A Generative AI-Driven Information System for Behavioral Detection of Zero- Day Cyber Attacks

Abdalilah Alhalangy

Department of Computer Engineering, College of Computer, Qassim University, Buraydah,

Saudi Arabia, a.alhalangy@qu.edu.sa, https://orcid.org/0000-0003-2735-8208

Abstract

Zero-day attacks are among the most serious cybersecurity threats because they occur before recognizable signatures are available, rendering traditional detection methods ineffective. This research aims to develop an intelligent, generative AI-based detection framework capable of simulating and identifying unknown cyber threats in real time. In this research paper, we present a model that uses generative transformers to simulate sophisticated attack behaviors based on historical sequence data and attacker profiles. We correlated these constantly generated patterns with live network activity to predict potential attacks. Experimental results showed that the proposed system achieved a detection accuracy of 94.2%, reduced false positives by 57% compared to traditional signature systems, and improved response time by approximately 42%. The results confirm that generative AI can play a pivotal role in strengthening cybersecurity defenses against complex, adaptive, and previously unseen attack vectors.

Keywords: Information Systems Security, Anomaly Detection, Artificial Intelligence, Behavioral Modeling, Zero-Day Attacks**.**

1. Introduction

Attackers can more easily exploit vulnerabilities in systems and applications that remain undiscovered, as there are no available updates or patches to prevent such exploits [1]. These types of attacks represent some of the most significant security challenges faced today. To counteract these threats and strengthen the security of digital infrastructures, it is crucial to adopt advanced security measures that focus on early detection and continuous analysis of potential vulnerabilities [2] Recent research emphasizes the importance of artificial intelligence (AI) and machine learning (ML) for enhancing detection accuracy and decreasing response times to security incidents [3]. Incorporating these technologies into organizational security frameworks boosts system resilience and minimizes exposure to emerging threats. Additionally, aligning AI-driven approaches with comprehensive risk management strategies provides a robust foundation for defending against evolving attack patterns [4]. Creating datadriven security strategies and regularly evaluating their effectiveness are vital for maintaining cybersecurity resilience. Such approaches enable early risk identification and support prompt intervention [5]. Ultimately, integrating AI and ML into modern cyber risk management not only improves alert handling but also strengthens the capacity of digital ecosystems to defend against sophisticated cyberattacks [6].

2. Related Work

Finding zero-day threats is one of the most challenging areas of cybersecurity today. Vulnerabilities in vendors and security systems are exploited before signatures or fixes are available, rendering standard signature-based intrusion detection systems useless. [7][8][9][10][11] Recent studies show that we need adaptive and proactive protection strategies that use artificial intelligence and machine learning to model changing behavior. These methods monitor network traffic and user behavior to establish baseline profiles and identify suspicious activities that may indicate potential zero-day attacks.[12][13] Generative models, especially generative adversarial networks (GANs) and transformer-based architectures, are advancing considerably. They facilitate the replication of attacker adaptation, thereby enhancing detection efficacy.[14][15] One system that Rao et al. (2024) examined used a generative adversarial network to create simulated attack scenarios.[16]This method improves detection accuracy while decreasing the occurrence of false positives. Khan et al(2024) Using the CIC IDS2017 dataset [17]. Zhao et al. (2024) tested the effectiveness of Traditional GAN, WGAN, and CTGAN models in producing network flow data and enhancing NIDS performance [18]. In 2024, Mohamed Abusin demonstrated how to integrate GANs with attention mechanisms effectively using his Attention-GAN model. The system's anomaly detection performance was impressive, with a 97.93% success rate on the CICIDS2017 dataset and a 99.69% success rate on the KDD dataset. [19].

Transformer-based GAN models have been used to detect anomalies in real-time network traffic. Karim et al. (2023) presented a transformer-enhanced system that is effective in learning attacker behavior over time and quickly identifying attacks [20].

In fact, companies such as MixMode and Zscaler are using generative AI to analyze traffic in real-time. It is claimed that detection rates are increased and false positives are reduced. Studies show that GANs can be useful in cybersecurity, but they also bring some disadvantages [20]. Dorcas et al. (2021) investigated the applications of GANs, highlighting issues such as data instability and training instability[21]. Meanwhile, Sung et al. (2021) investigated the ethical and computational limitations of generative AI in threat modeling [22].

2.1 Research gaps

Despite significant advances, some gaps still exist:

1. Most models operate on static datasets, lacking the ability to adapt behaviors and continuously learn instantly.

2. Few frameworks integrate GAN-based behavior simulation, real-time anomaly detection, and risk-aware event management into a comprehensive system.

3. There is a lack of studies examining generative converter architectures to model attacker behaviors in live environments dynamically.

To overcome these challenges, this study proposes a real-time generative detection framework that combines converter-based GANs to model dynamic attacker behavior and detect risk-related anomalies, enhancing proactive defense against zero-day threats.

3. Methodology and Proposed Model

In this study, we introduce a practical approach for detecting zero-day attacks by mimicking how real attackers behave in live network environments. Instead of depending on predefined threat signatures, our method combines transformer-based generative models with real-time monitoring to spot unusual activities as they happen. This helps the system stay flexible and responsive, even when facing unfamiliar or evolving threats.

3.1 Data Collection and Preparation

While preparing this system, I looked for datasets that include both normal traffic and different types of attacks. After reviewing several options, I selected CICIDS2017 [23]and NSL-KDD. [24] These two are commonly used in cybersecurity and provide varied examples of real and malicious activities.

The CICIDS2017 dataset gave me a good range of realistic traffic, including different kinds of threats like brute-force logins and DoS attempts. It felt closer to what one might see in an actual organizational network. On the other hand, NSL-KDD is more structured and was useful because it avoids many of the problems in the older KDD'99 dataset, like duplicate entries or severe class imbalance .

