performance metrics are used to gauge how accurate these predictions are, and the model is adjusted accordingly. The zero-day attack detection module uses machine learning techniques in addition to known known signatures to counter newly emerging, unknown attacks. Its ability to effectively identify and stop any possible unknown attacks is vital.

During the Real-Time Data Transmission, as shown in fig[2] the attack detection model receives real-time data streams continuously. Numerous parameters are included in this data, including system logs, network traffic, and any other pertinent data sources that might point to possible security risks. The implemented attack detection model is capable of identifying zero-day attacks, which means that it's made to find new or undiscovered threats that traditional signature-based systems might overlook. This model most likely uses deep neural networks or machine learning algorithms that have been trained to identify patterns suggestive of intrusions.

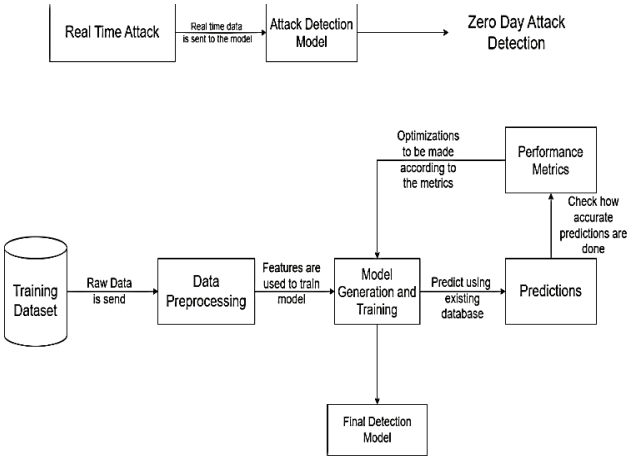

Fig.2. Proposed Algorithm Design

Initially the training dataset's raw data is sent for preprocessing, as shown in fig[2]. The data is cleaned, normalized, and converted into features that the model can use for training during preprocessing. The model's performance is assessed using performance metrics like accuracy, precision, recall, and F1-score. The detection model is created and trained using the preprocessed data, which contains the chosen features. The model will be trained using unsupervised learning techniques. The model picks up traits and patterns of typical behavior as opposed to possible attack patterns.

The model is optimized iteratively based on performance metrics. Real-time predictions are made on incoming data using the trained model. The model evaluates whether patterns in the data point to possible attacks. The accuracy and efficacy of the model's predictions are then confirmed by comparing them to known instances and performance metrics. The model, which engages in ongoing cycles of prediction and verification, is ready for real-time deployment.

A final, extremely sophisticated detection model is produced through this iterative process of data preprocessing, training, optimization, and prediction verification. With improved capabilities, this model, as shown in fig. [2], can accurately identify and anticipate possible attacks in real-time scenarios.

To develop a reliable and flexible system for identifying security threats, the algorithm continuously processes data, trains models, and refines them using real-time data streams. An intentionally selected dataset with a benign to malignant instance ratio of 6000:1 was used in this investigation. It was the intention of this purposeful imbalance to allow the model to concentrate on fully understanding the subtleties of typical behavior within the dataset. Every departure or anomaly from this established standard is expected to be more precisely recognized and categorized as possible deviations or attacks by giving priority to comprehending regular patterns.

The stated algorithm in fig[2] is evidence of the unwavering effort to strengthen security infrastructures against threats that are always changing. From data intake to model refinement, its complex layers represent an unwavering commitment to accuracy, flexibility, and real-time monitoring. Through the combination of cutting-edge methods, thorough performance assessments, and iterative improvements, this algorithm ultimately results in the development of a powerful detection model.

VI. RESULTS

Our assessment of the Dynamic LSTM-based Anomaly Detection (DLAD) model for detecting zero-day attacks is presented. With a focus on evaluating DLAD's capacity to identify new and previously undiscovered zero-day attacks, the evaluation was carried out using a diverse dataset that included both benign and attack instances.

To effectively detect zero-day attacks, one must be able to recognize and classify new instances of malware that have not been seen before. This is one area where the illustrated machine learning model shows promise, as evidenced by its excellent generalization performance. The model has been texted against real world dataset[15] and has provideed a high accuracy rate in detetcing zero day attacks. It is possible that the model performs well against zero-day malware that is displayed in fig[3]. The model's ability to identify zero-day attacks has been tested by training it on the larger and more varied dataset[15] that includes instances of zero-day malware.

The machine learning model's training and validation accuracy for malware detection and classification is displayed in fig[3]. The model's ability to predict the correct labels for training data is measured by its training accuracy, whereas its ability to predict the correct labels for data that has not yet been seen is measured by its validation accuracy. According to the graph in fig[3], as the number of training epochs increases, so do the training and validation accuracy. This suggests that the model is improving its ability to identify and categorize malware by learning from the training set.

