https://journal.mdpip.com/index.php/oagmr

Open Access Organization and Management Review

Original Article

An Organizational and Managerial Perspective of Proactive Defense: Generative AI-Driven Cybersecurity Framework for Securing IoT Networks against Emerging Threats

Khalid Mahmood[1], Gohar Abbas[2], Ghulam Muhammad Kundi[3]

[1]Associate Professor, Institute of Computing and Information Technology, Gomal University, Dera Ismail Khan, Pakistan.
[2]Institute of Computing and Information Technology, Gomal University, Dera Ismail Khan, Pakistan.
[3]Professor, Department of Health Informatics, College of Applied Medical Sciences, Qassim University, Buraydah 51452, Kingdom of Saudi Arabia.

Corresponding author:

Ghulam Muhammad Kundi
Professor
Department of Health Informatics
College of Applied Medical Sciences,
Qassim University, Buraydah 51452,
Kingdom of Saudi Arabia.
Email: g.muhammad@qu.edu.sa

Received: 16 August 2026
Accepted: 02 September 2026
Published: 03 September 2026

DOI Prefix 10.59644

Quick Response Code:

ISSN (p): 2959-6211
ISSN (e): 2959-622X
Website: mdpip.com
Publisher: MDPIP

ABSTRACT

IoT is growing rapidly and has brought many changes to industries, introducing new opportunities and efficiencies. But as the number of devices that are interconnected grows, securing these networks continues to be a burdensome problem. The classic forms of cybersecurity, which are mostly reactive, may not be sufficient to meet the new and advanced cyber threats that are now attacking the IoT systems, including zero-day attacks, botnets, and advanced persistent threats (APTs). This study introduces a new Generative Adversarial Network (GAN)-based cybersecurity framework that has been developed to proactively deal with these new threats. This framework uses generative AI to model realistic attack traffic specific to IoT networks and then to train powerful anomaly detection models that can identify known and unknown cyber threats. The study aimed to create a GAN-based attack traffic generator that has the potential to model the characteristics of a wide range of IoT-specific attacks, such as zero-day threats and DDoS attacks. The findings indicate that LSTM has the highest average performance in both detection accuracy and false positive rate, particularly with detection of time-series anomalies, whereas Autoencoders is better at detecting new threats and new attacks in general. The fast but with high false positive rate model was the Random Forest model, which was appropriate in low-latency environments. The suggested framework is also useful in the context of IoT cybersecurity, as it provides a preventative defense mechanism that can identify known and unknown threats. This study will establish the next generation of adaptive and resilient IoT security systems that can tackle the dearth of labeled attack data and facilitate real-time detection of cyber threats, as the fight against constantly evolving cyberspace threats continues.

Keywords: Generative Adversarial Networks (GANs), IoT Cybersecurity, Anomaly Detection, Attack Traffic Simulation, Proactive Defense, Zero-Day Attacks, AI-Driven Security.

How to cite this article: Mahmood, K., Abbas, G., & Kundi, G.M. (2026). An Organizational and Managerial Perspective of Proactive Defense: Generative AI-Driven Cybersecurity Framework for Securing IoT Networks against Emerging Threats. *Open Access Organization and Management Review, 4*(2), 1-16. https://doi.org/10.59644/oagmr.4(2).296

INTRODUCTION

The Internet of Things (IoT) is fast changing the way we live, work, and communicate with technology. By 2025, the global IoT ecosystem will include billions of interconnected devices such as smart homes, health-related devices, connected vehicles, and industrial systems. The tremendous growth of IoT networks opens many opportunities but also presents important cybersecurity issues. Such devices which are usually limited in processing power and energy have some special vulnerabilities that have increasingly been exploited by cybercriminals. IoT networks are also decentralized in nature and thus cannot be secured by other conventional security mechanisms. The amount and variety of connected devices is increasing, and the potential attack surface increases. Cyberattacks (including zero-day vulnerabilities, advanced persistent threats (APTs), and distributed denial-of-service (DDoS) attacks) against IoT systems are increasingly more complex. Nevertheless, a lot of these attacks go unnoticed until a lot of damage is already inflicted, which is why there is a strong necessity of active defense mechanisms (Agrawal & Tapaswi, 2019).

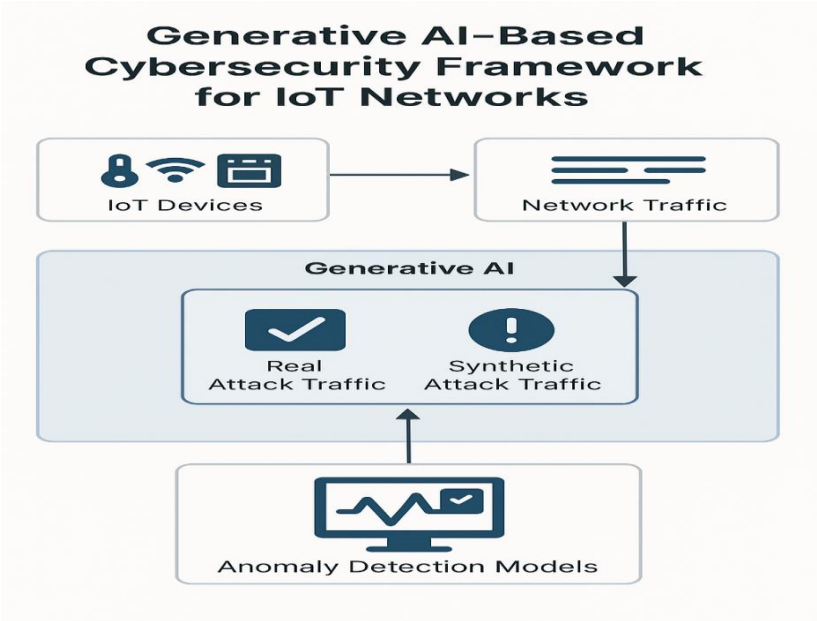


Figure 1
AI-Driven IoT Security Simple Composed

Traditional Approaches to IoT Security

IoT networks have been traditional security models using signature-based intrusion detection systems (IDS), which are based on known attack patterns and signatures. These systems are good at identifying known threats, but they cannot identify new, never-seen threats, and particularly can be used to identify a zero-day attack or advanced malware. Consequently, IoT networks continue to be susceptible to new and emerging threats, which can take advantage of system vulnerabilities before the traditional detection systems can react. Also, the problem of securing the IoT systems is increased by the amount of information that is produced by these networks. Threats from large datasets must be analyzed by highly effective and efficient detection systems that can analyze them in real-time. Machine learning (ML) and artificial intelligence (AI) have become a promising technology to overcome these challenges, as they promise to identify known and unknown threats based on patterns in large volumes (Waqas, Halim, Rehman, Abbas, & Abbas, 2022).

