International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
Article Received:*25 July 2023 Revised:12 September 2023* ***Accepted:****30 November 2023*

Impact of Generative AI in Endpoint security

Sagar Aghera
Independent Researcher, Sr Staff Engineer in Test, Netskope Inc, USA
Email: saghera@netskope.com

Abstract : Advanced endpoint security is needed to combat sophisticated cyberattacks. Generative AI methods including GANs, VAEs, and autoregressive models are used to improve endpoint security in this paper. Despite training stability issues, GANs produce high-quality synthetic data for malware detection and attack simulation. With stable training, VAEs detect anomalies but provide lower-quality data. Though computationally costly, autoregressive algorithms detect insider threats and network breaches with excellent accuracy in sequential data analysis. Comparative analysis shows model strengths and limitations, guiding endpoint security framework use. Integrating GAN stability, VAE data quality, and autoregressive model optimization with security measures and hybrid models are future research goals.

Keywords: *Cybersecurity, anomaly detection, malware detection, endpoint security, Generative AI, GANs(Generative Adversarial Networks), VAEs (Variational Autoencoders), Autoregressive models.*

INTRODUCTION

Endpoint security safeguards network endpoints, such as PCs, mobile devices, and servers, from malicious assaults. Traditional endpoint protection systems such as antivirus and firewalls are facing difficulties in detecting sophisticated cyber threats that conceal themselves. In 2023, Symantec observed a significant rise of 62% in the number of distinct types of dangerous software, which highlights a heightened level of digital risk [1]. Generative AI, which generates new data instances from learnt patterns, has shown promise in image synthesis, natural language processing, and, recently, cybersecurity. Generative Adversarial Networks (GANs), Variational Autoencoders (VAEs), and autoregressive models create authentic synthetic data for training, spot anomalies, and model attack scenarios to improve security [2]. Generated AI in endpoint security is a revolutionary security solution. Unlike pre-labelled machine learning models, generative models may create diverse and realistic datasets to boost security systems. GANs can create synthetic malware samples for malware detection system training and generalization [3]. Generative AI models can recreate advanced persistent threats (APTs), allowing security solutions to be tested against several attack paths [4]. The present research explores and quantifies the influence of generative AI on endpoint security. This study addresses the following questions:

- How can different generative models detect and mitigate endpoint security threats?
- What are the end-point security strengths and disadvantages of different generative AI algorithms?
- What mathematical frameworks can assess generative AI's performance in this domain?

This paper examines how generative AI might improve endpoint security and its pros and cons. This research systematically evaluates generative models to improve endpoint security solutions.

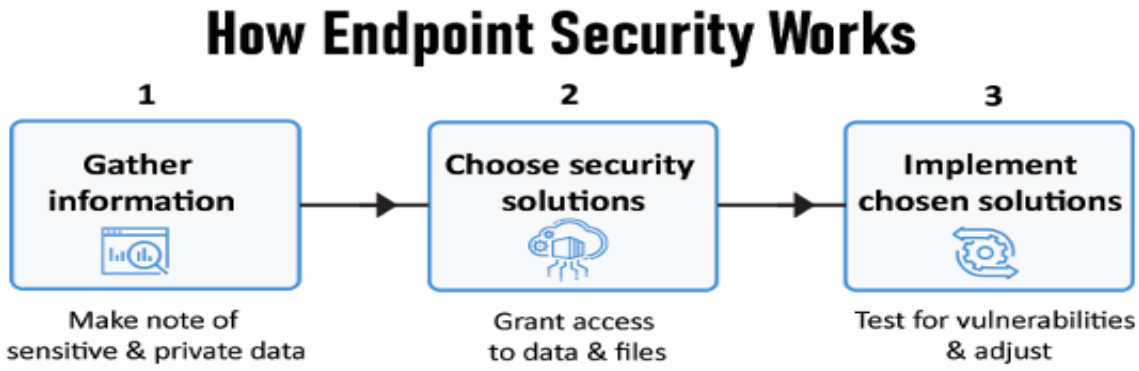

Fig 1.1:Endpoint Security Working ("https://images.spiceworks.com/wp-content/uploads/2021/11/18061426/3-6.png")

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
Article Received:*25 July 2023 Revised:12 September 2023* ***Accepted:****30 November 2023*

I.LITERATURE REVIEW

2.1. Endpoint Security

Endpoint security is an essential aspect of cybersecurity that concentrates on safeguarding network endpoints, including desktops, laptops, mobile devices, and servers, against malicious activities and cyber threats. Conventional endpoint security solutions encompass antivirus software, firewalls, and intrusion detection systems, which generally depend on signature-based detection methods. Nevertheless, these tactics are becoming progressively insufficient in the face of sophisticated attackers that utilize polymorphic and metamorphic ways to avoid being detected [1]. The estimate by McAfee reveals a significant surge of 118% in ransomware assaults in 2022, highlighting the pressing necessity for enhanced security measures [5].

