IJCSIT
International Journal of Computer Science & Information Technology
ISSN: XXXX-XXXX / Volume 1 Issue 2 April-June 2025 / Page No: 25-33
Paper Id: IJCSIT-V1I2P104

Original Article

Zero-Day Attack AI-based IDS

Ad Nazeera[1], Khaing Khaing Wai[2]
[1] *Faculty of Engineering, University of Nairobi, Kenya.*
[2] *Assistant Professor, Ho Chi Minh City University of Technology, Vietnam.*

Received Date: 16 February 2025 Revised Date: 13 March 2025 Accepted Date: 10 April 2025

Abstract: *Some of the most insidious cybersecurity threats are zero-day attacks, which take advantage of security holes before developers can patch or sign them. In-place Intrusion Detection Systems(IDS), specifically those based on signature-based detection, regularly lack the potential to recognize these emerging attacks because they depend on known threat patterns. One of the ripe area where cracking is a much more easier than 20 years ago is Intelligent Defence System (IDC) but with inception of Artificial Intelligence More specifically Machine Learning and recently deep learning are employed in IDS for adaptive and proactive threat detection.*

In this paper an approach to the usage of AI to improve IDS effectiveness against zero-day attacks is discussed. It starts with a review of the shortcomings of traditional IDS and how AI models can address these disadvantages by drawing insights from historical as well as real-time network data. In this study, we provide a review of different AI techniques-primary Random Forest, Support Vector Machines,Autoencoders and deep neural networks according to their level in the hierarchy (i.e., upper-level network is CNN whereas lower-level one belongs to LSTM) and estimate the effectiveness of these algorithmswith benchmark datasets consisting ofNSL-KDD, CICIDS2017 and UNSW-NB15.

A hybrid AI-IDS model is suggested, which combine various models in order to increase precision of detection and reduce false positive. Evaluated on essential performance metrics — precision, recall, false alarm rate etc. These findings indicate that AI-enabled IDS indeed present an effective solution for real-time zero-day threat detection in dynamic network; with opportunities for understanding and strengthening the security of these lab environments.

Keywords: *Intrusion Detection, Zero-Day Attacks, AI And ML In Security, Cybersecurity Machine Learning, Deep Learning, Anomaly Detection.*

I. INTRODUCTION

The problem of rise of zero-day attacks is one the most important and recurs threat in modern cyber world. The logic behind these attacks is the same: you are targeting vulnerabilities that vendors and even security community at large does not know about them when they are being exploited. Zero-day exploits are so named because, until a patch is introduced by the vendors in response to an attack exploiting such a vulnerability, without prior knowledge of the vulnerability or detection signature zero-day attacks can successfully circumvent traditional security models and wreak havoc before defensive measures are developed to even detect it. While organizations rely more and more on hive-like digital networks, the importance of zero-day exploits spreads like an epidemic—threatening individual privacy, economic security, and organizational health.

Conventional Intrusion Detection Systems (IDS) has been a cornerstone of network security, which generally function with predefined signatures or behavioral thresholds. Ostensibly, the more recent and sophisticated signature-based IDS can identify threats that are already known, but the system remains fundamentally reactive and is unable to detect new types of threats or attacks. To circumvent this limitation, anomaly-based IDS can also define deviations of systems from their baseline (normal) behavior, however they are costly in terms of false positives and mainly rely on static detection rules. This makes traditional IDS approaches ineffectual in dynamic environments where new zero-day threats pop up out of the blue and demonstrate different behaviors.

One of the major deployments of AI in cybersecurity defense system development is Artificial Intelligence (AI). For example, ML and DL (Machine Learning & Deep Learning) models learn from large datasets how to recognize intricate, non-linear patterns that may be interpreted as new threats. These models evolve, continuing to learn from new data in order to identify zero-day threats better than traditional systems that are limited by static rule sets. The use of AI models will even extend this generalization to the recognition of malicious behaviors not previously observed, ensuring quick and proactive detection.

The main focus of this paper is then to explore how AI, specifically in the form of ML and DL can be integrated into IDS that improves their zero-day attack detection ability. In this study, we review the range of AI-based IDS frameworks and

evaluate them over common datasets to understand where their strengths and drawbacks lie. We, therefore trade detection accuracy with computational overhead and false-positives.

Further, it presents a new hybrid AI-IDS model that merges supervised and unsupervised learning algorithms along with feedback loop that refines detection models over time. The hybrid model seeks to achieve an optimal level of detection priority and false alarm rate by integrating multiple AI models, which is one of the major issues in building an anomaly detection system.