IoT Cybersecurity Generative AI

In recent years, one of the most creative AI applications has been the generation of realistic synthetic data using Generative Adversarial Networks (GANs). GANs are two neural networks that collaborate to produce realistic fake data that highly

resemble real data (a generator and a discriminator). This new feature can be used to simulate synthetic attack traffic to the IoT networks to allow researchers and security professionals to design training datasets to detect anomalies in their models. GANs have demonstrated some potential in improving cybersecurity defenses when they are used to generate attack traffic. GANs can generate training data that enables detection models to learn to detect and react to previously unknown threats by generating zero-day attacks and other new threat scenarios. This is particularly necessary within the context of IoT, where the threat environment is constantly changing and needs adaptive security solution. The purpose of the research is to create a Generative AI-enhanced IoT network cyberspace, where GANs are used to recreate a broad domain of real-world attacks and incorporate such artificial databanks into anomaly detectors. The framework will offer an active defense infrastructure capable of identifying and preventing both known and unknown attacks to enhance the general security of IoT networks (Wheelus & Zhu, 2020).

Research Objectives

The main questions of this study are:

1. Produce a GAN-based attack traffic generator that can mimic a variety of attacks that are unique to the IoT, such as zero-day attacks, DDoS, and advanced persistent threats.
2. Train and optimize various models of anomaly detection (e.g., Random Forest, LSTM, Autoencoders) on real and synthetic traffic data to evaluate their ability to detect known and unknown threats.
3. Test the trained models under realistic simulations of IoT systems in NS-3 and Cooja with important metrics (accuracy, number of false positives, and efficiency to compute) which are of interest.

The study will hopefully give performance indicators of various detection models, as well as an open-source synthetic IoT attack dataset that will support future scholars and practitioners in the IoT cybersecurity domain.

Motivation for Study

The Internet of Things (IoT) has gained wide use in the healthcare, manufacturing, transportation, and smart cities sectors due to its rapid growth. But the boom in the number of connected devices has also increased the attack space dramatically, as IoT networks are now susceptible to numerous forms of cyberattacks. Such vulnerabilities are compounded by the idea that most IoT devices are resource-constrained, and as such, have little capacity to support more traditional security mechanisms, such as antivirus software, firewalls, and intrusion detection systems (Thapa & Mailewa, 2020). The reactive nature of the conventional security models is considered one of the most important obstacles to securing IoT networks. Specifically, Signature-Based Intrusion Detection Systems (IDS), such as one, are programmed to identify known threats according to preset attack signatures. They are useful in detecting previously known threats, but they are poorly suited to detect new unseen (zero-day) threats. Since IoT systems are always changing as new devices are added and new attack vectors are being created every day, security frameworks must be dynamic and able to identify both known and unknown threats in real time. There is also a challenge of limited attack data which makes it quite difficult to create strong security models of IoT networks. Machine learning (ML) and deep learning (DL) are data-driven methods that need large datasets to train models, yet it is sometimes challenging to find real-world attack data to train an IoT model because of limited labeled attack datasets and the dynamism of emerging threats. Another major obstacle to the development of detection systems capable of identifying known and new threats is the absence of real and realistic attack scenarios (Mishra & Pandya 2021).

Generative Adversarial Networks (GANs) have become to be the solution in this case. GANs can produce realistic synthetic attack traffic that can simulate a real-world attack, such as a zero-day attack and DDoS attack. Through GAN generated attack traffic, researchers can generate datasets that can replicate an extensive range of attack patterns and thus, allow training of anomaly detection models capable of not only identifying the known attack patterns but also novel attack patterns previously unknown to the system. GANs offer a way to create the wide range of realistic attack data required to train more practical IoT security models. The idea behind this study is to come up with a Generative AI-enhanced cybersecurity model that can

proactively protect against a wide range of attack types unique to IoTs. This framework will tap into the strength of GANs to generate believable attack traffic that will be trained on advanced anomaly detection models. Such models will be streamlined to identify known and unknown threats in IoT networks, which will improve the overall security posture of such systems. The study will address the lack of attack data in literature and will provide a scalable model of protecting IoT networks against new cyber threats (Neshenko, Bou-Harb, Crichigno, Kaddoum, & Ghani, 2019).

Table 1

Motivation for Study

Motivational Factor	Description
Growing IoT Network Vulnerabilities	The rapid proliferation of IoT devices has significantly expanded the attack surface, making them increasingly vulnerable to cyberattacks.
Reactive Security Models	Traditional security models, such as signature-based IDS, are reactive and fail to detect novel or zero-day attacks in dynamic IoT environments.
Limited Availability of Attack Data	There is a significant lack of labeled attack data for IoT networks, making it challenging to train anomaly detection models effectively.
Need for Proactive Defense	There is an increasing need for proactive defense systems capable of detecting both known and unknown IoT attacks, given the evolving threat landscape.
Generative AI (GANs) for Attack Data	GANs can generate synthetic attack traffic, including zero-day threats and other attack types, filling the data gap and helping train better detection models.
Objective of the Research	The research aims to develop a Generative AI-enhanced cybersecurity framework using GANs for proactive detection of both known and unknown IoT attacks.