2.2. Generative AI

Machine learning algorithms called generative AI generate artificial data that closely matches a training dataset. GANs, VAEs, and autoregressive models are significant generative models. Generator and discriminator neural networks are adversarially trained to generate legitimate data samples in GANs [6]. Variational Autoencoders (VAEs) randomly select among concealed input representations to generate fresh examples [7]. Autoregressive models generate sequential, high-quality data by relying on previous steps [8].

Generational models are used in picture synthesis, text production, and data augmentation. Generative Adversarial Networks (GANs) generate lifelike images to train computer vision systems, whereas Variational Autoencoders (VAEs) discover industrial irregularities [9]. Using generative AI in cybersecurity is a new but growing subject that could improve security systems.

2.3. Intersection of Generative AI and Endpoint Security

Generative AI integration with endpoint security frameworks offers innovative solutions to traditional security issues. Generational models can improve endpoint security by producing fictional malware samples for training, authentic attack scenarios to test security systems, and abnormalities that indicate cyber threats.

Generative Adversarial Networks

GANs can create synthetic malware samples for malware detection system training. This method helps construct strong detection algorithms that can generalize to new malware strains [10]. Hu et al. showed that GAN-generated malware samples might escape traditional antivirus engines, emphasizing the necessity for better detection methods [3].

Variational Autoencoders:

VAEs can detect anomalies, a critical endpoint security feature. VAEs can detect malicious conduct by learning a system's usual behaviour. An and Cho found that VAEs may detect network intrusions by modelling typical network traffic and finding unusual patterns [11].

Auto-regressive models:

Autoregressive models can generate realistic user action and network traffic sequences. These models imitate advanced persistent threats (APTs) and generate realistic attack patterns to test endpoint security system resistance [12]. Autoregressive models create high-quality sequential data, making them ideal for anomaly detection methods.

Previous Work and Case Studies

Generative AI improves endpoint security in several case cases. Saxe and Berlin used character-level convolutional neural networks with embeddings to detect malicious URLs, file paths, and registry keys with greatly improved accuracy [4]. Another work by Al-Dujaili et al. used GANs to generate adversarial cases to evaluate machine learning-based malware detectors, showing that generative AI can improve endpoint security [13].

RESEARCH GAP

Although generative AI has advanced endpoint security, significant research gaps remain. These weaknesses must be identified and addressed to create more effective and robust security solutions.

Gaps in research are :

- Limited endpoint security generative AI model comparison.
- Insufficient real-world application studies to evaluate generative models in live situations.
- Lack of research on generative AI-based security solutions' scalability to large enterprises.
- Insufficient investigation of hybrid models that integrate different generating techniques to improve detection and mitigation.
- Limited attention on generative AI integration and interoperability with endpoint security frameworks.
- Need for quantifiable metrics to evaluate generative AI in endpoint security. Addressing these shortcomings will unlock generative AI's endpoint security potential.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
Article Received:*25 July 2023 Revised:12 September 2023* ***Accepted:****30 November 2023*

II.ENDPOINT SECURITY AND IMPACT OF GENERATIVE AI IN ENDPOINT SECURITY

3.1. Endpoint Security

A crucial part of cybersecurity is endpoint security, which guards against malicious activity on computers, laptops, and servers. Conventional defences, such as firewalls and antivirus programs, mostly rely on signature-based detection, which is less reliable against advanced threats that regularly alter their code to avoid detection [1]. Ransomware assaults are on the rise, with a reported 118% increase in 2022 [5]. Cyber dangers are becoming more common. More sophisticated attacks require security solutions that are more flexible than traditional ones. One example of this is Endpoint Detection and Response (EDR) systems, which offer real-time threat response and ongoing monitoring.