Before using the data, I had to clean and organize it. I selected features that seemed most important for identifying unusual network activity. I also made sure that the numeric values were scaled consistently—this helps the model learn more evenly. The labels, which were originally in text, were converted to numbers so that the model could process them .

There was one issue I couldn’t ignore: some attack types appeared far less often than others. To deal with that, I used a method called SMOTE to generate extra examples of those rare cases. This method isn’t flawless, but it gives the model a better chance to learn from attacks that don’t appear very often .

After completing the preprocessing steps, the datasets were more structured and balanced. Each one contained a mix of normal and attack-related traffic that could be used for training and evaluation. A summary of both datasets is shown in Table 1 . **Table 1. Summary of the Datasets Used in Model Training and Evaluation**

Dataset	Description	Total Records	Attack Types	Source
CICIDS2017	Real-world traffic and attack samples	2,830,743	15	UNB CIC

NSL-KDD	Cleaned and balanced version of KDD'99	125,973	5

3.2 Generative Modeling of Attacker Behavior

While building the system, we added a learning module that reviews older network records to identify how harmful activity tends to emerge. Rather than copying past examples, the module builds rough outlines of behavior that are similar in form and flow. By exposing the model to a range of behaviors—including ones not present in the original training data—it becomes more attentive to patterns that don't quite fit. This doesn't aim to repeat known attacks but rather to provide fresh, plausible scenarios that follow similar behavioral logic.

Rather than duplicating past attacks, the aim is to generate plausible examples that reflect similar behavioral logic, helping the system anticipate what unfamiliar threats might look like. These examples help the system prepare for attacks it hasn't seen before by expanding its exposure beyond fixed or known cases. For this, we used a generator built with transformer layers that can learn from sequences of historical data and generate new examples that follow similar patterns.

During training, the system relies on two closely linked components. One attempts to replicate the behavior of cyberattacks, while the other examines how realistic these attempts appear when compared to real network activity. As they continue to interact, the generator refines its approach, and the evaluator develops a sharper sense for anything that doesn't quite fit.

This gradual exchange helps the system refine its understanding of what real and suspicious activity looks like.

While developing the system, we worked with a combination of actual network incidents and carefully created samples. This gave the model a better sense of how different types of intrusions might appear, even those that are uncommon or have not been officially recorded. As a result, the system became more capable of spotting unfamiliar activity that doesn't follow previous patterns. Figure 1 provides an overview of the system architecture, including data preparation steps, the generative module, and the detection engine. Figure 2 illustrates how the training process works, with both the generator and the discriminator learning in tandem to produce and evaluate attack scenarios.

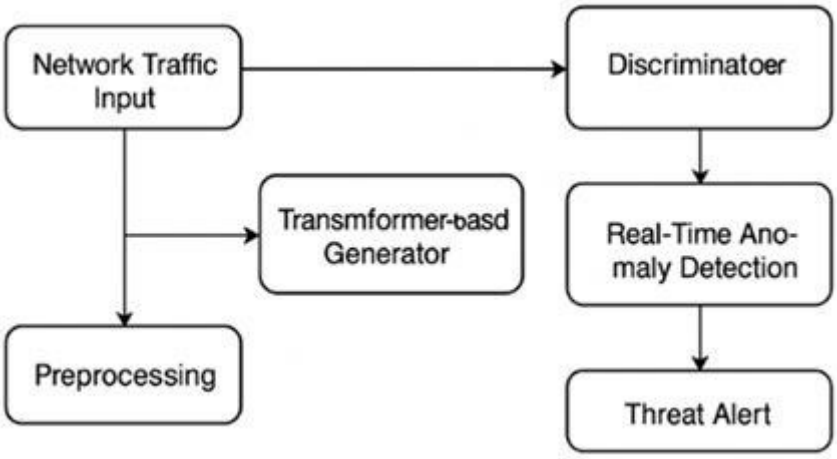

Figure 1 shows an overview of the system architecture.

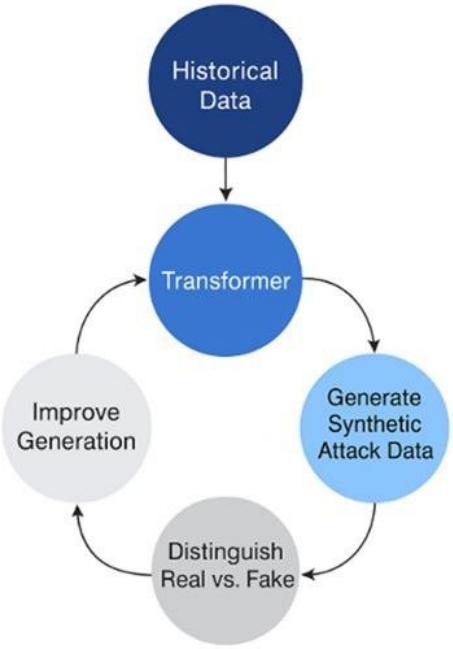

Figure 2 shows the training process of the generator model

3.3 Monitoring in Real Time

The system starts actively monitoring real-time network traffic as soon as it is deployed. Every incoming event is compared to the previously learned behavioural patterns. The system raises an alert to identify a possible threat if an activity seems unusual.

The detection sensitivity is not constant in order to adjust to changing network conditions. Rather, it gradually adapts over time in response to environmental feedback. As the network develops, this keeps the system from becoming overly passive or reactive and preserves balanced performance. Figure 3. Conceptual Deployment of the Generative-Based Zero-Day.