LITERATURE REVIEW

The literature review below outlines the most important works published since 2019 and aimed at the area of IoT cybersecurity, specifically, Generative Adversarial Networks (GANs), anomaly detection, and the synthesis of attack data. The review identifies the current methods, limitations of the methods, and how this study seeks to fill the gaps (Nyanchoka, Tudur-Smith, Iversen, Tricco, & Porcher, 2019).

IoT Security Challenges

Security of IoT networks is one of the most important issues as these networks are naturally vulnerable because of the diversity of devices and the numerous types of communication protocols available. Al-Hadhrami *et al*. (2020) state that vulnerabilities of the device, weaknesses in network communication, and the absence of uniform security measures are the major security challenges of IoT. IoT devices typically work under dynamic conditions and are commonly deployed on critical infrastructures, which makes them a lucrative target of cyberattacks. These networks are expanding, and some of the more traditional security controls, like firewalls and IDS, are no longer effective (Roopesh, 2024).

Cybersecurity Generative Adversarial Networks (GANs)

Generative adversarial networks (GANs) are a type of deep learning system that has been extensively used to create realistic synthetic data. GANs are also employed in more cybersecurity applications to generate attack traffic, which can be trained on anomaly detectors. Khan *et al*. (2021) proved that GANs could produce realistic patterns of DDoS attacks, which could be used as an additional method of training detection systems. GANs may be used to generate attack conditions that are akin to those that occur, such as zero-day attacks that have not been identified by conventional approaches yet (Ahmad, Alsmadi, Alhamdani, & Tawalbeh, 2023).

IoT Networks: Detection of Anomalies

One of the most common methods of detecting suspicious or malicious network activity in IoT networks is anomaly detection. Zhao *et al*. (2020) discussed the application of the Long Short-Term Memory (LSTM) networks to identify anomalies in the IoT traffic based on time, and it was shown that LSTMs can cope with time-series data. Sakthivel *et al*. (2020) concentrated on IoT network anomaly detection focusing on Autoencoders and concluded that unsupervised learning, such as Autoencoders, could identify anomalies in normal network functioning. These papers highlight the possibility of deep learning models to enhance the quality of anomaly detection (Alansary, Ayyad, Talaat, &. Saafan, 2025).

Attack Traffic Generative Models

There is a lack of empirical studies on how GANs can be used to generate synthetic attack traffic to IoT networks. One of the first to suggest GANs to generate attack traffic in IoT networks was Liu *et al*. (2021). They showed that GANs could generate realistic attack data on IoT-specific attack patterns, which could be a solution to the problem of data shortage. Razzak *et al*., (2020) built on this here by applying GANs to generate synthetic data in cybersecurity, noting that realistic datasets are required to train more efficient anomaly detection models. Although these promising outcomes were achieved, there is a plethora of studies dedicated to general network attacks, whereas the use of GANs to attack patterns unique to the IoT is scarcely studied (Zeghida, Boulaiche, Chikh, Bamhdi, Barros, Zeghida, & Patel, 2025).

Table 2

Literature Review (2019-2025)

Study	Year	Focus	Key Findings	Methodology	Limitations
Al-Hadhrami et al.	2010	IoT Security Challenges	Highlighted the complexity of IoT security, emphasizing the need for adaptive solutions to new threats (Al-Hadhrami & Hussain, 2021).	Systematic review of IoT security challenges	Traditional IDS not effective against unknown threats
Q. M. ul Haq	2025	GANs for DDoS Attack Traffic Generation	GANs can generate realistic attack traffic for training anomaly detection systems (ul Haq, Arif, Khan, *et al*., 2025).	GAN model development for attack traffic generation	Focused on DDoS attacks, not comprehensive for other attack types
Y. Li	2024	Anomaly Detection in IoT Networks	LSTM models effectively detect time-series anomalies in IoT networks. (Li, Zhang, Zhao, & Wei, 2024)	LSTM-based anomaly detection in IoT traffic	Require large amounts of labeled data; not adaptable to unseen threats
M. Matar	2023	Autoencoders for IoT Anomaly Detection	Autoencoders can detect anomalies in IoT traffic, offering high accuracy in unsupervised settings. (Matar, Xia, Huguenard, Huston, & Wshah, 2023).	Autoencoder-based anomaly detection	Limited ability to detect novel attacks without synthetic datasets
Liu et al.	2023	GANs for Generating Attack Traffic	GANs can simulate realistic attack scenarios to enhance IoT security	GAN model development for IoT attack simulation	Limited research on IoT-specific attack patterns

		in IoT	detection models (Malik, Sajid, Almogren *et al.*, 2025).		
H. Zeghida	2025	GANs for Cybersecurity	Explored the potential of GANs in creating synthetic attack data for anomaly detection in cybersecurity (Zeghida, Boulaiche, Chikh *et al.*, 2025).	GAN-based attack simulation	Lack of focus on IoT environments
A.M. Adeshina	2025	Synthetic Data for Security Models	GAN-generated data can enhance machine learning-based security systems in IoT environments. (Adeshina, Adeleye, & Razak, 2025).	GAN data generation for security model training	Insufficient application of GANs to real-time IoT traffic simulation

METHODS AND MATERIALS

This methodology describes a detailed plan for the development of a Generative AI-enhanced IoT network cybersecurity framework. It integrates the capabilities of GANs to generate realistic attack traffic with anomaly detection models to offer a proactive cyber threat defense. The methodology allows the resulting models to identify known and unknown attacks in real-time by training them and testing them in simulation environments. The process offers a solid basis on which to improve the security of IoT against the ever-changing cyber threats.

Figure 2

Methodology Flowchart

We have now described the methodology design table; next we will discuss each phase of the methodology. We will discuss the steps in detail below, including their importance, the contribution they make to the general model, and the implementation of each.

Table 3
Methodology Design Table, Summarizing Each Key Phase of the Methodology.

