SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V13I4P116

Volume 13 Issue 4, 203-211, April 2026

Original Article

Improved Generative Adversarial Network-based Ransomware Attack Detection Model with Enhanced Normalization Technique

G. Badrinath[1], Arpita Gupta[2]

[1,2]*Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, Telangana, India.*

[1]*Corresponding Author : badrinath.goteti@gmail.com*

Received: 12 January 2026 Revised: 14 February 2026 Accepted: 16 March 2026 Published: 30 April 2026

Abstract *- Generative Adversarial Network (GAN) has turned out to be one of the most devastating types of ransomware attack detection models, with enhanced normalization technique being the order of the day in most sectors. GAN methods of ransomware detection tend to be problematic in data Preprocessing, input dataset, and behavioural logs. In this paper, a better modification of GAN-based ransomware attack detection is proposed, which adds a framework such as a generator (G), discriminator (D), and auxiliary classifier (C). To achieve a better data representation, the GAN is used with Enhanced Normalization, with the enhancement of the normalization that stabilizes and reduces the occurrence of the mode collapse problem. Empirical tests reveal that the model under consideration is an improvement over traditional GAN-based and Map, instance normalization, Layer normalization, and hybrid normalization. Classifier Integration comprises the increased computational cost of adversarial training, the need for sigmoid activation, learning rate, total objective function, training, and Optimization when deploying in real-time scenarios on limited systems. Future directions will center on the optimization of lightweight flavors of the proposed model, the incorporation of federated learning as a privacy-preserving detection mechanism, and cross-domain generalization as a means of increasing protection to previously unseen ransomware families.*

Keywords *- Ransomware Attack Detection Model, Generative Adversarial Network, Enhanced Normalization, Cybersecurity, Classifier Integration.*

1. Introduction

In today's dual generative adversarial networks, ransomware has grown to be a serious cyber security issue, resulting in large financial losses and privacy violations for both individuals and businesses [1]. Encrypting users' important data and demanding decryption keys is the most damaging action of ransomware. Despite paying the ransom, customers will not be able to retrieve their data because attackers utilize Windows APIs or specially designed malicious operations to safely destroy, rewrite, or erase the original files. Furthermore, by launching secure contact with improving attack detection performance on servers, ransomware improves its flexibility and stealthiness [2]. This allows it to gather attack statistics, dynamically change configurations, and further govern the compromised computers.

The most effective protection is usually against known ransomware, and antivirus software usually uses signature-based techniques. These techniques include identifying and thwarting recognized threats by comparing attributes with those kept in a database. Even while the previously described techniques are more effective against known ransomware, they frequently fail to work against assaults that are not yet recognized. Additionally, ransomware used XSS attacks based on generative adversarial networks to avoid detection, including specifically encrypting user data and initiating attacks that are specific to a file based on its properties [3]. The usefulness of intrusion detection for cyber–physical systems in identifying ransomware is compromised by the complex malevolent behavior and variety of evasion measures, leading to significant false rates [4]. As a result, prompt identification and efficient protection against unidentified threats have emerged as critical issues in the field of cyber security.

Researchers deploy both dynamic and static approaches to identify a crypto ransomware detection system to combat growing ransomware threats [5]. These approaches provide more security and reduce feature extraction time expenses. However, malware's complication and packaging techniques make static analysis readily compromised. Dynamic analysis,

as opposed to static analysis, successfully copes with malware evasion strategies and discovers new ransomware strains; nevertheless, it often demands more processing resources and evaluation time. Furthermore, Deep Learning (DL) and Machine Learning (ML) approaches were extensively employed to identify and avert ransomware attacks by capitalizing on their superior identification of patterns and feature learning abilities.

These advanced techniques can learn automatically and retrieve complicated patterns and discriminative characteristics from enormous datasets, resulting in smart and strong ransomware recognition schemes. In comparison to previous methods, DL and ML algorithms can handle complicated data more effectively, learn malevolent activity patterns, and accomplish more precise and rapid detection.

This work was novel in the combination of a hybrid enhanced normalization approach into an AI-based framework of ransomware detection [6]. In contrast to the normal methods, which use only conventional batch normalization, our model dynamically combines instance and layer normalization, which collectively stabilize adversarial training, enhance the gradient flow, and reduce mode collapse. This guarantees more realistic, varied ransomware-like samples generated by the generator and, in turn, improves the classifier's robustness.

Moreover, unlike most previous studies, which use GANs exclusively to augment the data, the present study exploits the twofold purpose of GANs: (1) balancing the minority ransomware samples with synthetic versions thereof; and (2) enhancing targeted detection accuracy using a dedicated classifier fed by both real and synthetic samples. This way, not only is the problem of class imbalance eliminated, but it also promotes the resilience of the model to newer ransomware families.