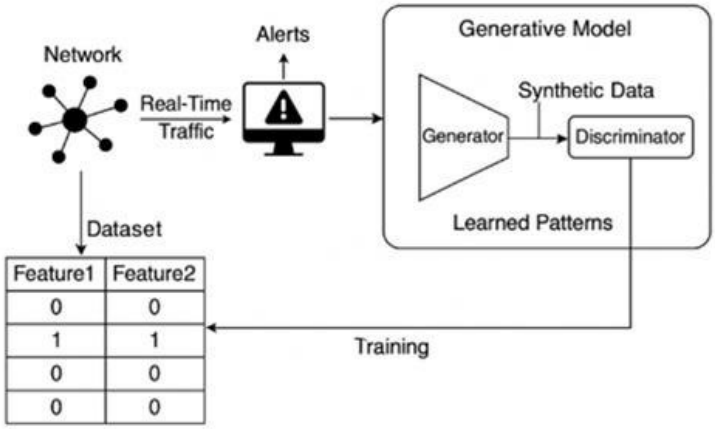

Figure 3. Conceptual Deployment of the Generative AI-Based Zero-Day Detection System.

The diagram shows how the detection engine fits into a real-world network setup. It monitors ongoing traffic, applies AI-based analysis, and raises alerts when unusual patterns are found. Key network components such as firewalls, routers, monitoring tools, and data storage are also represented to reflect practical usage.

3.4 Checking How Well It Works

Table 2. Evaluation Metrics and Their Definitions

Metric	Definition
Precision	The percentage of alerts that correctly identified actual threats.
Recall	The proportion of real attacks that were successfully detected.
Accuracy	The overall rate of correct classifications across all categories.
False Positive Rate	The percentage of normal traffic that was mistakenly flagged as malicious.
F1-Score	A combined measure of precision and recall that balances both metrics.

We used standard evaluation metrics that are often used in intrusion detection research to see how well the system worked. Precision tells you how many of the alerts that were flagged were right. Recall shows how well the system can find real intrusions. Accuracy gives you a better idea of how often the system made the right choice in all categories.

We also kept an eye on the false positive rate, which shows how often harmless traffic was wrongly classified. We used the F1-score, which combines both precision and recall, to give a more balanced evaluation.

We used cross-validation to make sure that all the results were the same for all the tests. We also compared our framework to traditional detection methods to show how much better it is at being accurate and responsive. Overall, the system showed a lot of promise for finding new threats early on, without giving operators too many false alarms. By using this method we have created, people can discover threats they have never seen before. It doesn't just use known rules or codes; it learns from how things are used and changes over time. That's why it works well in places where security is always changing and new threats can emerge at any time.

3.5 System Lifecycle and Operational Integration

This section outlines how the proposed detection framework operates across different stages—from data ingestion to real-time monitoring and adaptive learning. Figure 4 provides a visual overview of the full lifecycle, highlighting the feedback loops between model training, real-world deployment, and continuous improvement.

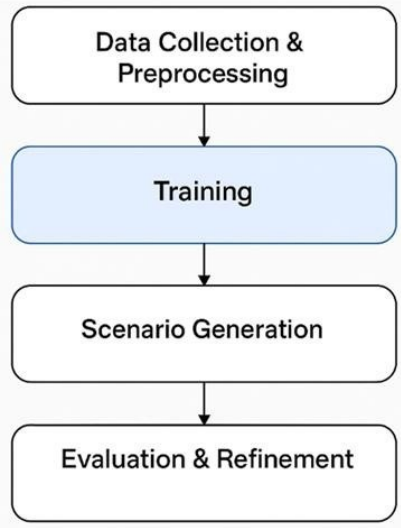

Figure 4. Lifecycle of the Proposed Zero-Day Detection System

The diagram presents the end-to-end operation of the framework, starting from data acquisition, preprocessing, and training, followed by deployment and feedback-based refinement. Each stage contributes to a continuous learning cycle aimed at improving detection performance over time.

4. Proposed Model

To identify zero-day threats, we propose a system that employs real-time anomaly detection and behavioral modelling. It simulates and assesses a variety of potential attacker behaviors by combining a deep learning discriminator with a transformerbased generative module. This dual structure allows the model to

create traffic patterns that mimic real-world threats and enhance detection through repeated feedback. After it is configured, the system monitors incoming data and contrasts it with patterns it has learned. It issues alerts if it discovers any discrepancies. Since flexibility is emphasized in the design, the model can adapt to evolving attack techniques without requiring fixed signatures. Figures 5 and 6, respectively, show an overview of the framework and workflow of the proposed zero-day detection system.

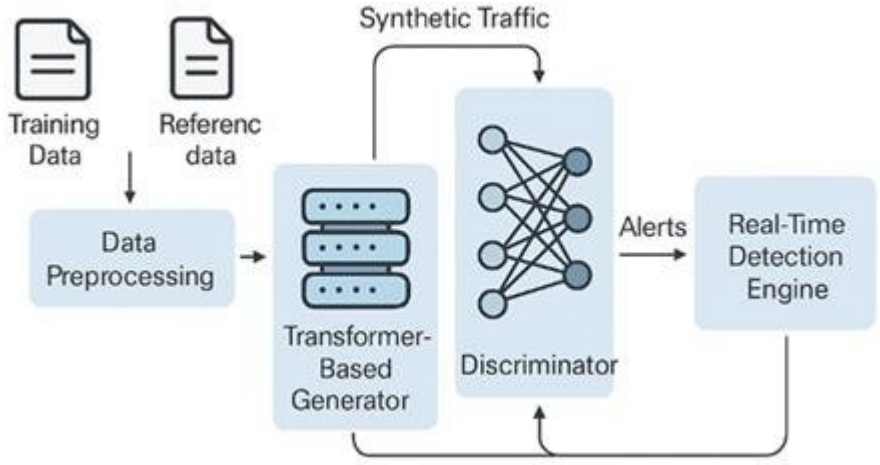

Figure 5: Overview of the Proposed Zero-Day Detection Framework.