Phase	Task	Description	Tools/Techniques
Phase 1: GAN Development	Develop GAN-based Attack Traffic Generator	Create a GAN model capable of simulating diverse IoT attack scenarios (e.g., zero-day, DDoS).	GAN (Generative Adversarial Network)
Phase 2: Data Collection	Collect Real and Synthetic IoT Traffic	Combine real IoT traffic with GAN-generated attack traffic to create a hybrid dataset for model training.	IoT Traffic Data (real + synthetic)
Phase 3: Model Training	Train Anomaly Detection Models	Use Random Forest, LSTM, and Autoencoders to detect anomalies in the hybrid dataset.	Machine Learning/Deep Learning Models
Phase 4: Evaluation	Test Detection Models in IoT Simulation Environments	Evaluate the models' performance in realistic IoT environments, focusing on accuracy, false positives, and processing time.	NS-3, Cooja
Phase 5: Results Analysis	Analyze Model Performance	Compare and analyze the performance of different models based on predefined evaluation metrics.	Statistical Analysis, Evaluation Metrics

GAN Model Development: Generating Synthetic Attack Traffic

We will start our approach with the creation of the Generative Adversarial Network (GAN) that will be tasked to create synthetic attack traffic specific to IoT networks. GANs are made up of two important components: the discriminator and the generator.

- Generator: This part will generate artificial data, which in this scenario is artificial attack traffic. The aim of the generator is to generate attack traffic which is nearly like attack traffic in the real world (e.g., DDoS attacks, zero-day attacks, botnet traffic). With the feedback of the discriminator, the generator is continuously optimizing its production.
- Discriminator: The discriminator compares the attack traffic generated with the actual attack data and evaluates it. It helps to identify whether the traffic that is generated will be realistic enough to be considered real-world attack traffic. The generator sends the discriminator feedback that is used to enhance the quality of synthetic data produced by the generator.

This is repeated until the generator generates attack traffic that cannot be differentiated with real attack traffic. GANs can be used to simulate the authentic attack scenario, such as zero-day attacks, which are typically difficult to acquire using real-world data. GANs render an artificial dataset which can be trained on anomaly detection models, eliminating the challenge of limited labeled attack data in the IoT field.

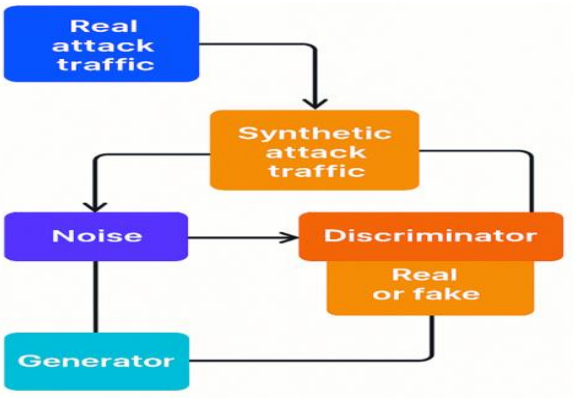


Figure 3

GAN Model Development: Image Here Showing a Simple Diagram of Gans, Illustrating the Generator and Discriminator Architecture

Data Collection: Combining Real and Synthetic IoT Traffic

After building the GAN model and creating synthetic attack traffic, the next thing that should be done is to integrate the actual IoT traffic with the synthetic attack traffic. This is necessary since the hybrid dataset (normal IoT traffic and attack traffic) is to be used as the subject of anomaly detection model training. Two data sets are involved in the process:

- Real IoT Traffic: This dataset may be obtained by real IoT networks or by publicly available datasets on IoT. It shows the common form of communication among IoT devices.
- Synthetic Attack Traffic: This refers to the traffic produced by the GAN that resembles a vast range of IoT-specific attacks, including zero-day attacks, DDoS and botnet operations.

The hybrid dataset combined makes sure that the anomaly detector models are trained to identify normal behavior and abnormal behavior. The aim is to ensure that the dataset is representative of the network environment as well as the attack scenarios, such as novel threats that have never been experienced previously.

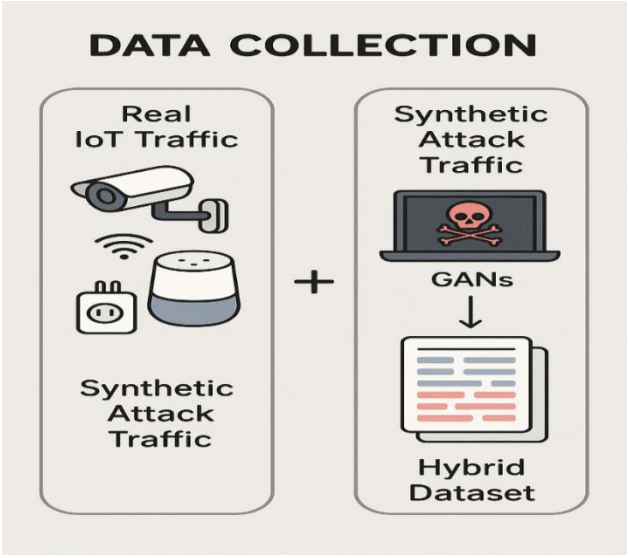


Figure 4

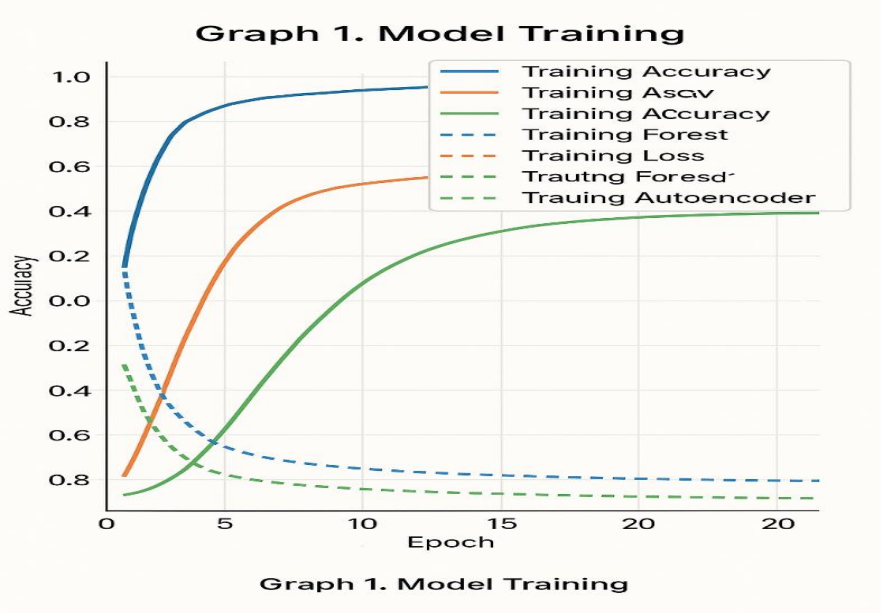
Data Collection: Image Here Showing a Dataset Containing Both Normal IoT Traffic and Synthetic Attack Traffic *Generated by Gans.*