The training and validation loss of a machine learning model intended for malware detection and classification is graphically represented in fig[4]. Validation loss evaluates how well the model generalizes to new, unseen data, whereas training loss measures the model's efficacy in learning from the training data. As the number of training epochs increases, the graph shows a trend toward diminishing training and validation loss. This means that the model's capacity to identify and categorize malware is improving as it gains more knowledge from the training set. Notably, though, is that the validation loss always stays marginally greater than the training loss. The reason for this discrepancy is that the model was unable to perfectly fit that particular dataset during training because it was not exposed to the validation data. A key feature for malware detection and classification is the model's ability to generalize to previously unseen data, which is suggested by the validation

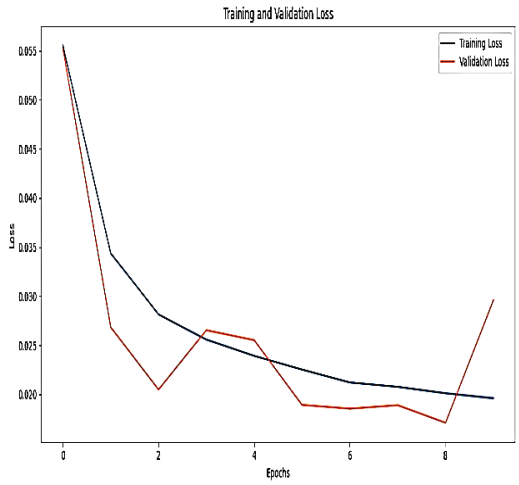

Fig. 3. Training and Validation Loss

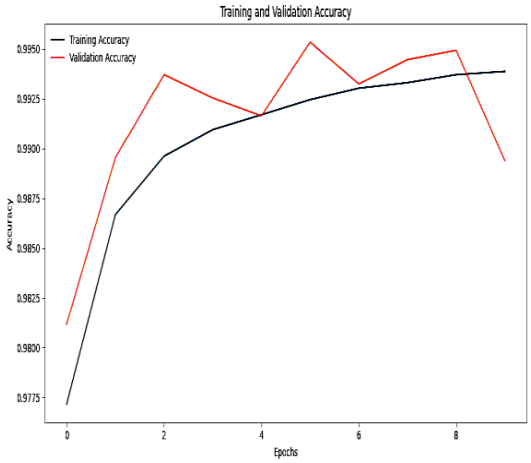

Fig.4. Training and Validation Accuracy

loss trend that has been declining over time. This competence guarantees that the model can successfully recognize and classify newly discovered malware instances.

The model can potentially detect zero-day malware patterns more accurately and adapt to new threats by integrating real-time threat intelligence feeds and continuous updates. Furthermore, adding strong anomaly detection methods to behavioral analysis can strengthen the model's capacity to recognize new attack patterns and increase its resistance to sophisticated adversarial efforts. Here are some more particular observations from fig[4] in addition to the previously mentioned ones:

A. After six epochs, the training accuracy reaches 99.50%, showing that the model is picking up the training data quite effectively.

B. After six epochs, the validation accuracy reaches 99.25%, which is also extremely high.

C. The model is generalizing well to new data, as evidenced by the relatively small difference between the training and validation accuracy.

D. After six epochs, the training and validation accuracy curves are both still slightly rising, indicating that additional training may be able to raise the model's accuracy even further.

E. The precision of 98.88% demonstrated by the model is outstanding and highlights its ability to correctly identify actual positives among the expected positives.

F. With a 98.78% recall rate, the model showed good sensitivity in identifying true positives while reducing false negatives.

G. Harmonizing accuracy and recakk, the model's robust performance in stiking a balance between accurate positive predictions and limiting false positives and false negatives was demonstrated by it's F1 score of 98.76%.

VII. Conclusion

The study presents DLAD, a novel Anomaly Detection model based on Dynamic LSTM that aims to strengthen intrusion detection systems against zero-day threats. It demonstrates how the model can quickly detect anomalies and adapt to changing network behaviors. It does, however, recognize the shortcomings of the existing analyses conducted against known datasets, emphasizing the need for more extensive and varied datasets that include instances of zero-day malware. The study recommends using adversarial training techniques to strengthen the model's defenses against sophisticated attacks. It shows excellent accuracy in detecting known threats, as well as detecting anomalies in the system and network. The work has proven its efficiency in detecting zero-day attacks .

References

[1] I. Mbona and J. H. P. Eloff, "Detecting Zero-Day Intrusion Attacks Using Semi-Supervised Machine Learning Approaches," *IEEE Access*, vol. 10, pp. 69822–69838, 2022, doi: 10.1109/ACCESS.2022.3187116.

[2] S. Tegane, F. Semchedine, and A. Boudries, "An extended Attribute-based access control with controlled delegation in IoT," *Journal of Information Security and Applications*, vol. 76, p. 103473, Aug. 2023, doi: 10.1016/j.jisa.2023.103473.