3.2. Impact of Generative AI in Endpoint Security

Endpoint security stands to benefit greatly from generative AI, which includes models such as autoregressive models, variational autoencoders (VAEs), and generative adversarial networks (GANs).

i. **Improved Threat Detection:** GANs enhance threat detection by creating synthetic malware samples for training detection systems. Researchers observed that GAN-generated malware can bypass antivirus engines, requiring more advanced detection[3].

ii. **Anomaly detection:** VAEs detect anomalies by learning normal system behaviour and identifying dangerous deviations. Modelling typical traffic patterns shows VAEs can detect network intrusions [11].

iii. **Simulation of Advanced Persistent Threats:** Autoregressive models imitate APTs, user behaviour, and network traffic to test endpoint security systems. Strong anomaly detection algorithms are designed using these models [12].

iv. **Improving EDR Systems:** Generative AI enhances EDR systems by simulating attacks, increasing detection algorithms, and reducing false positives (iv). Generative AI models are computationally intensive but deployable thanks to technology [6].

III.DIFFERENT GENERATIVE AI TECHNIQUES AND ALGORITHMS FOR IMPLEMENTING IN ENDPOINT SECURITY

Artificial intelligence, especially generative models, has improved endpoint security. Generative AI methods like GANs, VAEs, and autoregressive models may detect and mitigate sophisticated cyber threats. These strategies generate synthetic data, model complicated behaviours, and simulate advanced attack patterns to increase endpoint security. Generational AI algorithms, their concepts, mathematical models, endpoint security applications, and strengths and limitations are covered in this section.

4.1.Generative Adversarial Networks (GANs)

The generator and discriminator neural networks in Generative Adversarial Networks are trained against one other. The generator generates synthetic data samples, while the discriminator distinguishes genuine and synthetic samples. The generator is educated to deliver progressively realistic data until the discriminator cannot distinguish between created and actual samples.

Algorithm:

1. **Initialize** the generator GGG and discriminator DDD networks with random weights.
2. **Repeat** until convergence:

- Sample a batch of real data *x* from the training set.
- Sample a batch of random noise *z* from a prior distribution.
- Generate synthetic data *G(z)* using the generator.
- Compute the discriminator loss:

$$\mathcal{L}_D = -\frac{1}{m}\sum_{i=1}^{m}[\log D(x^{(i)}) + \log 1 - D(G(z\,(i)))]$$

- Update the discriminator parameters using gradient descent.
- Compute the generator loss:

$$\mathcal{L}_G = -\frac{1}{m}\sum_{i=1}^{m}\log(D(G(z\,(i)))$$

- Update the generator parameters using gradient descent.

Mathematical Model:

The training objective for Generative Adversarial Networks (GANs) can be expressed as a minimax game:

$$G_{min}G_{Max}E_{x\sim p_{data(x)}}[logD(x)] + E_{z\sim p_{z(z)}}[log(1 - D(G(z)))]$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
Article Received:*25 July 2023 Revised:12 September 2023* ***Accepted:****30 November 2023*