This paper is associated with the main contributions as follows:

- Enhanced GAN protocol to detect Ransomware - GAN design that works well with ransomware behavioral data and can create plausible synthetic samples, to enlarge training sets.
- Enhanced Normalization Technique (EN) - Proposing a Map, instance normalization, Layer normalization, and hybrid normalization that stabilizes adversarial training and reduces mode collapse, and further contributes to a more efficient adversarial training convergence rate in comparison with the state-of-the-art normalization techniques.
- To obtain data preprocessing, input dataset, behavioral logs (API calls, registry changes, file operations).
- Observations on GAN Framework - generator (G) (synthetic ransomware), discriminator (D) (real and generated samples), auxiliary classifier (C).
- Classifier Integration: sigmoid activation, learning rate, total objective function, Training and Optimization

With these contributions, the paper lays down a generalizable framework of ransomware detection that supersedes the current state-of-the-art in ransomware detection and that provides insights that would be helpful in its deployment in today's cybersecurity systems.

2. Related Study

It performed well in weighted generative adversarial networks [10]. The ransomware threat and its impact on SCADA and generator engage in games throughout training until the discriminator was highly proficient in identifying unknown attacks [11]. Improved accuracy in detection by the suggested work was demonstrated in the experiment.

In 2022, X. Zhang et al. [1] introduced a model that used a file-distributing traffic study to identify and halt ransomware activities. This was the first proposal that was intended to function with both encrypted file-sharing protocols and clear-text protocols.

From network data, the attributes were extracted that characterized file opening, closing, and modification activities. The characteristics make it possible to distinguish between ransomware action and high activities from programs that are innocuous. This article validates the presented technique by examining the false rates and the volume of user file data that the ransomware might encode before being discovered.

In 2021, P. Freitas de Araujo-Filho et al. [4] suggested an Intrusion Detection technique that checks authorizations, and network-driven aspects both dynamically and statically by checking call logs, memory utilization, and usage of CPU. Here, the dynamic and static characteristics were gathered and trained on the proposed model. The experiments demonstrated the betterment of the suggested ensemble detection approach in categorizing ransomware behavior, hence mitigating adversarial evasion efforts.

In 2024, J. Ferdous et al. [6] suggested a ransomware detection method dubbed AI-Based Ransomware Detection. This system intends to achieve timely ransomware detection and protection by recording and analyzing subtle API call activity prior to the beginning of an encryption attack.

The dynamic behavioral data from the pre-attack stage were examined, and NLP methods were deployed to extract and represent essential elements from API sequences. To discriminate between ransomware and innocuous software, an intrusion detection system was developed based on these characteristics [18]. Experimental results show that the developed framework performed exceptionally well in early ransomware detection across many datasets.

In 2023, B. J. Chinmaya et al. [7] proposed targeted ransomware attacks, a novel approach that enables robust detection of both known and unknown ransomware variants. The developed work leveraged co-clustering and transfer learning techniques for bridging the gaps between the target and source domains.

The suggested technique has a high rate of detection, far surpassing baseline methods. Comprehensive trials show TLERAD's efficacy in real-world circumstances, showcasing its flexibility in the continually changing ransomware ecosystem.

In 2023, S. Razaulla et al. [8] presented the age of ransomware, a ransomware detecting approach that can identify zero-day ransomwares in their earlier stages. ZRS uses the PE header (portable executable header) characteristics for detecting the ransomware. It has 2 stages: "auto-encoding network-based core attribute learning (AE-CAL) and self-attentive mechanism-based convolutional neural network inference (SA-CNN-IS)". AE-CAL extracts the essential properties of known and undiscovered ransomware classes using self-encoding networks, whereas SA-CNN-IS identifies ransomware.

In 2023, M. Wazid et al. [9] discussed the ransomware attacks, which may identify crypto-ransomware before it is encrypted. PEDA offers two stages of detection. The initial level of analysis occurred before the ransomware was triggered by comparing its signature to that of a known crypto-ransomware. Another stage of detection employed a Learning Algorithm (LA), which may detect crypto-ransomware based on a pre-encryption Application Programming Interface (API). In addition, our study successfully discovered fourteen key APIs that may distinguish ransomware.

In 2025, G. Gebrehans et al. [15] suggested a weighted GANs (wGANs) approach. First, the suggested wGAN was utilized to produce synthetic data that mimicked ransomware behavior and simulated the progression of assaults. The intrusion detection was then utilized to quantify the relevance of characteristics over various times, allowing the introduced model to manage behavioral deviations in developing ransomware strains [19]. Experimental assessment shows that the suggested wGAN was more resistant to behavioral deviations than extant methods. The wGAN exhibited improved accuracy and fewer false alarms.