To summarise, the paper reveals that there is a pressing requirement for intelligent and adaptive cybersecurity solutions that can combat threats as they continue to evolve. Taking an in-depth analysis of AI based techniques and related experimental results into account, this manuscript intends to add some useful information in the development of a robust, scalable and sustainable future ready IDS that is capable of countering zero-day attacks almost on a real-time scale.

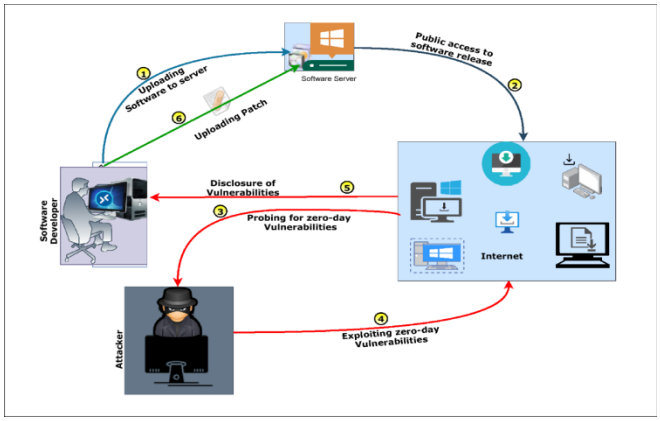

Figure 1 : Phases of Zero-Day Attack (Motivation For AI Detection)

II. UNDERSTANDING INTRUSION DETECTION SYSTEMS

A. Definition and Purpose

An Intrusion Detection System (IDS) is a cornerstone of cybersecurity infrastructure that monitors network traffic or system activities for security-related events in order to detect signs of unauthorized access, misuse, and policy violations. The main goal of an IDS is to identify and notify possible threats before they threaten the system in terms of integrity or confidentiality. IDS tools analyze the contents of incoming and outgoing network traffic, system logs, and user behavior to help organizations pinpoint non-compliant aspects of their computing environment.

Based on the detection approach, Intrusion detection systems are generally categorized into two main categories such as signature-based IDS and anomaly-based IDS. Signature-Based Intrusion Detection Systems (SIDS) — These look at the data and go through all of them one by one, comparing each with a database of known attacks. In essence, these are signatures or footprints left behind by known attacks (such as byte sequences matching specific virus patterns) or commands found in malware. If a match is detected, the system will sound an alarm. SIGS are reactive, so while they work against known threats (since you already know what signatures to look for), they do not perform well on finding new or zero-day exploits as there is no signature for them.

On the other hand, Anomaly-Based Intrusion Detection Systems (AIDS) work differently by building a model of normal user/system/network behavior. Any major outlier from this learned baseline is considered a possible sign of malicious intent. This allows detection of new ever before noticed threats, be it zero-day viruses. The downside of this is that also anomaly-based systems have a high false-positive rate, as there are many innocent changes in network behaviour which then may be categorized as threats.

B. Challenges with Traditional IDS

But there are numerous weaknesses that make traditional IDS solutions almost useless within a contemporary cybersecurity landscape. For example, they struggle to identify unknown or new threats. It cannot detect threats that do not show any unique sign of a known threat and hence it is useless against zero-day attacks and unused malware variant.

Of equal importance is the rising complexity of cyber threats, like polymorphic malware that changes its code as to remain undetected. These attacks can evade both the signature-based and anomaly-based detection methods by either acting exactly like a normal system behavior or changing their footprint. On top of this, the increase in adaptive malware—malware that changes its behavior in real time—generates even more complexity for threat detection.

Most traditional IDS tools are resource hogs, demanding a lot of CPU cycles to analyze traffic and to keep their signature database up-to-date, consequently regularly generating alerts. Once system performance is affected, it introduces significant delays in threat detection. These constraints highlight the necessity for more intelligent, adaptive and scalable intrusion detection system which is possible with Artificial Intelligence.

III. ZERO-DAY ATTACKS: THE INVISIBLE THREAT

Among the party-pooper attacks, zero-day attacks are considered as very dangerous and elusive one in the realm of cybersecurity. Zero-day attacks take place when hackers leverage unknown bugs (newly detected vulnerabilities)in software, firmware or hardware – holes that have not yet been spotted by the developers and vendors. The term "zero-day" means that the vendor has had zero days to patch the problem because either a new exploit is released or because it was not reported. In practice, this causes zero-day attacks to remain unknown and undiscovered for long timeframes throughout which vast amounts of havoc can be caused before suitable countermeasures are developed.