[3] M. Soltani, B. Ousat, M. Jafari Siavoshani, and A. H. Jahangir, "An adaptable deep learning-based intrusion detection system to zero-day attacks," *Journal of Information Security and Applications*, vol. 76, p. 103516, Aug. 2023, doi: 10.1016/j.jisa.2023.103516.

[4] A. K. Shukla, "An Efficient Hybrid Evolutionary Approach for Identification of Zero-Day Attacks on Wired/Wireless Network System," *Wireless Pers Commun*, vol. 123, no. 1, pp. 1–29, Mar. 2022, doi: 10.1007/s11277-020-07808-y.

[5] U. Zahoora, M. Rajarajan, Z. Pan, and A. Khan, "Zero-day Ransomware Attack Detection using Deep Contractive Autoencoder and Voting based Ensemble Classifier," *Appl Intell*, vol. 52, no. 12, pp. 13941–13960, Sep. 2022, doi: 10.1007/s10489-022-03244-6.

[6] B. I. Hairab, M. Said Elsayed, A. D. Jurcut, and M. A. Azer, "Anomaly Detection Based on CNN and Regularization Techniques Against Zero-Day Attacks in IoT Networks," *IEEE Access*, vol. 10, pp. 98427–98440, 2022, doi: 10.1109/ACCESS.2022.3206367.

[7] N. Sameera and M. Shashi, "Deep transductive transfer learning framework for zero-day attack detection," *ICT Express*, vol. 6, no. 4, pp. 361–367, Dec. 2020, doi: 10.1016/j.icte.2020.03.003.

[8] H. C. Altunay and Z. Albayrak, "A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks," *Engineering*

Science and Technology, an International Journal, vol. 38, p. 101322, Feb. 2023, doi: 10.1016/j.jestch.2022.101322.

[9] A. G. Sreedevi, T. Nitya Harshitha, V. Sugumaran, and P. Shankar, "Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review," *Information Processing & Management*, vol. 59, no. 2, p. 102888, Mar. 2022, doi: 10.1016/j.ipm.2022.102888.

[10] Y. Guo, "A review of Machine Learning-based zero-day attack detection: Challenges and future directions," *Computer Communications*, vol. 198, pp. 175–185, Jan. 2023, doi: 10.1016/j.comcom.2022.11.001.

[11] M. Zhang, "Network Attack Surface: Lifting the Attack Surface Concept to Network Level for Evaluating the Resilience against Zero-Day Attacks".

[12] D.-O. Won, Y.-N. Jang, and S.-W. Lee, "PlausMal-GAN: Plausible Malware Training Based on Generative Adversarial Networks for Analogous Zero-Day Malware Detection," *IEEE Transactions on Emerging Topics in Computing*, vol. 11, no. 1, pp. 82–94, Jan. 2023, doi: 10.1109/TETC.2022.3170544.

[13] T. Zoppi, A. Ceccarelli, and A. Bondavalli, "Unsupervised Algorithms to Detect Zero-Day Attacks: Strategy and Application," *IEEE Access*, vol. PP, pp. 1–1, Jun. 2021, doi: 10.1109/ACCESS.2021.3090957.

[14] P. Pitre, A. Gandhi, V. Konde, R. Adhao, and V. Pachghare, "An Intrusion Detection System for Zero-Day Attacks to Reduce False Positive Rates," in *2022 International Conference for Advancement in Technology (ICONAT)*, Jan. 2022, pp. 1–6. doi: 10.1109/ICONAT53423.2022.9726105.

[15] "Wireless Security Auditing: Attack Vectors and Mitigation Strategies - Amrita Vishwa Vidyapeetham." Accessed: Nov. 23, 2023. [Online]. Available: https://www.amrita.edu/publication/wireless-security-auditing-attack-vectors-and-mitigation-strategies/

[16] S. Akarsh, K. Simran, P. Poornachandran, V. K. Menon, and K. P. Soman, "Deep Learning Framework and Visualization for Malware Classification," in *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, Mar. 2019, pp. 1059–1063. doi: 10.1109/ICACCS.2019.8728471.

[17] Q. Zhou and D. Pezaros, Evaluation of Machine Learning Classifiers for Zero-Day Intrusion Detection -- An Analysis on CIC-AWS-2018 dataset. 2019.

[18] F. Alhaidari *et al.*, "ZeVigilante: Detecting Zero-Day Malware Using Machine Learning and Sandboxing Analysis Techniques," *Computational Intelligence and Neuroscience*, vol. 2022, p. e1615528, May 2022, doi: 10.1155/2022/1615528.

[19] "IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB." Accessed: Nov. 15, 2023. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html

[20] "Reinforcement learning algorithm for 5G indoor device-to-device communications - Sreedevi - 2019 - Transactions on Emerging Telecommunications Technologies - Wiley Online Library." Accessed: Nov. 23, 2023. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3670