Table 1. Review of literature

Author [Citation]	Methodology	Features	Challenges
[1] X. Zhang *et al.*	DGAN	Dual Generative Adversarial Networks	Encryption Ransomware Attack Detection
[4] P. Freitas de Araujo-Filho, *et al.*	Cyber–Physical Systems	Intrusion Detection for Cyber–Physical Systems	Generative Adversarial Networks
[6] J. Ferdous *et al.*	Ransomware Detection	AI-Based Ransomware Detection	A Comprehensive Review
[9] M. Wazid *et al.*	BSFR-SH	Blockchain-Enabled Security Framework	Ransomware Attacks
[10] U. Urooj *et al.*	Addressing Behavioral Drift	Ransomware Early Detection	Generative Adversarial Networks
[14] B. Kc, S. Sapkota *et al.*	Generative Adversarial Networks	Anomaly Detection and Malware Detection	A Comprehensive Survey

The crypto-ransomware early detection model was a type of malware that was always changing and posing a serious risk to cybersecurity [12]. Ordinary users often lack the skills to identify potentially dangerous apps, and by the time they realize a ransomware attack has occurred, it is typically too late to take appropriate action. Therefore, it is essential to detect ransomware attacks early on in order to safeguard consumers' digital assets properly. In order to detect ransomware, traditional detection systems usually use signature-based techniques. These techniques restrict the quantity of files that are lost during the encryption stage by stopping any processes that exhibit traits and behaviors comparable to those of ransomware. Nevertheless, ransomware has evolved defenses against antivirus software, making signature-based detection techniques useless for spotting new or undiscovered malware.

Furthermore, it is crucial to remember that in order to extract features from dynamic feature-based detection techniques, files usually need to be run in an isolated environment. Rapid ransomware detection was hampered by a conditional tabular generative adversarial network, as it not only requires a significant amount of time and computing power but also raises the possibility of malware leaks [13]. Thus, one of the most urgent challenges in the realm of ransomware detection is creating a quick and efficient technique for the speedy identification.

3. Proposed Methodology

The proposed ransomware detection model is built on an improved Generative Adversarial Network with an enhanced normalization technique to achieve stable training, effective feature representation, and superior classification performance [1]. The methodology integrates data preprocessing, GAN training, hybrid normalization, and classifier optimization. Each stage is mathematically defined to clarify the workflow.

3.1. Proposed Encoding Method

Step 1: Log Tokenization
Each behavioral log sequence is represented as:

$$S = \{e_1, e_2, e_3, \ldots, e_n\}$$

where each event e_i corresponds to $i = 1,2,3,\ldots,n$ and is based on an API call, File operation, and Registry modification.

Step 2: Vocabulary Mapping
A dictionary V is constructed: V:$e_i \rightarrow k_i \in \mathbb{N}$

Step 3: Normalized Intensity Mapping
The token index is normalized into pixel intensity: $p_i = \frac{k_i}{|V|}$

Step 4: Image Construction
Let fixed image size as 64 × 64 grayscale, truncated to length 4096, and Row-major reshaping:

$$I = reshape(p_1, p_2, p_3, \ldots, p_{4096}) \in \mathbb{R}^{64\times64}$$

3.2. Vectorization Approach

It employed One-Hot Encoding with frequency weighting for Raw Logs → Tokenization → One-Hot Vector → Image Encoding:
For each sequence: $x_i \in \mathbb{R}^{|V|}$,
where:$x_i[j]$=frequency of token j in sequence i.

3.3. Key Innovations Over Standard AC-GAN

Generator (G) Enhancements
Input: Noise vector $z \sim N(0,1)$class label y

Architecture: Dense → Reshape → 4 Transposed Conv layers

Activation: LeakyReLU (α = 0.2), Hybrid Normalization Layer
Discriminator (D) Enhancements

Input: 5 Convolutional layers

Outputs: Real/Fake (sigmoid); Class label (softmax)
Hybrid Normalization
Combination of Instance Normalization & Layer Normalization

$$\mathrm{HN}(x) = \alpha\cdot\mathrm{IN}(x) + (1\text{-}\alpha)\cdot\mathrm{LN}(x)$$

where α=0.5

The Impact of the model discussed stabilizes training dynamics, improves feature generalization, and reduces sensitivity to batch size.

3.4. Augmentation and the "Map" Technique

(A) Data Augmentation
It was performed in two stages:
1. GAN-based Augmentation
Generator(G) produces synthetic ransomware samples:

$$x_{fake/real} = G(z, y)$$

2. External Augmentation
The Sequence perturbation was a random insertion of benign API calls and sequence shuffling.
(B) Map Technique (Normalization Mapping)

The Map function $M(x)$ transforms feature distributions before normalization:

$$M(x) = \frac{x - \mu_{local}}{\sigma_{local} + \in}$$

Where μ_{local}=local mean, σ_{local}=local standard deviation, ∈=error.