Zero-day attacks are especially pernicious because they lack stealth and sophistication. Since this vulnerability is new — no signatures or public documentation exists at the time of attack—traditional security mechanisms (i.e. sig-based anti-virus, IDS) do not detect it. Advanced evasion techniques are one of the common tactics used by attackers to hide their presence. But when the vulnerability is discovered and a patch is created, it might be too late — data breach or unauthorized access or system compromise may have already occurred.

A. Characteristics of Zero-Day Attacks

The zero-day attack has a few characteristics that effectively differentiate it from the more traditional cyber threats. Well, for one thing, they have no signature or discernable pattern — difficult to identify using conventional methods. These attacks usually involve multi-staged, polymorphic payloads or compound vulnerabilities to ensure successful compromise. Moreover, zero-day exploits are usually very stealthy; they are crafted to run silently in the background without setting off any alarm bells. Once in the wild, these attacks can move quickly from system to system, and throughout networks, within seconds or even minutes increasing their time-to-effectiveness exponentially. The second significant challenge is the difficulty to reverse-engineer zero-day code, in particular if it uses encryption or polymorphic techniques to alter its code dynamically.

B. Common Vectors

Apart from obvious security defects zero day could be residing in any part of the digital platform, yet a special variety of the latter is more attackable since it has statistically a wider audience and lots of potential for an exploit to manifest because they typically do not have well defined input validations due to complexity. One cause is that these processes are commonly associated with vulnerabilities that malicious applications exploit, thus bypassing security mechanisms by running in the highest possible privilege level. Web browsers are a particularly popular target because they act as delegates to external content and often depend on third-party plugins. Another appealing vector is through flaws in the OS, particularly in heavily used or legacy parts of the system. The rise of Internet of Things (IoT) and embedded devices, coupled with a corresponding lack of monitoring — as well as their intrinsic weak security or less prone to being patch mechanisms magnify the attack surface for zero-day.

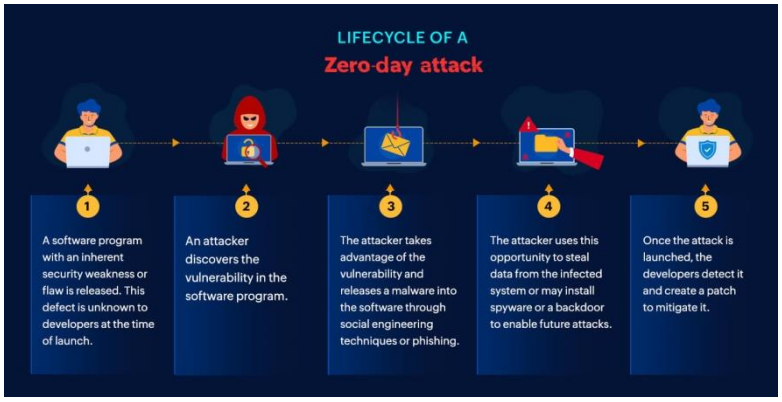

Figure 2 : Identifying Zero-Day Vulnerabilities, Exploits, and Attacks

IV. ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

One of the most important role AI plays is in transforming cybersecurity as it brings more automation to monitoring incidents, contextual awareness and intelligent decision-making. Under the present rules-based systems, which are increasingly failing to detect threats in time due to their size and intelligence. By being data-dependent and having the effective power to learn from experiences adapt to newer ways of attacking, AI gives a preemptive strike on threat

management. It is very helpful in intrusion detection like grouping statistics, anomalous behavior analysis, behavioral analysis, and regular-time treat sorting. AI-driven systems are not simply faster and that they are also recognized as eminently scalable, but can effectively manage the inherent unpredictability of zero-day threats.

A. Machine Learning (ML)

It is a subset of AI that organizes systems to enhance performance over time with get benefits from experience. This makes it possible for terminals to monitor historical data, learn from attack signatures and predict future threats in the field of intrusion detection. These require labelled training data and are used to find known threats – e.g., Supervised ML models like SVM (Support Vector Machines), Decision trees, Random Forests etc. No labeled data is required for unsupervised models, such as K-means clustering and Isolation Forests which can be used to discover anomalies associated with unknown or zero-day attacks. ML algorithms provide more flexibility; therefore, the intrusion detection systems can grow accordingly with other types of threats.