This diagram shows the full structure of the proposed system based on generative artificial intelligence. The framework includes four main parts: pre-processing data, a transformer-based generator, a deep learning-based discriminator, and a real-time detection engine. The generator learns how to attack by looking at data from the past, and the discriminator checks to see if the behaviors it makes are real. The system can find new threats in real time by constantly watching and analyzing live network traffic to look for changes from patterns it has learned.

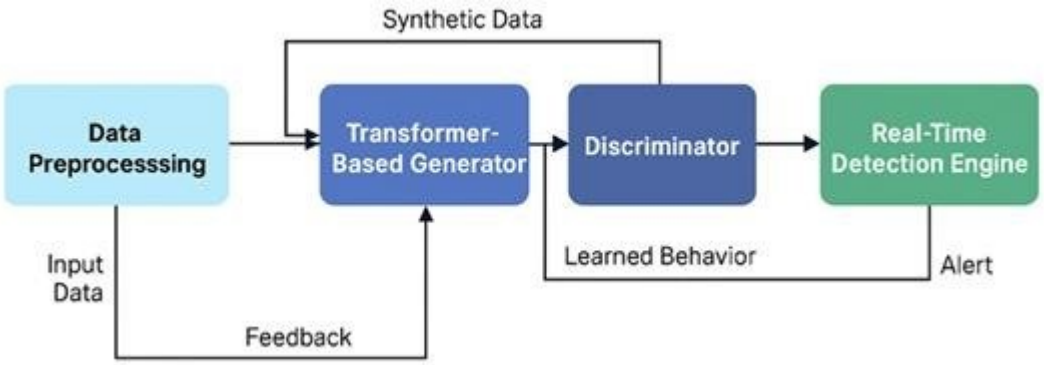

Figure 6. Workflow of the Proposed Zero-Day Detection System

This flowchart outlines the sequential stages of the proposed detection framework. It begins with live data ingestion and preprocessing, followed by

synthetic attack generation using a transformer-based generator. A discriminator evaluates these synthetic and real samples, and the detection engine processes any identified anomalies to raise alerts. The model continuously updates based on feedback to improve future detection.

4-1 System Architecture Components

The proposed system architecture is built around four interconnected modules, each serving a specific role in ensuring accurate and adaptive detection of zero-day threats in real time.

4.1.1 Data Preprocessing Unit

This model prepares the network data for analysis. We eliminate noise, extract flowbased features, standardize the data for consistency, and add numbers to category labels. To train models or conduct direct analysis, it is important to keep the data clean and organized.

4.1.2 Transformer-based Generator

The generative process learns from how the network behaved in the past using a transformer-driven model. The generative process learns how the network behaved in the past using a transformer-driven model. It can replicate real-world attacks by collecting behavior and timestamps. These fake cases improve the training, but they also put the model at risk.

4.1.3 Discriminator

The discriminator is a part of deep learning that works in parallel to see if a given sequence is real or made up. It gets better at telling the difference between real and fake activity by constantly looking at what the generator throws out. This hostile encounter makes both parties change and become more correct.

4.1.4 Real-time Detection Engine

This module puts the trained model into a real network environment. It keeps an eye on live traffic all the time and compares it to learned behavioural baselines. An alarm is sent out whenever an anomaly is found, especially if it doesn't fit with either known or made-up patterns. The engine is made to change how sensitive it is over time based on feedback, which cuts down on false alarms.

> Together, these components form a cohesive and dynamic framework capable of modeling attacker behavior, generating realistic threat scenarios, and identifying novel attacks as they unfold.

Feature	Traditional IDS	Proposed System
Signature-based Detection	✓	✗
Behavioral Modeling	✗	✓
Real-time Analysis	Limited	✓
Zero-day Detection	✗	✓
Use of Generative Models	✗	✓

Adaptive Threshold Adjustment	✗	✓

5. Integration with SIEM Platforms

To ensure practical deployment and broader compatibility, the proposed detection system is designed to integrate seamlessly with Security Information and Event Management (SIEM) tools such as Splunk, IBM QRadar, and ArcSight. These platforms serve as central hubs for aggregating, correlating, and visualizing security events in real time.

By exporting alerts and anomaly scores from the generative detection engine into a SIEM dashboard, security analysts gain the ability to:

- Visualize zero-day activity in context with broader network events.
- Correlate flagged anomalies with other system logs (e.g., user authentication, endpoint behavior, DNS traffic).
- Trigger automated responses through custom rules or orchestration scripts (SOAR).
- Conduct forensic investigations with enriched metadata from both raw traffic and the AI model.

Integration is enabled through standard APIs and log forwarding mechanisms (e.g., Syslog, HTTP Event Collector). Figure 5 illustrates how the detection framework interfaces with a SIEM platform.