It aims to align heterogeneous log distributions, reduce variance across samples, and enhance GAN training stability. The input dataset consists of behavioral logs (API calls, registry changes, file operations). Let the dataset be represented as:

$$D = \{(x_i, y_i) \mid x_i \in \mathbb{R}^n, y_i \in \{0,1\}\} \quad (1)$$

where x_i is the feature vector of dimension n and y_i denotes the class label ($0 =$ benign, $1 =$ ransomware). Normalization of raw features is applied to reduce scale variations:

$$\hat{x}_{ij} = \frac{x_{ij} - \mu_j}{\sigma_j} \quad (2)$$

where μ_j and σ_j are the mean and standard deviation of feature j.

The GAN consists of a generator (G), a discriminator (D), and an auxiliary classifier (C). The generator maps a noise vector z from a latent space $Z \sim \mathcal{N}(0,1)$ into a synthetic ransomware-like sample:

$$G(z; \theta_G): Z \rightarrow X \quad (3)$$

The discriminator attempts to distinguish between real and generated samples:

$$D(x;\theta_D): X \to [0,1] \tag{4}$$

The adversarial objective of GAN is defined as:

$$\min_G \max_D V(D,G) = \mathbb{E}_{x\sim p_{\text{data}}(x)}[\log D(x)] + \mathbb{E}_{z\sim p_z(z)}[\log(1-D(G(z)))] \tag{5}$$

To address GAN instability, a hybrid normalization technique is applied. For each feature map h, instance normalization is:

$$\text{IN}(h_i) = \frac{h_i - \mu(h_i)}{\sigma(h_i)} \tag{6}$$

Layer normalization is:

$$\text{LN}(h) = \frac{h - \mu(h)}{\sigma(h)} \tag{7}$$

The hybrid normalization combines both:

$$\text{HN}(h) = \alpha \cdot \text{IN}(h) + (1-\alpha) \cdot \text{LN}(h) \tag{8}$$

where α is a learnable parameter. The classifier C leverages both real and synthetic samples. For a sample x, the classifier output is:

$$C(x) = \sigma(Wx + b) \tag{9}$$

where σ is the sigmoid activation. The binary cross-entropy loss is defined as:

$$\mathcal{L}_C = -[y\log C(x) + (1-y)\log(1-C(x))] \tag{10}$$

The total objective function of the model combines GAN loss, classifier loss, and normalization stability loss:

$$\mathcal{L}_{\text{total}} = \lambda_1 \mathcal{L}_{CAN} + \lambda_2 \mathcal{L}_C + \lambda_3 \mathcal{L}_{HN} \tag{11}$$

where $\lambda_1, \lambda_2, \lambda_3$ are balancing coefficients. The generator is updated using gradient descent on the loss:

$$\theta_G \leftarrow \theta_G - \eta \nabla_{\theta_G} \mathcal{L}_{\text{total}} \tag{12}$$

The discriminator update rule is:

$$\theta_D \leftarrow \theta_D - \eta \nabla_{\theta_D} \mathcal{L}_{\text{total}} \tag{13}$$

And the classifier update rule (where $\boldsymbol{\eta}$ is the learning rate):

$$\theta_C \leftarrow \theta_C - \eta \nabla_{\theta_C} \mathcal{L}_C \tag{14}$$

This developed work aims to propose a novel ransomware attack detection approach with the following steps:

1) GAN Framework
2) Enhanced Normalization
3) Classifier Integration

Initially, data preprocessing will take place using two procedures, namely, data normalization and data conversion. Here, the data will be normalized using an Improved normalization technique. Data is converted to an image for further processing**.** Subsequently, the data will be augmented using a data augmentation technique. Finally, attack detection will be performed using an improved Generative Adversarial Network. The developed work on the ransomware attack detection model will be implemented using Python. The efficiency of the developed model will be measured by comparison of its performance over existing models by means of varied metrics. The proposed overall architecture is illustrated in Figure 1.