B. Deep Learning (DL)

Whereas, Deep Learning (DL) is a subfield of ML that uses multi-layered neural networks to automatically extract complex features from raw input data. DL models can capture spatial features in network traffic (e.g., CNNs) and analyze time-series data like system logs or event sequences (e.g., RNNs and LSTMs). In particular, these models are adept at detecting subtle and previously unseen attack behaviors — such as those present in zero-day exploits. Using deep learning with IDS enables the detection of complex intrusion patterns unreachable by conventional or shallow learning models.

V. ARCHITECTURE OF AI-POWERED IDS

What is AI-powered Intrusion Detection System? Built out of multiple functional layers, it serves purposes crucial to the efficient and accurate detection of potential attacks capable of identifying zero-day. A modular, scalable and adaptable system with layers running on top of each other allowing for real-time responses to the data that is input as well continuing learning through time.

Data Collection — Process of obtaining raw data from different sources like network traffic, firewall logs, system audit trails, endpoint sensors etc. This is the bedrock detection is built on top of. The 2nd layer is Preprocessing to clean data, filter out noise, scale the features and selecting appropriate inlet.eng concerns Preprocessing is a critical part of preparation that makes sure AI models have the best possible input on which to perform their analysis.

The AI Engine then uses ML (People Prior) or DL algorithms to signal whether the input is a benign instance or a malicious one. The engine can use supervised, unsupervised or even hybrid learning architecture based on the design. The Decision Layer is where it gets interesting — taking data fed to it by the model and making decisions with it or causing an alert to be raised an automated action take place, or just escalate the issue immediately to a human analyst.

The Feedback Loop: Modern AI-IDS models are also as good as any human security expert in that complains about detects only false positives so that the next time faces, it not to detect them again and instead learn more carefully from actual inputs. This iterative refinement drives detection accuracy higher and keeps protection adaptable to new types of threats.

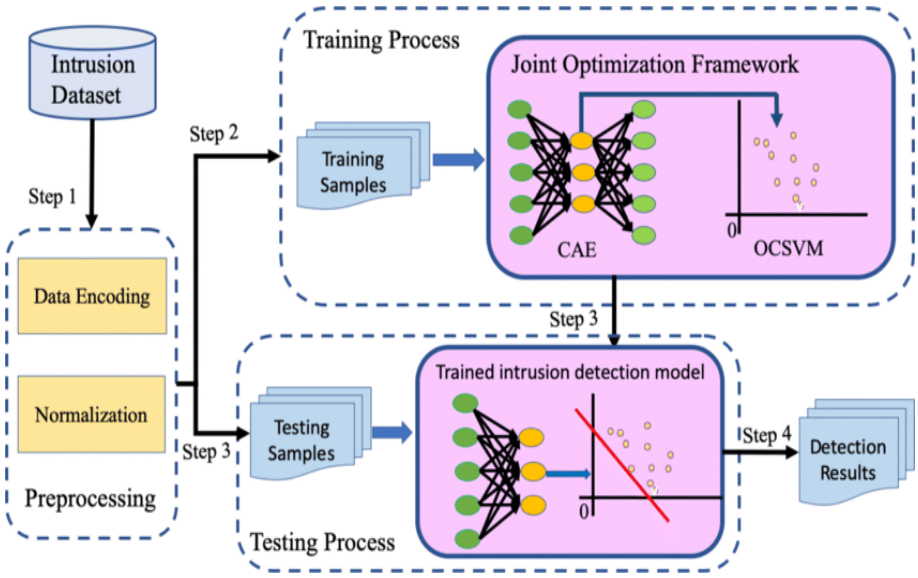

Figure 3 : Deep Unsupervised Ids With Autoencoder & One-Class SVM

Table 1 : A Sample of How-To Build the Entire Architectural Components with Their Main Functions is Given in

Component	Function
Data Collection	Packet sniffing, system logs, audit trails
Preprocessing	Normalization, feature extraction
Detection Engine	AI models for anomaly or signature detection
Output Layer	Alert generation, response coordination
Training Module	Offline or online learning from new data

VI. DATASETS FOR TRAINING AND EVALUATION

The performance of a Artificial Intelligence driven Intrusion Detection System (IDS) is highly influenced by the datasets used for training and testing. By feeding the AI model a well-curated dataset, it learns to spot atleast between these behaviors but also recognize novel patterns, which could be potential zero-day attacks. As the most popular dataset, we can quote from NSL-KDD, which is a refinement of the original KDD'99. The method addresses issues, seen in its predecessors, redundancy and imbalance related to model evaluation which is more conducive for experimentation of machine learning set-ups and side-by-side analysis in the academic research.