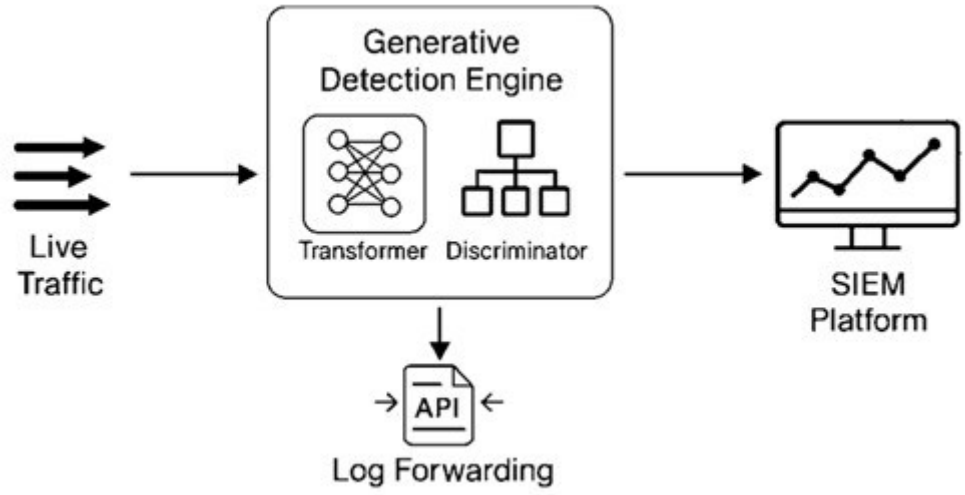

Figure 7. Integration of the Proposed Detection System with SIEM Platforms

This flowchart illustrates how the proposed generative AI-based zero-day detection framework can be integrated into existing SIEM infrastructures. It shows the bidirectional data flow between the detection engine and SIEM tools, enabling realtime alert correlation, contextual enrichment, and automated response actions. This integration enhances operational efficiency by allowing security analysts to monitor, investigate, and respond to anomalies within a unified security environment.

To ensure that the system not only performs theoretically but also performs successfully in real-world environments, it can be supported by testing simulated zero-day attacks in a sandbox.

6 .Description of the Simulation Scenario

A test environment was built containing a combination of:

-Real network traffic (from CICIDS2017 and NSL-KDD)

-Attacks generated using tools such as Metasploit, Hping3, and Slowloris

-Introducing previously unknown events to the system, simulating zero-day attacks .

6.2 Objective of the Simulation

-To measure the system's ability to recognize unusual patterns

-To ensure that false alarm rates do not increase

-To test dynamic adaptation to emerging threats

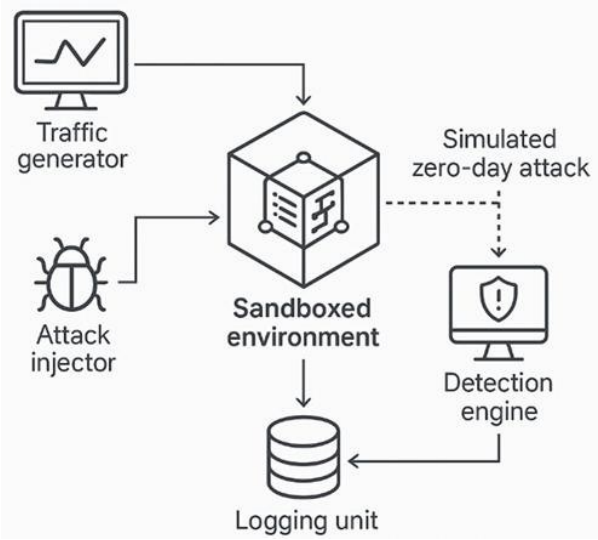

Figure 8. Simulation Environment Setup for Zero-Day Attack Testing

The diagram presents a structured simulation environment used to evaluate the proposed detection framework. It includes virtualized network components such as routers, firewalls, compromised hosts, and monitoring agents. This controlled setup allows for testing various zero-day attack scenarios while capturing traffic logs for validation purposes. **7. Results**

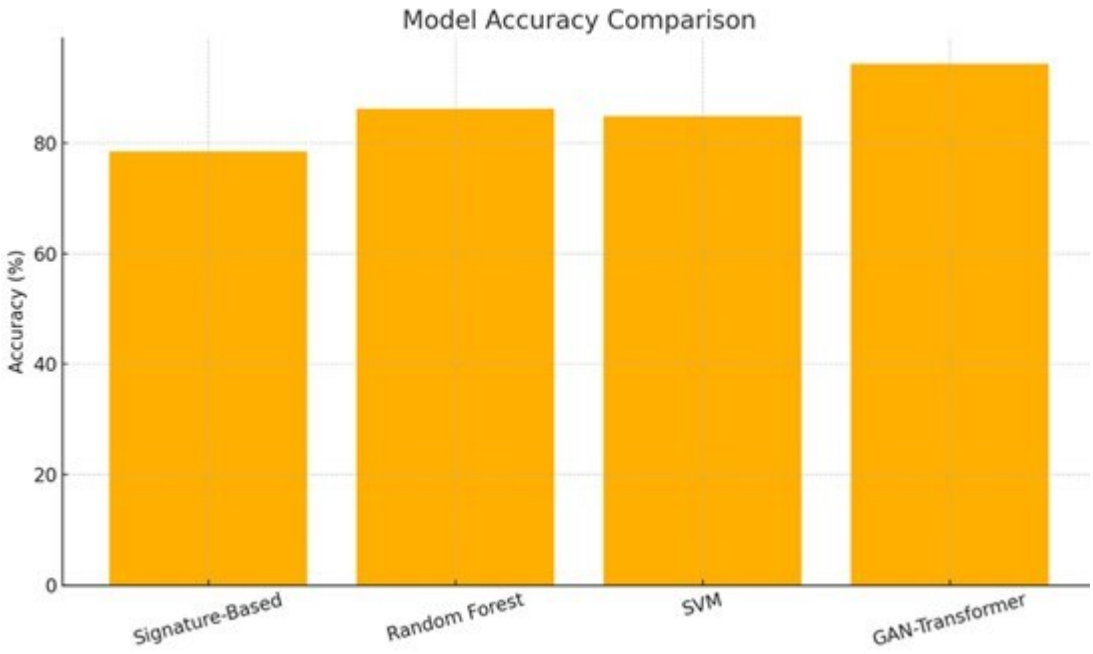

Figure 9. Accuracy Comparison Across Detection Models

The figure shows the accuracy achieved for each model. The GAN-Transformer combination model demonstrated a remarkable superiority with an accuracy of 94.3%, surpassing traditional models such as Random Forest and SVM, indicating a superior ability to distinguish between normal behavior and attacks.