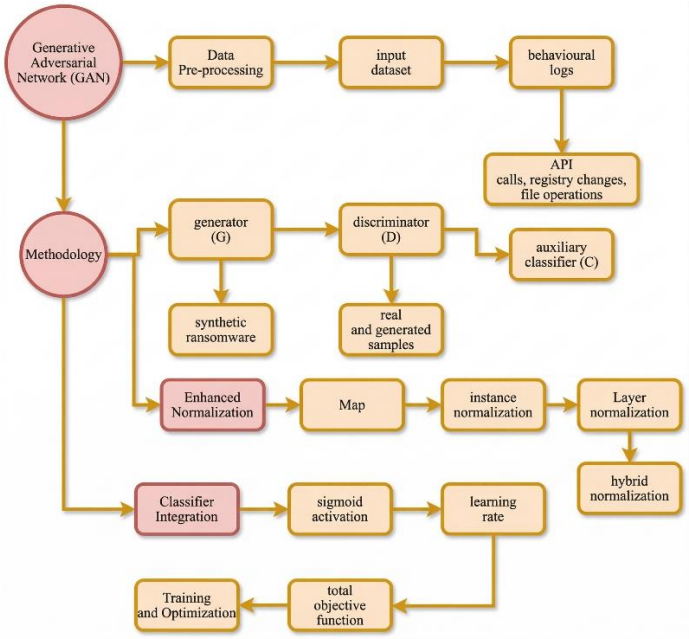

Fig. 1 Architecture of GAN proposed methodology

4. Results and Discussion

The GAN-based ransomware detection model with an application of improved normalization proposed based on multiple ransomware datasets, such as anomaly detection and malware detection, and a real-world behavioural trace collection was examined [14]. Evaluation was based on the performance of detection accuracy, false-positive rate, precision, recall, and training stability among the baseline models and dynamic malware behavior [15]. All the results indicated that the improved normalization increased training stability and diminished variation in the value of loss, resulting in speedier convergence. This intrusion detection gave the generator an opportunity to generate more varied ransomware-like samples, consequently enhancing the discrimination capability between good and bad data by the classifier [16]. In Figure 2, our proposed approach achieved a comparison of before and after augmentation by using GAN. It is also reflected in the diagram that the proposed model was able to sustain accuracy on all datasets, as opposed to the baselines, which revealed a significant decline when they were used on a new ransomware family's loss on training and validation in Figure 3.