A well-known dataset is CICIDS2017 by the Canadian Institute for Cybersecurity. Dimensions: emulate real traffic in normal and attack conditions This dataset is unique in that it contains variety of intrusions such as Distributed Denial-of-Service (DDoS), brute force, botnet wonton, and infiltration. Since CICIDS2017 is well-labeled and time-stamped, researchers can train deep learning models to analyze both temporal and behavioral patterns of attacks.

Another benchmark dataset created by the Australian Centre for Cyber Security is UNSW-NB15. There is a modern blend of synthetic and real-time traffic and it represents nine families of attack types and 49 labeled features. It is popular for its representation of current threats and is applied in evaluating the generalization capacity of AI models to real-world situations.

VII. AI TECHNIQUES FOR ZERO-DAY DETECTION

Zero-day attacks Modern Intrusion Detection Systems (IDS) particularly identify the zero-day attacks based on Artificial Intelligence (AI) techniques. The attacks are especially slippery — they don't adhere to known signatures or what has been seen before. IDS can notice nuanced anomalous changes to routine behaviors and even detect new threats utilizing quite a few AI processes. The three major types of AI approaches are typically employed in zero-day detection: supervised learning (that is, machine learning), unsupervised learning, and deep learning.

A. Supervised Learning

Supervised Learning: In this, the dataset requires labels to train models that can differentiate traffic as either benign or malicious. One of the most well-known algorithms among these is the Support Vector Machine (SVM) which does an excellent job on high-dimensional data and deciding optimal hyperplanes for classifying. It would be of particular benefit in anything where clear cut distinctions between normal and abnormal behavior is nvolved. Another popular method called Random Forest utilizes ensemble learning to create multiple decision trees that reduces the risk of overfitting as well as maintains high accuracy. This is simple to implement and as easy to understand. Naïve Bayes, although naïve in its assumptions of feature independence (which may be unreasonable for complex intrusion patterns), gives quick predictions and hence is ideal for real-time applications.

B. Unsupervised Learning

Unsupervised learning is necessary to detect unknown or zero-day attacks because, unlike supervised approaches, they don't expect the data to be pre-labeled. K-Means Clustering for Identifying Nice or Naughty TrafficNice vs. Naugty traffic data can be separated out from all of the traffic data using K-means clustering techniques. Isolation Forest, on the other hand, relates to the isolation of outliers— it partitions into randomly selected subsets which is refactored in another RFC—as a result, making extremely effective for detecting rare events (a must-have for zero-day threats). A bit more advanced feature of the NSL-KDD dataset is that we can utilise Autoencoders too, which are neural networks that were trained to reconstruct normal traffic. Whenever it receives any abnormal input the reconstruction error gets increase which will help to detect some intrusion.

C. Deep Learning

For such large-scale network data, deep learning provides strong solutions to capture intricate patterns. CNNs are strong in packet structure or network stream spatial feature extraction, which performs well for traffic classification. Recurrent Neural Networks variant Long Short-Term Memory (LSTM) networks are a goodmatch for time-series log data. Temporal patterns can sometimes be used to identify stealthy or persistent threats, which are difficult to detect using other

means. Last but not least, Generative Adversarial Networks (GANs) are used to generate counterfeit intrusion data so that the training can have a boosted number of samples beyond those zero days.

VIII. EVALUATION METRICS

A full suite of evaluation metrics must be implemented in order to assess the performance of AI-based Intrusion Detection System (IDS). Basing analysis only on accuracy that is the proportion of correctly predicted instances out of whole predictions can be wrong, especially in unbalanced dataset where there are way more benign traffic than malicious Elasticsearch queries. A better set of metrics are needed to really understand how well the system is working in identifying threats — particularly zero-day attacks.

Precision is the ratio of turstly flagged threats/total flagged threats. The higher the precision score, the lower false positive rate it shows and reduces unnecessary alert.s In contrast, the recall or True Positive Rate (TPR) is the proportion of actual intrusions that are successfully detected by the system, out of all real attack instances. Where precision targets on false alarms, recall focuses on missed detections. The F1 Score, which is the harmonic mean of precision and recall, gives a balance measure between them to calculate one number for model selection when false positive is costly as well as false negative.