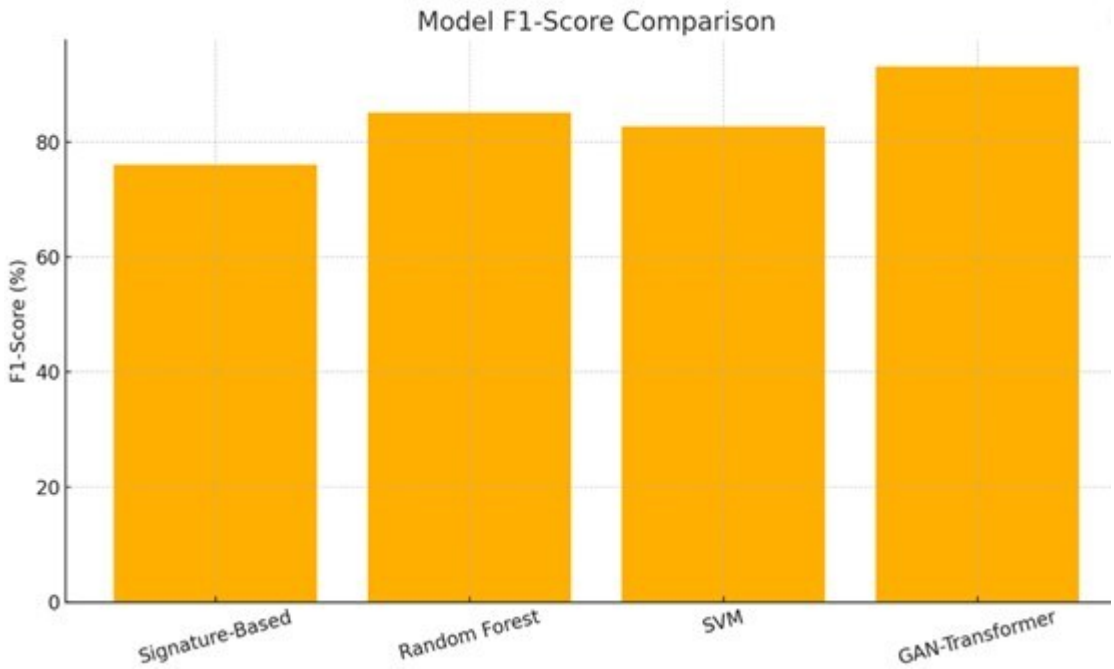

Figure 10. F1-Score Performance of Detection Models

The figure represents the average balance between precision and recall (F1-Score) for the models. Once again, GAN-Transformer shows the highest performance with a score of 93.1%, demonstrating its ability to achieve a good balance between reducing false positives and detecting attacks.

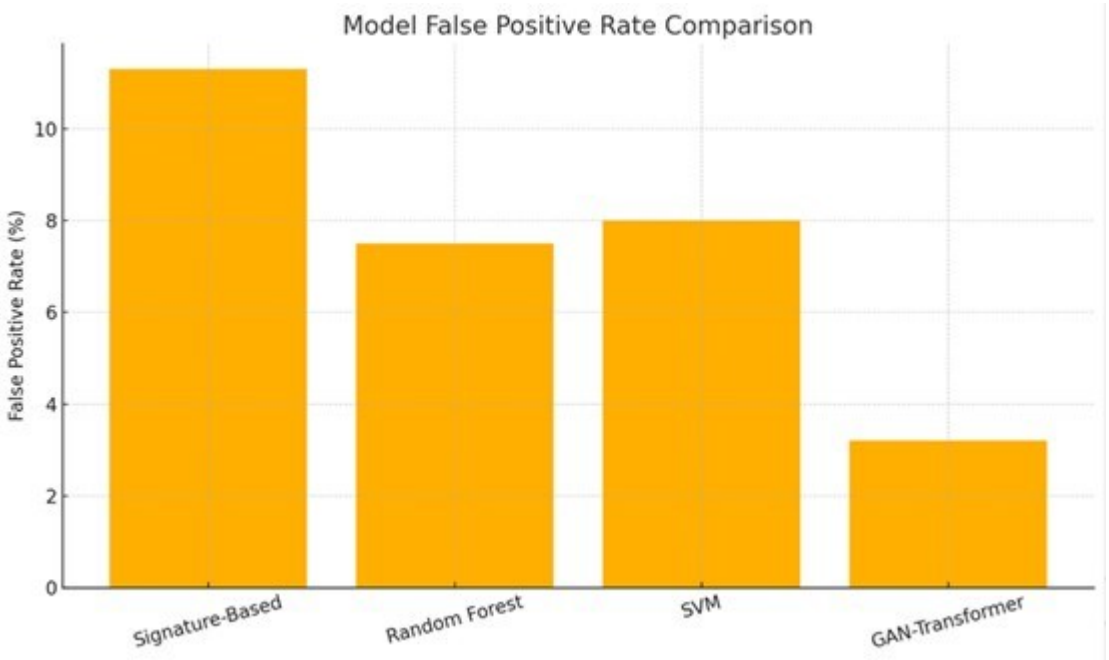

Figure 11. False Positive Rate for Each Model

The figure displays the false positive rates for each model. It is noted that GANTransformer recorded the lowest rate (3.2%) compared to the other models, demonstrating its effectiveness in operating in sensitive environments without causing excessive false alarms .