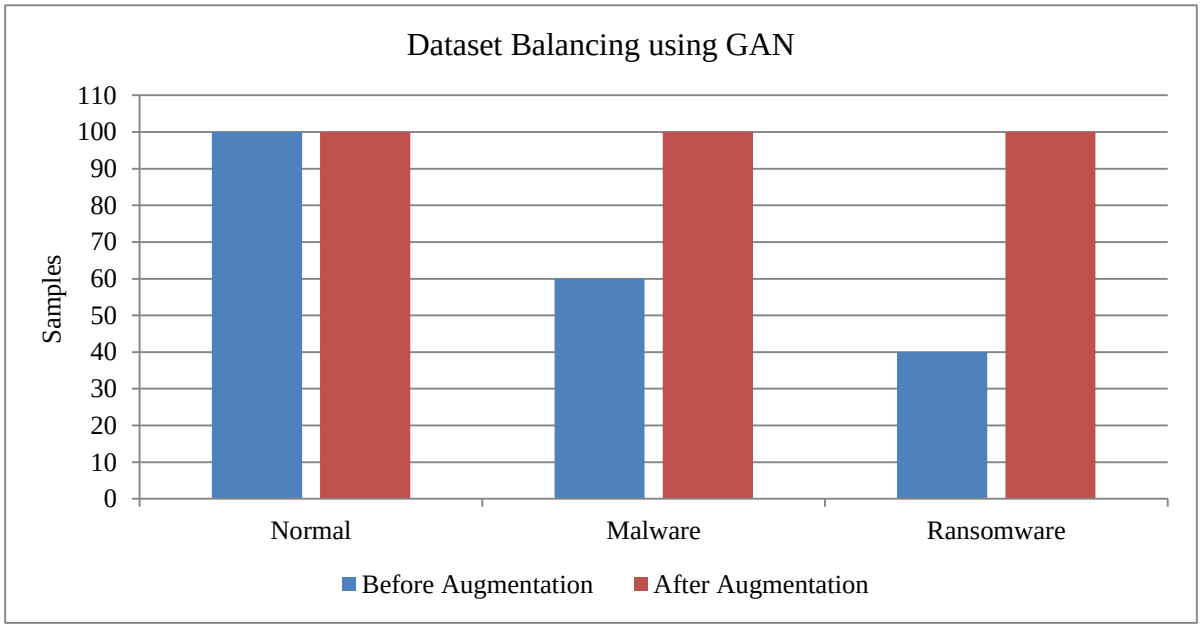

Fig. 2 Comparison of before and after augmentation by using GAN

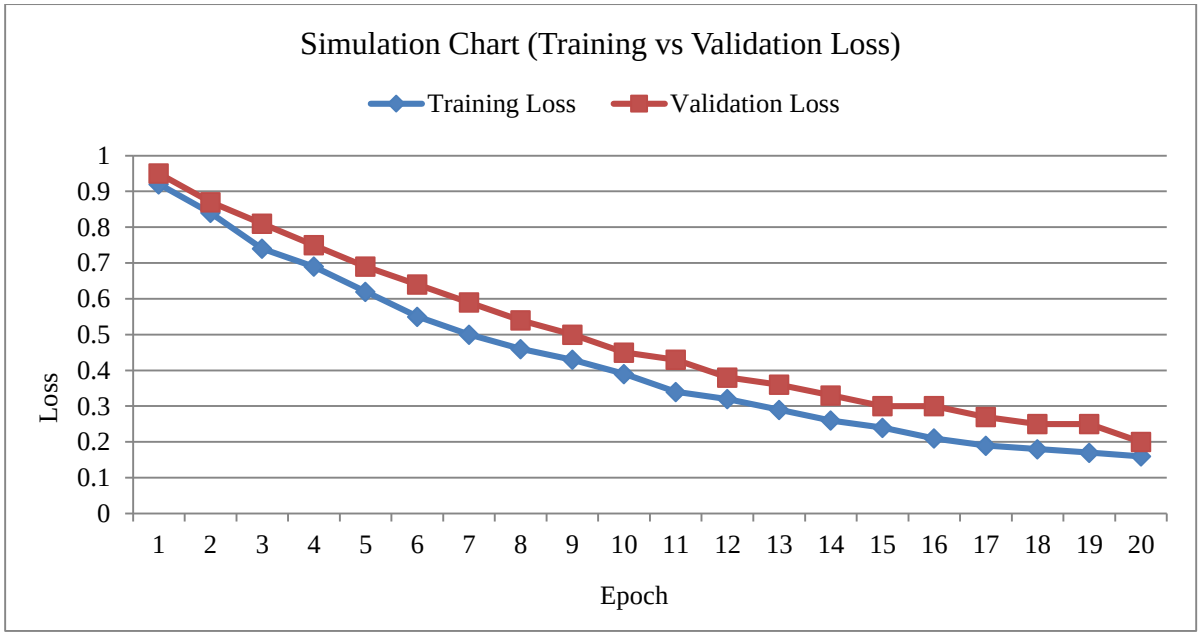

Fig. 3 Simulation of loss on training and validation

The mention of precision and recall serves to illustrate that most of the conventional models have an extremely high false positive rate, severely dampening their practical application. The presence of a high false positive will result in benign applications being reported as ransomware, which will lead to a lack of trust in security systems.

The likelihood of false positives found in the comparative false-positive rates across models was greatly decreased, as shown in Table 2. Here, the improved normalization was essential to stabilize the training, provide balanced decision boundaries, and prevent a bias of the classifier in favor of the benign class. This, in itself, led to better recall without a loss in precision.

Table 2. Comparative false-positive rates across models

Model	False Positive Rate (%)	Recall (%)	Precision (%)
CNN-Based Model	7.8	86.5	88.2
RNN-Based Model	6.4	88.9	90.1
Conventional GAN	5.9	90.2	91.7
Proposed Model	3.2	95.6	96.8

Stability of adversarial training was also a significant point. Classical GAN-based ransomware detectors have considerable mode collapse that causes skewed classifiers. This issue was adequately reduced in the proposed GAN frameworks with their confusion matrix in Figure 4. Evidence of this enhancement in normalization is the rapid convergence of the proposed model training over epochs, where they converge within almost 35 epochs when conventional GANs require more than 50 epochs with oscillations in the loss curves. This quicker convergence not only makes it more accurate but also reduces computational cost in the long-run deployment of the heatmap in Figure 5.

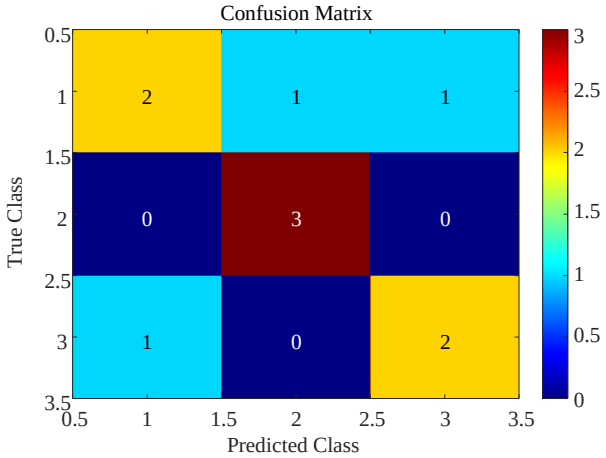

Fig. 4 Confusion matrix for classes

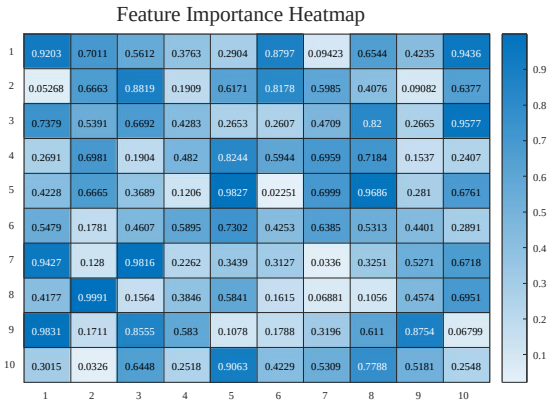

Fig. 5 Heatmap frameworks

The invulnerability of the model was also evaluated against polymorphic ransomware samples, which are usually hard to detect as they may be obfuscated and encrypted. Experimental results indicate that, in contrast to traditional deep learning models, where the accuracy decreased by up to 15 % on these samples, the accuracy of the proposed model only dropped by 4 %.

This reflects improved generalization, which is a vital attribute when it comes to ransomware families that constantly keep evolving. The accuracy, recall, and F1-score of polymorphic and standard ransomware samples are compared in detail in Table 3.