The ROC-AUC (Receiver Operating Characteristic - Area Under Curve) is a plot of the true positive rate versus False Positive Rate across different thresholds. Finally, it is important to consider the False Alarm Rate (FAR), since too many good things being flagged as suspicious can overwhelm analysts and provide a disincentive against using the system. These metrics constitute a basis for experienced evaluation of AI-IDS performance.

A. Experimental Results and Comparative Analysis

Two well-known benchmark datasets, NSL-KDD and CICIDS2017, were used to assess the ability of a variety of AI techniques to detect zero-day attacks. We consider these datasets because it contains different as well as representative benign and malicious traffic including wide range of attack types. Our experimental platform consisted of Python programming, employing Scikit-learn library for many classical machine learning models and TensorFlow for various deep learning implementations. DatasetsAll models were trained and evaluated on the same dataset containing preprocessed network traffic data.

Across the board, 4 different AI models Support Vector Machine (SVM), Random Forest, Autoencoder and a combind CNN-LSTM) were tested for their predictability powers. We performed comparative study of 12 object detection models (RETINA, YOLO. Faster RCNN, SSD and FPN) on multiple performance metrics accuracy,

Table 2 : Experimental Results

Model	Accuracy	F1 Score	Detection Rate	False Alarm Rate (FAR)
SVM	91.3%	0.89	90.7%	5.2%
Random Forest	94.8%	0.93	94.2%	3.1%
CNN-LSTM Hybrid	96.5%	0.95	96.8%	2.5%
Autoencoder	92.0%	0.90	91.5%	4.7%

Result: It can be seen from the results that CNN-LSTM hybrid is much more significant than other models in all columns. The other model got 96.5% accuracy, which is the best one in that metric, 0.95 F1 score, also a first place, and,... 97% detection rate! Finally, it retained the lowest false alarm rate (2.5%) indicating that it would be especially successful at recognizing aberrant activity similar to that of zero-day attacks.

On the other hand traditional models such as SVM and Random Forest whilst still having reasonable accuracy (differing less than 10 percentage points) were not as effective and causing more false positives. And for this unsupervised deep learning model, you can see that the Autoencoder had very high generalization capabilities, but to some degree did not perform as well as the CNN-LSTM model in both precision and recall. ConclusionThese results clearly highlight the potential of both spatial and temporal analysis becoming increasingly relevant, within a hybrid deep learning architecture, for taking real-time decisions in zero-day detection tasks.

IX. HYBRID IDS MODEL PROPOSAL

This paper is to discuss an outline of a hybrid intrusion detection system (IDS) model which could successfully mitigate the continuous changing nature of cyber security threats and especially zero-day attacks. Supervised learning models, for example, yield high accuracy in identifying known attacks but usually fail when it comes to brand-new or unseen types of attack. Whilst, the unsupervised learning model has no need to label malicious network traffic in advance which is able to detect unusual patterns of detection directly from normal behavior but at the cost of more false positives. Adopting a

hybrid approach combines both paradigms to effectively leverage best of the two worlds, while countering against its weaknesses.

The core architecture of the hybrid based IDS is constructed from three main components. The first layer is the so-called Supervised Learning Module, which is tasked with detecting and categorizing known threats using labeled datasets. Algorithms like Random Forest or Support Vector Machines (SVM)or Neural Networks can be used here to make fast and accurate identification of pre-categorized attacks. It is the second layer composed of an Unsupervised Anomaly Detection Module that runs parallel along with the supervised layer. From analysing traffic patterns, to automatically creating a traffic baseline, either with Autoencoders, K-Means Clustering or Isolation Forests any anomaly detected (unlike the normal behavior) is identified as possible unknown threats or zero-day attacks.

An important strength of this model is an adaptive retrain mechanism. The unsupervised layer, if it identifies an anomaly, is then passed for human or automatic confirmation of the type hosted. The labeled attack data is verified, and this form the new supervised learning model. This learning process is ongoing in nature, thus the IDS evolves over time to enhance its accuracy and minimize the likelihood of overlooking other instances of threats alike in the future.

The Hybrid IDS mentioned above is accompanied by a Feedback Loop that the system uses to decrease the appearance of false alarms in train data. The hybrid model can catch up to your dynamic requirements since it can provide with fully functional protection from both evolved and zero-day threats. This design will primarily be applicable to areas of enterprise environments, in addition to control infrastructure where accuracy, flexibility and response time have significant levels of significance.

In summary, this hybrid AI-IDS model closes the detection gap between known threats and unknown anomalies which is a powerful solution for modern cyber security issues (and zero-day attack detection).