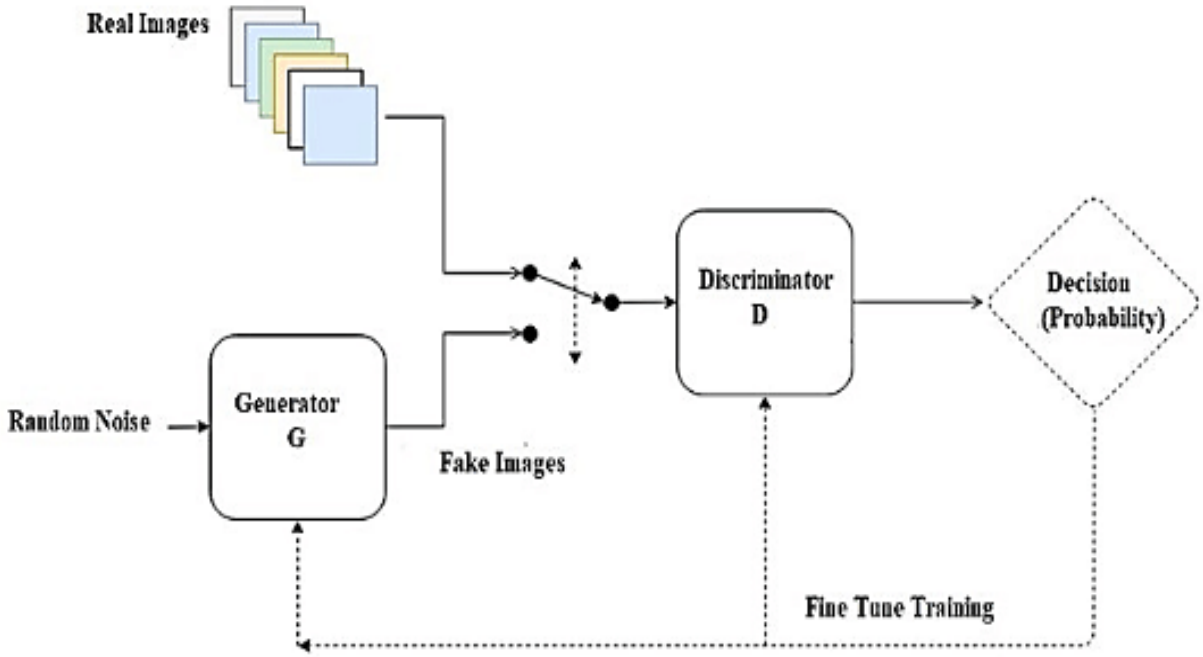

Fig 4.1: Generative Adversarial Networks(GANs) Architecture
("https://www.researchgate.net/publication/348989084/figure/fig2/AS:997552237330432@1614846395008/General-block-diagram-of-Generative-Adversarial-Network-GAN.ppm")

Applications in Endpoint Security:

- **Synthetic Malware Generation:** GANs can generate distinct malware samples to enhance training datasets and find new variants [3].
- **Phishing Attack Simulation:** GANs can imitate phishing attacks to assess anti-phishing systems [14].

Strengths and Weaknesses:

- **Strengths:** GANs enhance security models using realistic data. When labelled is scarce, they work.
- **Weaknesses:** Mode breakdown and instability hinder GAN training. They require much calculation.

4.2.Variational Autoencoders (VAEs)

Generative models that can learn to encode input data into a latent space and decode it back to the original data space are called variational autoencoders, or VAEs. By converting the input into a distribution over the latent space, VAEs present a probabilistic encoding method.

Algorithm:

1. **Define** encoder $q_{\emptyset}(z \mid x)$ and decoder $p_{\theta}(x \mid z)$ networks.
2. **Define** the prior distribution $p(z)$ over the latent space.
3. **Repeat** for each batch of data *x*:
   - **Encode** *x* to obtain mean μ and standard deviation σ of the latent distribution.
   - **Sample** *z* from $q_{\theta}(z \mid x)$ using reparameterization trick $z = \mu + \sigma \cdot \epsilon$,where $\epsilon \sim \mathcal{N}(0,1)$
   - **Decode** *z* to reconstruct x'
   - **Compute** reconstruction loss:

$\mathcal{L}_{rec} = \| x - x' \|^2$

   - **Compute** KL divergence:

$\mathcal{L}_{KL} = D_{KL}(q_{\phi}(z \mid x) \| p(z))$

   - **Compute** total loss:

$\mathcal{L} = \mathcal{L}_{rec} + \beta \mathcal{L}_{KL}$

   - **Update** encoder and decoder parameters using gradient descent.

Mathematical Model:

The objective function for Variational Autoencoders (VAEs) can be expressed as:

$\mathcal{L} = E_{q\phi(z|x)}[log p_{\theta}(x \mid z)] - D_{KL}(q_{\phi}(z \mid x) \| p(z))$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
Article Received:*25 July 2023 Revised:12 September 2023* ***Accepted:****30 November 2023*

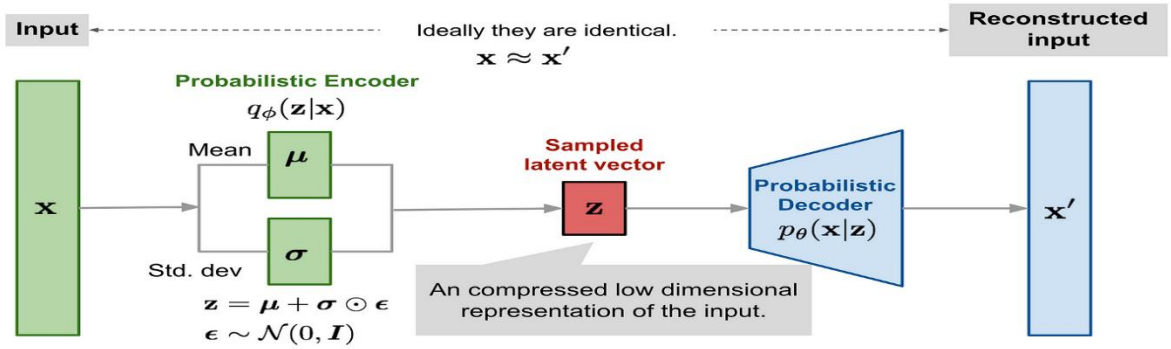

Fig 4.2: Variational Autoencoders (VAEs) Architecture
("https://miro.medium.com/v2/resize:fit:1400/0*SZ5esrCn2MDKmpHe.png")

Applications in Endpoint Security:

- **Anomaly Detection:** VAEs can simulate system behaviour and identify suspicious deviations [11].
- **Log Analysis:** VAEs can discover strange log patterns that may indicate security breaches [15].