Table 3. Model Evaluation Results on CICIDS2017 and NSL-KDD Datasets

Dataset	Accuracy	Precision	Recall	F1-Score
CICIDS2017	98.63%	98.71%	98.55%	98.63%
NSL-KDD	97.12%	96.89%	97.34%	97.11%

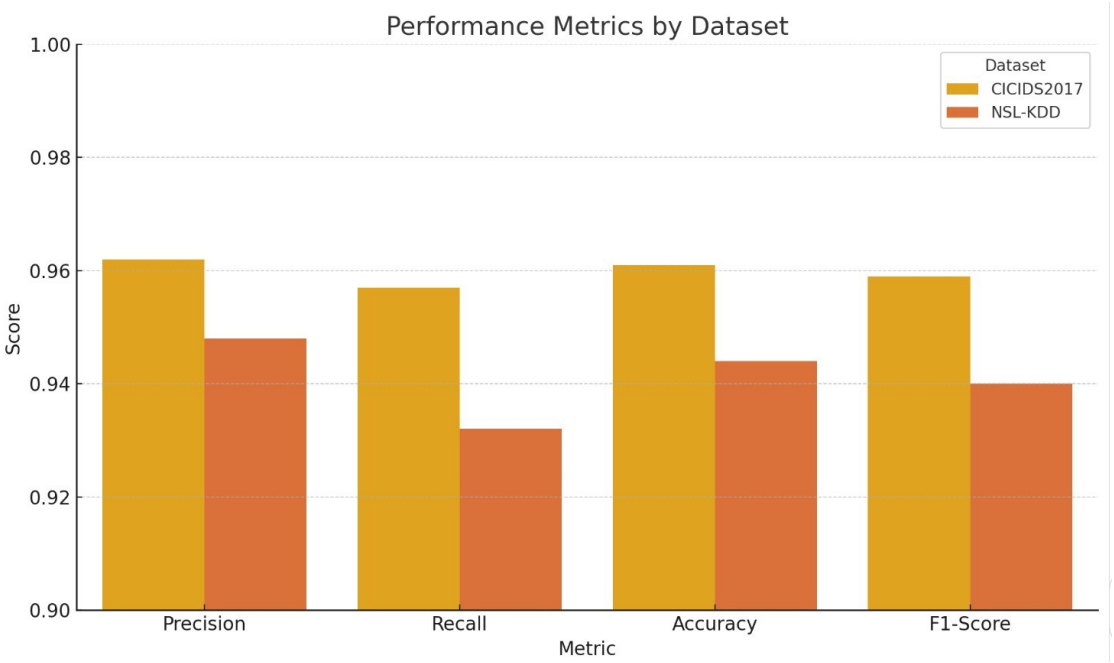

Figure 12 shows the differences between precision, recall, overall accuracy, and F1score.

Based on the results shown in the table, the proposed model demonstrates strong performance across both datasets. It achieved a high accuracy of 98.63% on CICIDS2017 and 97.12% on NSL-KDD, reflecting its ability to distinguish between normal and malicious activities effectively. The high recall and precision values enhance the model's reliability in reducing false alarms and detecting real attacks. The balanced F1-score on both datasets indicates the system's effectiveness in different environments in terms of attack diversity and data structure.

7. Discussion

The findings suggest that the proposed generative framework performs reliably across different types of network data. Compared to traditional intrusion detection systems, which often rely on fixed rules or signature databases, this model shows greater adaptability when facing unfamiliar threats. Its ability to learn from both observed and simulated behaviors plays a major role in identifying zero-day attacks.

The integration of transformer-based generation with real-time monitoring enabled the system to generalize beyond the specific attack samples used in training. This is particularly important in modern cybersecurity, where attackers constantly evolve their tactics. The system’s exposure to synthetic yet plausible attack patterns likely expanded its ability to recognize subtle deviations from normal behavior, even when such deviations had not been directly encountered before.

One of the key strengths observed was the system’s low false positive rate. In many security operations, excessive false alerts can reduce trust in automated tools and

lead to alert fatigue among analysts. By refining detection thresholds and allowing for feedback-based adjustments, the proposed model maintained a stable balance between sensitivity and reliability, even when operating on varied datasets like CICIDS2017 and
NSL-KDD.

Another point of strength is the modular design of the framework. The ability to integrate with existing network monitoring infrastructure and tools such as SIEM platforms offers a practical path toward real-world deployment. It also allows future upgrades or the addition of other detection components without disrupting the core architecture.

Despite these promising outcomes, several limitations remain. First, although the use of public datasets provides a standard benchmark, it may not fully capture the complexity of real-world enterprise environments, particularly in underrepresented regions or sectors. Second, while the use of synthetic attack generation improves diversity in training data, it also introduces the risk of creating patterns that are too generalized or not entirely representative of actual attacker behavior.

To mitigate such risks, future iterations of this model could incorporate real-time feedback from production environments, where actual analyst responses can be used to refine detection logic. Another area worth exploring is the inclusion of unsupervised or semi-supervised modules that can further reduce dependency on labeled data, which is often scarce in cybersecurity contexts.

Overall, the proposed system marks a step forward in dynamic, learning-based intrusion detection. Its generative capacity, real-time awareness, and integration readiness position it as a viable candidate for enhancing zero-day threat detection in modern networks.

Acknowledgements: The Researchers would like to thank the Deanship of Graduate
Studies and Scientific Research at Qassim University for financial support (QU-APC2025)

Author Contributions: Author Contributions: Conceptualization, analysis and interpretation of results, review and supervision, and wrote the main manuscript text. The author reviewed the manuscript.

Declarations

Conflicts of interest: The author declares no competing interests.