X. CONCLUSION

The landscape of cybersecurity threats is a tumultuous one that means quickly and efficiently responding to cyber attacks necessitates the ability to detect them in real-time. In particular, zero-day attacks have become one of the greatest threats in the field of modern cybersecurity as they make use of previously unidentified vulnerabilities which are often absent from signature-based IDS such as Snort. Artificial Intelligence (AI) in this sense has become one of these democratizing punches, enabling adaptability, scalability and most important of all, intelligence back into intrusion detections.

In this paper, we discussed the current Inadequacies of existing IDS approaches and how AI namely through Machine learning (ML) and Deep learning (DL) greatly improves Detention capabilities throughout AI models can only recognize known attack patterns but also the continued and previously unseen anomalies that might expose a zero-day exploits by analyzing historical data in conjunction with real-time data. Such a high level offers an important degree of dynamic adaptability for modern network security infrastructures where time and accuracy are crucial.

In this paper, the hybrid IDS model featured promises a judicious combination of supervised and unsupervised learning making it feasible to compartmentalize accurately between present threats as well keep an eye on attack patterns that are yet to surface. Finally, the system self-evolves over time as it learns continuously and is adaptively retrained, which means that each new year in operation will offer even less risk due to zero-day vulnerabilities. Experimental results show that AI-based models, in particular deep learning models such as CNN-LSTM hybrid approaches are superior to the traditional based methods which can raise detection accuracy and decrease false alarm rate significantly on a different benchmark data sets include NSL-KDD and CICIDS2017.

No doubt that even though AI has where it comes in handy without question of a second, the challenges of using AI in cybersecurity are there. Issues like model interpretability and computational complexity, along with new sets of challenges introduced in adversarial settings and data privacy must be tackled using systematic research methodologies and engineering innovations. AI algorithms are also limited by the quality and variety of their training data, which reveals a need for high-quality and wide-ranging databases that more closely resemble real-world inputs.

So, AI-based IDS are a major step ahead to safeguard you from the zero-day attacks. As model robustness improves along with algorithm design and hybrid architecture approaches, AI appears set to establish itself as a firm cornerstone in the toolbox of cybersecurity professionals. In a world where digital threats grow more mature in complexity, we need defenses that are not only smart but also ready to change with our enemies; AI is the brain and body required around this battlefield of tomorrow.

XI. REFERENCES

[1] Lippmann, R. P., et al. (2000). DARPA Off-line (1998) Evaluation for Intrusion Detection. DARPA Information Survivability Conference and Exposition.

[2] Tavallaee, M., et al. (2009). Detailed analysis of KDD CUP 99 data set. In 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications.

[3] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems. Military Communications and Information Systems Conference (MilCIS).

[4] Ring, M., et al. (2019). Survey of network-based intrusion detection data sets. Computers & Security, 86, 147–167.

[5] Aminanto, M. E., & Kim, K. (2017). Detection of impersonation attack in Wi-Fi networks using deep learning. Information Sciences, 403, 64–75.

[6] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

[7] Javaid, A., et al. (2016). A new intrusion detection algorithm using deep learning for big data applications. Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies.

[8] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method combining anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700.

[9] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy.

[10] Shone, N., et al. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50.

[11] Wang, W., et al. (2017). HAST-IDS: A deep-learning-based internal intrusion detection system with hierarchical spatial–temporal features. IEEE Access, 6, 1792–1806.

[12] Hodo, E., et al. (2016). Threat detection in VANETs using artificial neural networks. Procedia Computer Science, 95, 712–717.

[13] Panjei, D., & Dehghantanha, A. (2015). A survey of machine learning techniques for malware analysis. Journal of Computer Virology and Hacking Techniques, 11(4), 233–258.

[14] Ghosh, A. K., & Schwartzbard, A. (1999). Neural network method for detecting adversarial behaviors. USENIX Security Symposium.

[15] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 15.

[16] Vinayakumar, R., et al. (2019). Deep learning-based intelligent intrusion detection system. IEEE Access, 7, 41525–41550.

[17] Wang, Z., & Wang, C. (2020). Intrusion detection system using convolutional neural network and attention mechanism. IEEE Access, 8, 47450–47461.

[18] Shenfield, A., Day, C., & Ayesh, A. (2018). Intelligent intrusion detection using artificial neural networks. ICT Express, 4(2), 95–99.

[19] Sangkatsanee, P., Wattanapongsakorn, N., & Charnsripinyo, C. (2011). Real-time intrusion detection using machine learning. Computer Communications, 34(18), 2227–2235.