Table 3. Performance on polymorphic Vs standard ransomware samples

Model	Standard Accuracy (%)	Polymorphic Accuracy (%)	F1-Score (%)
CNN-Based Model	91.2	77.8	83.4
RNN-Based Model	92.6	79.5	85.1
Conventional GAN	94.1	81.4	87.2
Proposed Model	96.7	92.5	94.8

The scalability of the model was also implemented in regard to throughput during deployment in a simulated enterprise network. In Figure 6, the three different types of enhanced normalization demonstrate the ability of the proposed model to contain false positives and high throughput.

This indicates that the enhanced normalization helps stabilize training not only but also makes the inference process more efficient, with a loss of generator and decimator in Figure 7. The performance gap especially occurred during the loss of weight landscape throughput across models demanded when the 3D models became slow in Figure 8.

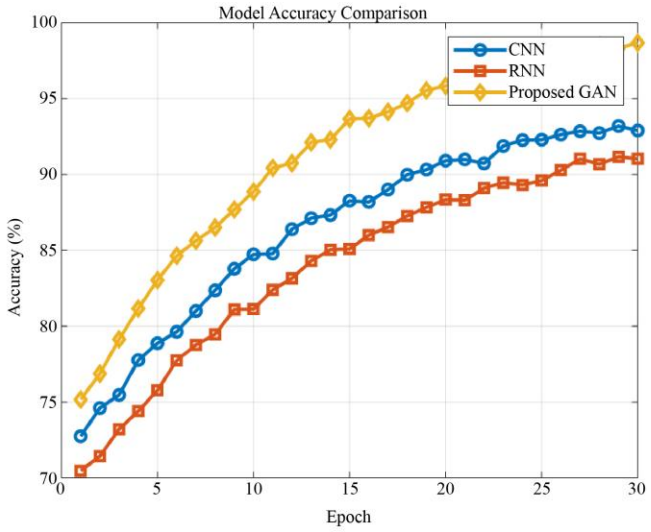

Fig. 6 Accuracy comparison: Enhanced normalization throughput across models

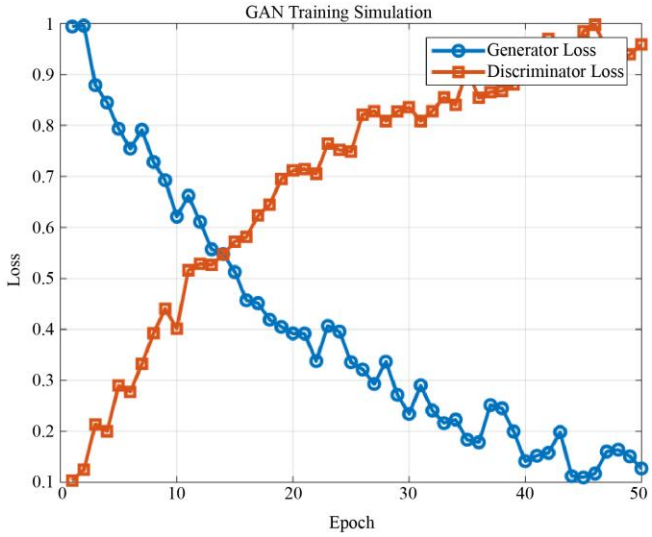

Fig. 7 GAN under loss of generator and decimator

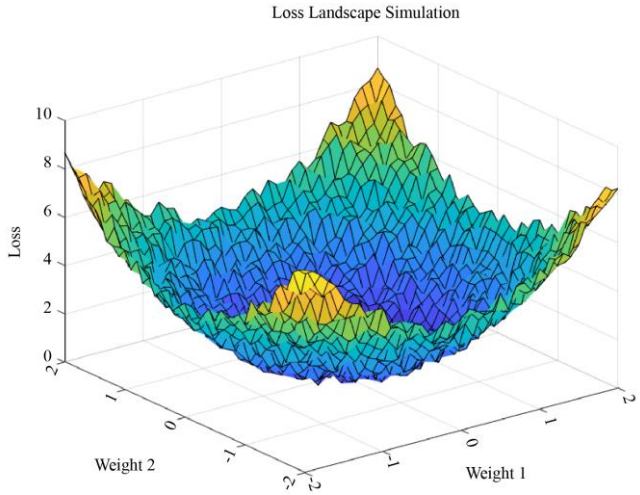

Fig. 8 Loss of weight landscape throughput across models

This discussion showed clearly that the improved normalization has a double role of stabilizing the adversarial training and improving the overall reliability in detection. The concrete outcome of this enhancement is the increased speed of convergence, a drop in false alerts, and smoother resistance to autonomous anomaly detection [17]. It is also pointed out that, though the proposed model performs better during offline tests, running in real-time settings still presents a computational difficulty. This implies a compromise between accuracy and efficiency that will have to be balanced in future studies.