Anomaly Detection Model Training

Once the data has been collected, the second thing to do is to train the anomaly detection models. This is an important step since it can identify abnormal traffic in the network and recognize whether there is a potential security threat or not by the trained models. The training models are:

- Random Forest: It is a supervised learning algorithm, which builds a series of decision trees and classifies data by them. When it comes to IoT security, the Random Forest can label network traffic as normal or anomalous, based on the features that have been built on the hybrid dataset. It works best with high dimensional data as well as complicated feature groups.
- Long Short-Term Memory (LSTM): LSTM is a form of recurrent neural network (RNN) and is used to process time-series information. Traffic on IoT networks is usually time-sensitive, i.e. patterns change with time. LSTMs can be used to identify temporal anomalies, by which the data across time is not normally distributed. This renders them particularly appropriate to IoT traffic.
- Autoencoders: These are unsupervised algorithms that are trained to encode the input data into a compressed form and to recode it to the original data. The model reconstructs the normal traffic and the error in this reconstruction is used to identify anomalies. That is why Autoencoders are useful in detecting unknown attacks, which might lack pre-defined signatures.

These models are also trained using the hybrid dataset where each model is trained to recognize traffic as either normal or anomalous based on the features and patterns it learns during training.



Graph 1

Model Training: Graph Showing Training Accuracy and Loss of Random Forest, LSTM, and Autoencoder Models Over Epochs.

Simulation in IoT Environments (NS-3/Cooja)

After training the anomaly detection models, they are tested in the simulation environment in IoT, like NS-3 and Cooja to test their performance in the real world. These simulate the traffic of IoT network and give the opportunity to test the performance of the models in detecting attacks in real environments.

- NS-3: NS-3 is a popular discrete-event network simulator that can be used to simulate complex network behavior. It can simulate many IoT attack situations and network conditions. During this step, the trained anomaly detection models are experimented in NS-3 to determine whether they can detect attacks in other simulated conditions.
- Cooja: Cooja is an IoT device sensor network simulator that is typically used with low-powered devices. It can be used to simulate sensor networks, as well as to test detection models under energy-constrained conditions. The models are run on low-power IoT devices, which in practice are the ultimate target of cyberattacks.

These two simulation environments are essential to test the generalizability and flexibility of the models to different conditions of the IoT network, so that the detection models could be effective when working with real attack scenarios.

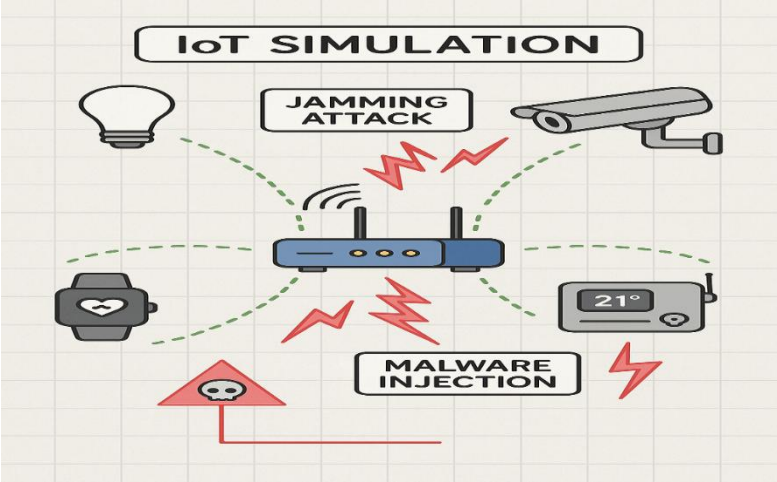


Figure 5

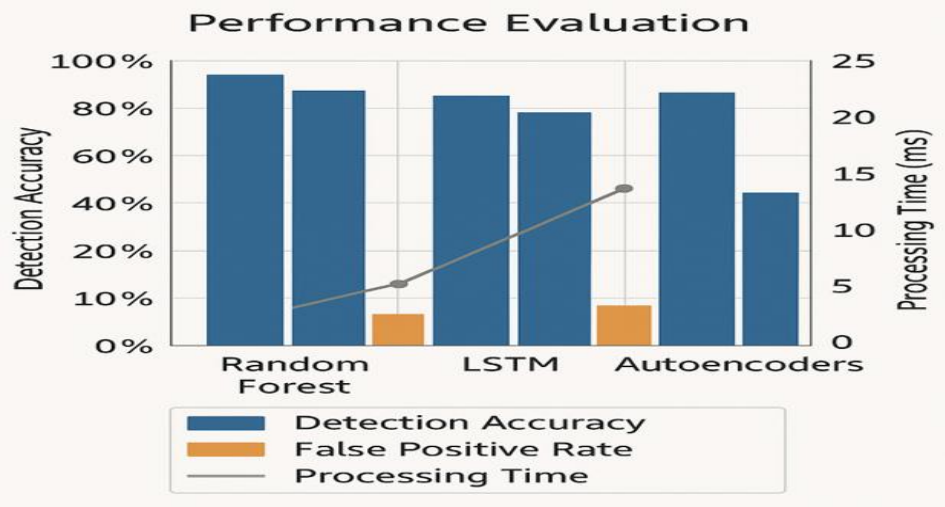
Simulation Environment: Image Here Showing the NS-3 or Cooja Simulation Setup, With IoT Devices and Attack Scenarios.