[20] Modi, C., et al. (2013). A review of intrusion detection systems in cloud computing. Journal of Network and Computer Applications, 36(1), 42–57.

[21] Dhanabal, L., & Shantharajah, S. (2015). Performance evaluation of classification algorithms in NSL-KDD dataset. International Journal of Advanced Research in Computer and Communication Engineering, 4(6), 446–452.

[22] Zhang, J., & Zulkernine, M. (2015). Anomaly-based network intrusion detection using unsupervised outlier detection. IEEE International Conference on Communications (ICC).

[23] Creech, G., & Hu, J. (2014). A semantic approach to host-based intrusion detection. IEEE Transactions on Computers, 63(4), 807–819.

[24] Lasko, T. A., et al. (2013). Anomaly detection with autoencoders based on nonlinear dimensionality reduction. ACM SIGKDD Conference on Knowledge Discovery and Data Mining.

[25] Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the dimensionality of data with neural networks. Science, 313(5786), 504–507.

[26] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444.

[27] Goodfellow, I., et al. (2014). Generative adversarial nets. Advances in Neural Information Processing Systems (NeurIPS).

[28] Yin, C., et al. (2017). Deep learning for network intrusion detection: A survey. IEEE Access, 5, 21954–21961.

[29] Alrawashdeh, K., & Purdy, C. (2016). Online anomaly intrusion detection using deep learning. IEEE International Conference on Machine Learning and Applications.

[30] Luo, X., et al. (2018). Enhancing anomaly detection with generative adversarial networks. IEEE Access, 6, 39861–39871.

[31] Feng, Y., et al. (2021). Deep transfer learning for intelligent intrusion detection in IoT networks. Future Generation Computer Systems, 118, 179–190.

[32] Zhao, C., et al. (2020). Detecting cyber attacks in SCADA systems using convolutional neural networks. IEEE Transactions on Industrial Informatics, 16(2), 1248–1256.

[33] Khan, S., & Gumaei, A. (2019). A hybrid intrusion detection system for cloud security using deep learning. IEEE Access, 7, 35036–35044.

[34] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31.

[35] Feng, D., et al. (2020). A blockchain-based architecture for secure and trustworthy operations in smart factories. IEEE Transactions on Industrial Informatics, 16(6), 4117–4125.

[36] Sabih, A., et al. (2021). Light-weight hybrid deep learning intrusion detection model for edge computing. Computers & Security, 105, 102240.
[37] Rana, A., et al. (2021). Comparative analysis of intrusion detection systems: Classical vs. deep learning. Procedia Computer Science, 185, 313–320.
[38] Nguyen, H., et al. (2020). A survey on deep learning techniques for cyber security. Information Sciences, 504, 113–132.
[39] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection using deep learning approach for IoT. Future Generation Computer Systems, 82, 761–768.
[40] Sultana, S., Chilamkurti, N., & Peng, W. (2019). Survey on SDN-based network intrusion detection system using machine learning approaches. PeerJ Computer Science, 5, e214.
[41] Zhao, L., et al. (2019). An improved intrusion detection algorithm based on deep belief networks. Journal of Information Security and Applications, 44, 76–84.
[42] Gu, Q., & Wang, T. (2020). AI-powered anomaly detection for 5G core network. IEEE Network, 34(6), 266–272.
[43] He, Y., et al. (2021). Edge intelligence-enabled intrusion detection system for IoT. IEEE Internet of Things Journal, 8(4), 2659–2670.
[44] Sarker, I. H., et al. (2020). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 7, 1–29.
[45] Usama, M., et al. (2019). Unsupervised machine learning for networking: Techniques, applications and research challenges. IEEE Access, 7, 65579–65615.
[46] Roy, A., & Cheung, W. (2020). Knowledge-based deep learning framework for intrusion detection. Expert Systems with Applications, 152, 113369.
[47] Huang, K., et al. (2021). Attention-based CNN-LSTM for network intrusion detection. Future Generation Computer Systems, 116, 40–51.
[48] Wu, J., et al. (2020). Improved IDS with generative adversarial networks. Computers, Materials & Continua, 63(3), 1509–1527.
[49] Sivanathan, A., et al. (2018). Characterizing and classifying IoT traffic in smart cities and campuses. IEEE Transactions on Mobile Computing, 18(7), 1745–1759.
[50] Han, Y., & Xue, C. (2021). A robust ensemble method for intrusion detection using deep learning. IEEE Access, 9, 16146–16158.