5. Conclusion

This paper proposed a GAN-based ransomware attack detection model on an enhanced normalization technique with a new, more stable. It showed that GAN frameworks include a generator (synthetic ransomware), a discriminator (real and generated samples), and an auxiliary classifier. Although the model was so effective, its application has some practical limitations, such as a lot of computational demands, the need for reliable datasets, and difficulties with its use in real-time in limited environments. In addition, enhanced normalization leads to improved resilience of a system; it is likely to lead to map, instance normalization, layer normalization, and hybrid normalization.

Furthermore, the classifier integration detected the sigmoid activation, learning rate, and total objective function, Training and Optimization. The above enhancements will make the GAN-based ransomware detection systems usable across the various and dynamic cybersecurity environments.

References

[1] Xueqin Zhang, Jiyuan Wang, and Shinan Zhu, "Dual Generative Adversarial Networks Based Unknown Encryption Ransomware Attack Detection," *IEEE Access*, vol. 10, pp. 900-913, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Dongyang Li, Daisuke Kotani, and Yasuo Okabe, "Improving Attack Detection Performance in NIDS Using GAN," *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, Madrid, Spain, pp. 817-825, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Xueqin Zhang et al., "Adversarial Examples Detection for XSS Attacks Based on Generative Adversarial Networks," *IEEE Access*, vol. 8, pp. 10989-10996, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Paulo Freitas de Araujo-Filho et al., "Intrusion Detection for Cyber–Physical Systems Using Generative Adversarial Networks in Fog Environment," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6247-6256, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ahmad O. Almashhadani et al., "A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware," *IEEE Access*, vol. 7, pp. 47053-47067, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Jannatul Ferdous et al., "AI-Based Ransomware Detection: A Comprehensive Review," *IEEE Access*, vol. 12, pp. 136666-136695, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] B.J Chinmaya, Sujay Arun Kudtarkar, and Mohana, "Targeted Ransomware Attacks and Detection to Strengthen Cybersecurity Strategies," *2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS)*, Pudukkottai, India, pp. 1039-1044, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Salwa Razaulla et al., "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions," *IEEE Access*, vol. 11, pp. 40698-40723, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Mohammad Wazid, Ashok Kumar Das, and Sachin Shetty, "BSFR-SH: Blockchain-Enabled Security Framework against Ransomware Attacks for Smart Healthcare," *IEEE Transactions on Consumer Electronics*, vol. 69, no. 1, pp. 18-28, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Umara Urooj et al., "Addressing Behavioral Drift in Ransomware Early Detection Through Weighted Generative Adversarial Networks," *IEEE Access*, vol. 12, pp. 3910-3925, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Usman Javed Butt et al., "Ransomware Threat and its Impact on SCADA," *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, London, UK, pp. 205-212, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] Umara Urooj, Mohd Aizaini Bin Maarof, and Bander Ali Saleh Al-rimy, "A Proposed Adaptive Pre-Encryption Crypto-Ransomware Early Detection Model," *2021 3rd International Cyber Resilience Conference (CRC)*, Langkawi Island, Malaysia, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Zhor Ismaili et al., "Toward a New Approach Based on Conditional Tabular Generative Adversarial Network for Ransomware Attack Detection in IoT Systems," *2025 International Conference on Intelligent Systems: Theories and Applications (SITA)*, Rabat, Morocco, pp. 1-6, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[14] Bishal Kc, Shushant Sapkota, and Ashish Adhikari, "Generative Adversarial Networks in Anomaly Detection and Malware Detection: A Comprehensive Survey," *Advances in Artificial Intelligence Research*, vol. 4, no. 1, pp. 18-35, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] Ghebrebrhan Gebrehans et al., "Generative Adversarial Networks for Dynamic Malware Behavior: A Comprehensive Review, Categorization, and Analysis," *IEEE Transactions on Artificial Intelligence*, vol. 6, no. 8, pp. 1955-1976, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[16] Song Han et al., "Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges," *IEEE Systems Journal*, vol. 8, no. 4, pp. 1052-1062, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[17] Tharindu Lakshan Yasarathna, Madhusanka Liyanage, and Nhien-An Le-Khac, "Deep Learning-Based Autonomous Anomaly Detection for Security in SDN-IoT Networks," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 8007-8048, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Wanning Liu et al., "ETFIDS: An Entropy-Driven, Time-Frequency Analysis Framework for In-Vehicle CAN Signal Intrusion Detection," *IEEE Internet of Things Journal*, vol. 12, no. 12, pp. 21507-21522, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] Xingxing Wang et al., "Intrusion Detection for Intelligent Vehicle CAN Bus Based on Tsetlin Machine," *2024 8th CAA International Conference on Vehicular Control and Intelligence (CVCI)*, Chongqing, China, pp. 1-5, 2024. [CrossRef] [Google Scholar] [Publisher Link]