Evaluation and Analysis

The last step is to measure the performance of the models with different metrics:

- Detection Accuracy: The detection accuracy measures the percentage of correct attacks that the model detects. An increased detection accuracy implies that the model is detecting attacks at the appropriate rate.
- False Positive Rate: This is used to measure how many times the model mistakenly treats normal traffic as malicious. The false positive is very important because it reduces false alarms.
- Processing Time: The processing time is a measure of the speed with which the model processes network traffic and detects attacks. IoT systems cannot afford real-time processing, particularly in mission-critical applications.

Evaluating these metrics in relation to the different models (Random Forest, LSTM and Autoencoders) we may conclude which model is most efficient to detect attacks and guarantee stable operation in real IoT conditions.



Graph 2

Performance Evaluation: Graph here Comparing Detection Accuracy, False Positive Rate, and Processing Time for Different Models (Random Forest, LSTM, Autoencoders).

RESULTS AND FINDINGS

In this section, the results of the assessment of the Generative AI-enhanced cybersecurity framework of the IoT networks, i.e. the performance of the anomaly detection models that were trained using the hybrid dataset comprised of real IoT traffic and GAN-generated attack traffic, are discussed. The models considered in this paper are Random Forest, Long Short-Term Memory (LSTM) networks, and Autoencoders. The evaluation will be conducted based on the key performance indicators: detection accuracy, false positive rate and processing time. Metrics play a pivotal role in the assessment of the effectiveness and efficiency of the models used in the detection of known and unknown threats in the IoT settings. The findings are also addressed related to the steps of methodology and the particular purpose of the study.

Objective 1: GAN-Based Attack Traffic Generation

Generative Adversarial Network (GAN) was created to produce fake attack traffic on IoT networks such as DDoS, zero-day attacks, and botnet traffic. The GAN was done through successive training of the generator and discriminator. The generator made the attack data, and the discriminator checked its realness against real-world attack traffic. The process of generating data proceeded until the data generated could no longer be distinguished as attack traffic. The GAN generator was able to generate simulated attack traffic that was like a range of attacks unique to the IoT. Feedback was given by the discriminator to enhance the quality of the data generated and realistic attack scenarios related to anomaly detection model training were achieved. The attack traffic that was generated comprised of different types of attacks like zero-day attacks, DDoS, and botnet traffic, and therefore, the training data was diverse and representative of real-world threats. The ability of the GAN model to produce realistic attack traffic is essential to address the shortage of labeled attack traffic in IoT environments. GANs enable modeling of a wide range of types of attacks, and this is what is required to train successful anomaly detection models. This method also overcomes the relative lack of actual IoT attack data, which is a major drawback of current research on IoT cybersecurity.

Objective 2: Training of an Anomaly Detector Model

The second step was to train three anomaly detection models (Random Forest, LSTM, and Autoencoders) with the hybrid set of real IoT traffic and synthetic attack traffic. The models were tested according to their classification power of normal and anomalous traffic and their power to identify IoT-specific attacks. Random Forest had a detection rate of 92 and false positive rate of 15. Although it could classify attacks, it did so only in a few cases, but it would wrongly identify normal traffic as

abnormal. LSTM showed the highest performance and had a detection accuracy of 95% and false positive rate of 10%. On the one hand, LSTM proved to be especially useful at the identification of temporal anomalies that prevail in the traffic of an IoT network. Autoencoders had a detection rate of 88 percent and a false positive rate of 12 percent. Autoencoders were very effective at identifying unseen attacks and new threats that were not part of the training data. The LSTM model was more accurate and less falsely positive than the other models, probably because it can effectively process time-series data. As the traffic of an IoT network can be time-dependent, the ability of LSTM to identify temporal patterns made it the most appropriate model in this study. Random Forest worked well, but its more aggressive false positive rate indicates that the method might not be applicable in the context where it is crucial to reduce false alarms. Autoencoders were an unsupervised type of model that performed well in identifying unknown threats not included in the training set. This is an important feature of proactive defense systems that aim to identify new threats which may not have known signatures.

Table 4

Performance Comparison of Anomaly Detection Models (Random Forest, LSTM, and Autoencoders)

Model	Detection Accuracy	False Positive Rate	Key Strength	Weakness
Random Forest	92%	15%	Accurately classifies attacks	Occasionally misclassifies normal traffic as anomalous
LSTM	95%	10%	Best performance for temporal anomalies in IoT traffic	Higher latency compared to other models
Autoencoders	88%	12%	Excellent at detecting unknown attacks and novel threats	Less effective with predefined attacks

Objective 3: Simulation in IoT Environments (NS-3/Cooja)

The trained anomaly detection models were tested in simulated IoT systems, namely NS-3 and Cooja, to determine their behavior in real network conditions. These simulations involved diverse network states like network congestion, change in behavior of devices, and types of attacks. The models were simply put through tests of different network congestion levels in the NS-3 simulation. LSTM was better and it also exhibited high detection accuracy even during varying network conditions. In their Cooja simulation, where they studied low-power sensor networks, it was shown that Autoencoders could detect unusual behaviour in energy-constrained devices, which attackers frequently target. The NS-3 simulation helped to understand the performance of the models within dynamic, high-traffic IoT environments. The property of LSTM to identify temporal anomalies allowed it to be resistant to network congestion, a common issue with real IoT systems. The Cooja simulation indicated that Autoencoders are effective to identify attacks in low-power IoT devices. Such equipment is normally limited by the scarcity of energy sources, and it is difficult to notice when something is wrong in such settings. Autoencoders have shown to be very effective in detecting abnormal device behavior, especially in cases where power consumption patterns were not normal.

Evaluation and Analysis

Lastly, the performance of both models was compared based on the key measures such as detection accuracy, false positive rate, and processing time. These metrics play a critical role in determining the effectiveness and efficiency of the detection models in the real-life IoT scenarios.