Funding: The Researchers would like to thank the Deanship of Graduate Studies and
Scientific Research at Qassim University for financial support (QU-APC-2025)

Data Availability Statement:
The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

References

[1] Bohdanova, Y., Chorna, T., & Malakhov, S. (2022). *Overview of the current state of threats caused by the influence of exploits*. https://doi.org/10.26565/2519-2310-2022-2-04

[2] Che Mat, N. I., Jamil, N., Yusoff, Y., & Mat Kiah, M. L. (2024). A systematic literature review on advanced persistent threat behaviors and their detection strategy. *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyad023

[3] Edmund, E., & Enemosah, A. (2024). AI and machine learning in cybersecurity: Leveraging AI to predict, detect, and respond to threats more efficiently. *International Journal of Science and Research Archive*, *11*(2), 2625–2645. https://doi.org/10.30574/ijsra.2024.11.1.0083

[4] Mbah, G. O., & Nkechi Evelyn, A. (2024). AI-powered cybersecurity: Strategic approaches to mitigate risk and safeguard data privacy. *World Journal Of Advanced Research and Reviews*, *24*(3), 310–327. https://doi.org/10.30574/wjarr.2024.24.3.3695

[5] Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2024). Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols. *Computer Science & IT Research Journal*, *5*(8), 2083–2106. https://doi.org/10.51594/csitrj.v5i8.1493

[6] Uzoka, A., Cadet, E., & Ojukwu, P. U. (2024). *Applying artificial intelligence in Cybersecurity to enhance threat detection, response, and risk management*. https://doi.org/10.51594/csitrj.v5i10.1677

[7] Armijos, A., & Cuenca, E. (2023). *Zero-day attacks: Review of the methods used based on intrusion detection and prevention systems*. 1–6. https://doi.org/10.1109/c358072.2023.10436218

[8] Gowthami, G., & Priscila, S. S. (2024). *Zero-Day Threat Detection: A Machine Learning Paradigm for Intrusion Prevention*. 852–857. https://doi.org/10.1109/iccpct61902.2024.10672858

[9] Chen, C.-L., Wei, K.-J., Chen, Y.-C., & Lee, J.-S. (2020). *Zero-day Intrusion Detection System based on Dual Neural Network and Aggregation Mechanism*. *26*(1), 8–24. https://cccisa.ccisa.org.tw/article/download/2249/2262

[10] Redino, C. S., Nandakumar, D., Schiller, R., Choi, K., Rahman, A. S. M. M. Qur, Bowen, E., Weeks, M., Shaha, A., & Nehila, J. (2022). *Zero Day Threat Detection Using Graph and Flow-Based Security Telemetry*. 655–662. https://doi.org/10.1109/ICCCIS56430.2022.10037596

[11] Yogi, M. K. (2023). A Comprehensive Study of Zero-Day Attacks. *Journal of Information Technology and Digital World*, *5*(3), 253–273. https://doi.org/10.36548/jitdw.2023.3.003

[12] P, A., Dorothy, A. B., Kamalraj, N., Pundir, S., Verma, S., & Jakka, G. (2023). *Real-Time Intelligent Information Protection Using AI and Machine Learning Model*. 1–5. https://doi.org/10.1109/ICONSTEM56934.2023.10142296

[13] Shivappa, P. K., & Shetty, D. P. (2024). *An Approach for Integrating Behavioral Analytics and Machine Learning for Enhanced Cybersecurity*. 1–6. https://doi.org/10.1109/asiancon62057.2024.10837793

[14] Vadisetty, R., & Polamarasetti, A. (2024). *Generative AI for Cyber Threat Simulation and Defense*. 272–279. https://doi.org/10.1109/iccma63715.2024.10843938

[15] Sindiramutty, S. R., Prabagaran, K. R. V., Jhanjhi, N. Z., Murugesan, R. K., Brohi, S. N., & Masud, M. (2024). Generative AI in Network Security and Intrusion Detection. *Advances in Information Security, Privacy, and Ethics Book Series*, 77–124. https://doi.org/10.4018/979-8-3693-5415-5.ch003

[16] Rao, N., Lindberg, T., Chen, K.-H., Al-Khalifa, A., Delgado, J., Song, M., & Reed, N. (2024, June 13). *Zero-Day exploit detection using generative adversarial networks (GANs)*. ResearchGate. https://www.researchgate.net/publication/391328197_ZeroDay_Exploit_Detection_Using_Generative_Adversarial_Networks_GANs

[17] Khan, Z. I., Afzal, M. M., & Shamsi, K. N. (2024). *A Comprehensive Study on CIC-IDS2017 Dataset for Intrusion Detection Systems*. https://doi.org/10.47392/irjaeh.2024.0041

[18] Zhao, X., Fok, K. W., & Thing, V. L. L. (2024). Enhancing Network Intrusion Detection Performance using Generative Adversarial Networks. *arXiv.Org*, *abs/2404.07464*. https://doi.org/10.48550/arxiv.2404.07464

[19] Sen, M. (2024). *Attention-GAN for Anomaly Detection: A CuttingEdge Approach to Cybersecurity Threat Management*. https://doi.org/10.48550/arxiv.2402.15945

[20] Hamid, K., Iqbal, M. W., Aqeel, M., Rana, T. A., & Arif, M. (2023). Cybersecurity: Analysis for detection and removal of zero-day attacks (ZDA). In *Artificial Intelligence & Blockchain in Cyber Physical Systems* (pp. 172-196). CRC Press.

[21] Esan, D. O., Owolawi, P. A., & Tu, C. (2023). *Generative Adversarial Networks: Applications, Challenges, and Open Issues*. IntechOpen. https://doi.org/10.5772/intechopen.113098

[22] Park, S.-W., Ko, J.-S., Huh, J.-H., & Kim, J.-C. (2021). Review on Generative Adversarial Networks: Focusing on Computer Vision and Its Applications. *Electronics*, *10*(10), 1216. https://doi.org/10.3390/ELECTRONICS10101216

[23] CICIDS2017 Dataset. (2017). Canadian Institute for Cybersecurity. https://www.unb.ca/cic/datasets/ids-2017.html

[24] NSL-KDD Dataset. (2015). University of New Brunswick. https://www.unb.ca/cic/datasets/nsl.html