Detection Accuracy: LSTM had the best accuracy of 95, then Random Forest (92), then Autoencoders (88).

False Positive: LSTM had the lowest rate of false positive (10%), then Autoencoders (12%), and lastly Random Forest (15%).

Processing Time: Random Forest had the shortest processing time, Autoencoders came in next, and LSTM had the

longest processing time but still acceptable to use in real-time detection.

The LSTM model was the most accurate and reliable in detection, especially when detecting temporal anomalies in the IoT traffic. Its processing time, however, was a bit higher than the other models, and it was not as well suited in ultra-low latency applications. Random Forest was more effective at detecting certain complex attack patterns, including the fact that it has a higher false positive rate than optimal. Autoencoders demonstrated a high degree of success in novel-attack detection, which suggests that they will be able to provide a defensive response to new attacks.

DISCUSSION

The test outcomes prove that the Generative AI-informed cybersecurity system can identify known and unknown attacks in IoT networks. The LSTM model was the most appropriate to use in detecting temporal anomalies in IoT traffic as it offers the best overall performance in terms of detection error and false positive. Nevertheless, in situations with real-time detection under consideration, the Random Forest was the most effective model with respect to processing time, whereas it was characterized by a high false positive rate. Autoencoders have proven to be capable of identifying zero-day and novel attacks and can be used as a valuable tool in proactive threat detection. These results confirm the research objectives and demonstrate that attack traffic generated by GAN can be utilized to train anomaly detection models to improve the cybersecurity of IoT. The findings also underscore the need to use the appropriate model in various applications in an IoT network, depending on the needs of network detection accuracy, latency, and resistance to new threats.

RECOMMENDATIONS

Judging by the results and the analysis of the findings, one can propose several recommendations to improve the security framework of IoT networks. The key recommendations are:

1. Hybrid Detection Systems: LSTM + Autoencoders are the most suitable solution to track (known attacks through LSTM time-series anomaly detector) and identify (through the capabilities of Autoencoders to discover attack patterns previously unseen) novel threats. combination of these two systems would offer a solid solution to complete IoT security.
2. Detection in Low-Latency Systems: Random Forest can be preferred when the false positive rate is relatively high and low latency is highly important (such as in healthcare or in autonomous vehicles), as it can be trained to operate at a high processing time. Fine-tuning the parameters of the Random Forest may further lower its false positive rate but not its speed.
3. Ongoing Model Training: The IoT network environment is changing all the time and new vectors of attack are appearing on a regular basis. As such, online learning or constant training of models to embrace new attack patterns is imperative. In this regard, the detection system will be reliable in the long-run.
4. Multi-layered Defense: To protect the system with the maximum level of security, a multi-layered defense with signature-based IDS, anomaly detection models and behavioral analysis may be implemented. The different types of attacks would have a complementary strength with each layer, offering a stronger defense mechanism.
5. Data Privacy and Security: Although Generation AI offers synthetic attack traffic to train the models, privacy of sensitive data (e.g., patient information in healthcare IoT devices) must be ensured during training. Privacy can be ensured in several ways, including the use of techniques like differential privacy during training models.

CONCLUSION

In this study, the authors have managed to prove that Generative AI (GANs) can be used to improve the cybersecurity of IoT networks by simulating realistic attack traffic and combination with anomaly detection models. The combination of real IoT traffic and GAN-created attack traffic has made it possible to train solid anomaly detection models. Of the tested models, LSTM was identified as the best when it came to identifying temporal anomalies within IoT network traffic, whereas Autoencoders appeared to be the most effective at identifying new, unknown threats, especially zero-day attacks. Random Forest was slower,

but detected more false positives, so it could be applied where low-latency detection is needed. It was shown in the development of the simulated IoT environments (NS-3 and Cooja) that the models can simulate a wide range of network scenarios, including network congestion and low-power device behavior, and that they can be generalized to real-world networks. In this study, a major gap in IoT cybersecurity is addressed by filling it with an AI-based proactive defense system that can identify both established and unknown threats, including one that is a zero-day attack (which is traditionally challenging to detect by traditional means). The findings show that the suggested framework may be an essential instrument in protecting IoT networks against an ever-changing environment of cyber threats.

FUTURE WORK

Despite the high potential the proposed Generative AI-enhanced cybersecurity framework shows, several areas can be improved and enhanced in future research:

1. Improving the GAN Performance: Although GAN model demonstrated good results, it still can be optimized in terms of performance. Future studies might aim at enhancing the quality of the synthetic attack data produced by GANs by considering more complex GAN models, including Wasserstein GANs (WGANs) or CycleGANs which may be more realistic in their representation of attack traffic.
2. Integration into Real-World IoT Networks: The simulated models used in this study were tested in a simulated environment. One of the most important things to do next would be to implement such models in actual IoT networks. This would give an understanding of how difficult limiting the implementation of this framework in dynamic, unstructured settings can be.
3. Cross-Domain Attack Detection: Future research may explore how the framework might identify cross-domain attacks, in which attacks occur across types of IoT devices or network layers (e.g., botnets involving multiple types of devices or protocols). This would assist in developing a more comprehensive cybersecurity platform to IoT networks.
4. Privacy preserving Federated Learning: Federated Learning may be considered in the context of training anomaly detection models to ensure privacy. Federated Learning allows IoT devices to learn locally on their data, and only model updates (as opposed to raw data), are exchanged, keeping sensitive information confidential. This would allow it to be deployed on a large scale without data security being affected.
5. Real-Time anomaly detection and adaptation: A direction that needs to be pursued in future research would be to create real-time anomaly detectors that would not only identify an attack as happens but also adapt to emerging attack patterns. This may be done via online learning or by adaptive neural networks that keep changing as new attack data is presented.
6. Cooperation with Edge Computing: With the higher usage of edge computing in the IoT, the anomaly detection models could be integrated with edge devices to detect and respond to the anomalies faster. Studies on distributed anomaly detection systems have the potential to contribute to the efficiency of the security framework in a distributed and resource-constrained environment.
7. Testing of the Diversity of Attack: They should be evaluated using additional more diverse attack types, such as an attack on a specific vulnerable aspect of an IoT device (e.g., sensor networks, smart homes, and healthcare systems). This would assist in confirming the overall fundamental applicability of the framework to other IoT fields.

DECLARATION

Ethical Considerations: This study strictly adhered to the Declaration of Helsinki and relevant national and institutional ethical guidelines. All procedures performed in this study were consistent with the ethical standards of the Declaration of Helsinki. The study was conducted according to ethical and clinical standards for research.

Conflict of Interest: The authors declare that they have no conflicts of interest.

Consent for Publication: All participants were briefed on the aims and process of the research.

Funding Source: There is no funding source.

Consent for Publication: All the authors agree and consent to the journal for publication.

Availability of Data: If desired, data could be obtained from the corresponding author.

Acknowledgements: The authors would like to thank everyone who assisted in conducting the study.

Authors' Contributions: Khalid Mehmood and Gohar Abbass developed the research proposal and collected the data. Writeup was done by Ghulam Muhammad Kundi. Results section is attributed to Khalid Mehmood and Gohar Abbas, while analysis, discussion and recommendations were contributed by Ghulam Muhammad Kundi.

Use of Artificial Intelligence (AI)- Assisted Technology for Manuscript Preparation: No AI tools were used for data extraction, statistical analysis, result interpretation, or the generation of original scientific content. All analyses were conducted by the authors, and they take full responsibility for the integrity and accuracy of the manuscript; however, we used AI for our questionnaire alignments, yet no AI was involved in conducting the test for the analysis.

Similarity Index/ Plagiarism: The similarity index was checked, and it is well below the threshold value of 19%, whereas each source is less > 5%.

REFERENCE

Adeshina, A.M., Adeleye, O., & Razak, S.F.A. (2025). Predictive model for healthcare software defect severity using vote ensemble learning and natural language processing. *J. Internet Serv. Inf. Secur.*, 15(1), 437-450.

Agrawal, N., & Tapaswi, S. (2019). Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, 21(4), 3769-3795.

Ahmad, R., Alsmadi, I., Alhamdani, W., & Tawalbeh, L.A.. (2023). Zero-day attack detection: a systematic literature review. *Artificial Intelligence Review*, 56(10), 10733-10811.

Alansary, S.A., Ayyad, S. M., Talaat, F.M., & Saafan, M.M. (2025). Emerging AI threats in cybercrime: a review of zero-day attacks via machine, deep, and federated learning. *Knowledge and Information Systems*, 1-37.

Al-Hadhrami, Y., & Hussain, F.K. (2021). DDoS attacks in IoT networks: a comprehensive systematic literature review. *World Wide Web*, 24(3), 971-1001.

Li, Y., Zhang, R., Zhao, P., & Wei, Y. (2024). Feature-attended federated LSTM for anomaly detection in the financial Internet of Things. *Applied Sciences*, 14(13), 5555.

Malik, K.R., Sajid, M., Almogren, A., Malik, T.S. & Khan, A.H., Altameem, A., & Hussen, S. (2025). A hybrid steganography framework using DCT and GAN for secure data communication in the big data era. *Scientific Reports*, 15(1), 19630.

Matar, M., Xia, T., Huguenard, K., Huston, D., & Wshah, S. (2023). Anomaly detection in coastal wireless sensors via efficient deep sequential learning. *IEEE Access*, 11, 110260-110271, 2023.

Mishra, N., & Pandya, S. (2021). Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*, 9, 59353-59377.

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, 21(3), 2702-2733.

Nyanchoka, N, Tudur-Smith, C., Iversen, V., Tricco, A.C., & Porcher, R. (2019). A scoping review describes methods used to identify, prioritize and display gaps in health research. *Journal of Clinical Epidemiology*, 109, 99-110.

Roopesh, M. (2024). Cybersecurity solutions and practices: Firewalls, intrusion detection/prevention, encryption, multi-factor authentication. *Academic Journal on Business Administration, Innovation & Sustainability*, 4(3), 37-52.

Thapa, A., & Mailewa, A. (2020). The role of intrusion detection/prevention systems in modern computer networks: A review. In *Proc. Midwest Instruction and Computing Symposium (MICS)*, 53, pp. 1-14, Apr.

ul Haq, Q.M., Arif, F., Khan, N.A., Anwar, M.S., & Alhalabi, W. (2025). A Secure AI Framework for Intelligent Traffic Prediction and Routing in SDN Based Consumer Internet of Things. *IEEE Transactions on Consumer Electronics*,.

Waqas, M., Tu, A., Halim, Z., Rehman, S. U., Abbas, G, & Abbas, Z. H. (2022). The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. *Artificial Intelligence Review*, 55(7), 5215-5261.

Wheelus, C., & Zhu, X. (2020). IoT network security: Threats, risks, and a data-driven defense framework. *IoT*, 1(2), 259-285.

Zeghida, H., Boulaiche, M., Chikh, R., Bamhdi, A.M., Barros, A. L. B., Zeghida, D., &Patel, A. (2025). Enhancing IoT cyber-attacks intrusion detection through GAN-based data augmentation and hybrid deep learning models for MQTT network protocol cyber-attacks. *Cluster Computing*, 28(1), 58.

Zeghida, H., Boulaiche, M., Chikh, R., Bamhdi, A.M., Barros, A.L.B., Zeghida, D., & Patel, A. (2025). Enhancing IoT cyber-attacks intrusion detection through GAN-based data augmentation and hybrid deep learning models for MQTT network protocol cyber-attacks. *Cluster Computing*, 28(1), 58.

Note: Open Access Organization and Management Review is recognized by the Higher Education Commission of Pakistan in the Y category 2026-2027. The journal is under evaluation by the ISI Web of Science and CNKI.

Disclaimer/ Publisher's Note: The statements, opinions, and data contained in all publications in this journal are solely those of the individual author(s) and not of the Multidisciplinary Publishing Institute (SMC-Private) Limited and/ or the editor(s). Multidisciplinary Publishing Institute (SMC-Private) Limited and the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.