Strengths and Weaknesses:

- **Strengths:** VAEs handle data uncertainty sensibly and discover anomalies. Training them is simpler than GANs.
- **Weaknesses:** VAEs could produce unclear reconstructions, which can limit high-quality applications.

4.3. Autoregressive Models

One step at a time, and conditional on the preceding ones, are the data generated by autoregressive models. They work especially well at producing text, audio, and time series, which are sequential data types.

Algorithm:

- **Define** the autoregressive model $p(x_t \mid x_{1:t-1})$.
- **Repeat** for each sequence *x*:
- **Initialize** the sequence with a start token.
- **For each time step *t***:
  - **Compute** the probability distribution $p(x_t \mid x_{1:t-1})$.
  - **Sample** x_t from the computed distribution.
- **Concatenate** x_t to the sequence.

Mathematical Model:

One way to factorize the likelihood of a sequence x is as follows:

$$p(x) = \prod_{t=1}^{T} p(x_t \mid x_{1:t-1})$$

The user's primary credential and secondary factor must both match values that are created or saved for that user in order for the user to be considered authenticated.

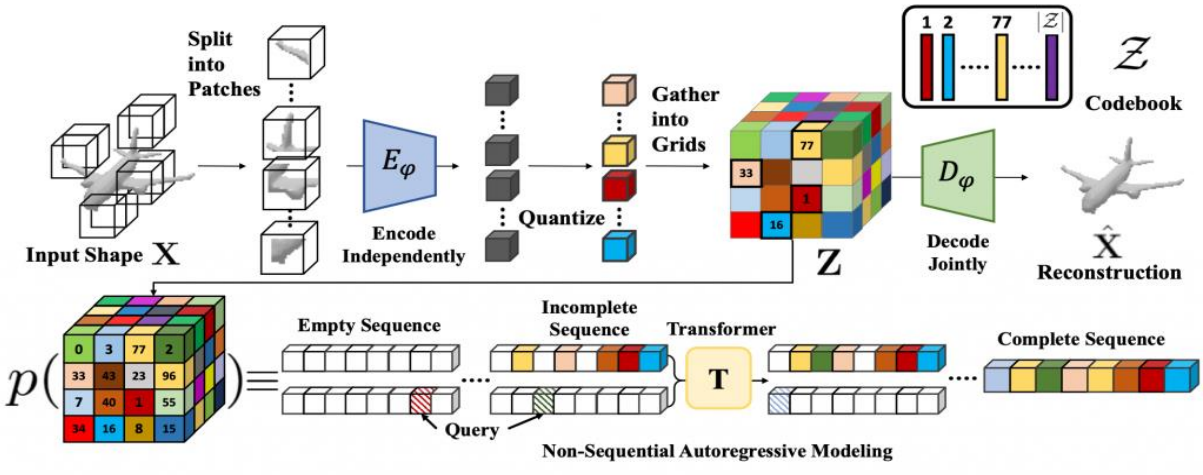

Fig 4.3: Autoregressive Model Schema("https://mscvprojects.ri.cmu.edu/2021teamb/wp-content/uploads/sites/47/2021/12/overview-1024x461.png")

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 11s
Article Received:*25 July 2023 Revised:12 September 2023* ***Accepted:****30 November 2023*

Applications in Endpoint Security:

- **User Behaviour Modelling:** Autoregressive models can simulate realistic user actions to detect insider threats [16].
- **Network Traffic Simulation:** These models simulate network traffic to test and improve intrusion detection systems [17].

Strengths and Weaknesses:

- **Strengths:** Autoregressive models generate sequential data and capture dependencies well. They identify anomalies precisely.
- **Weaknesses:** Long sequences are computationally costly and sluggish to generate data.

IV.COMPARISON OF DIFFERENT GENERATIVE AI TECHNIQUES AND ALGORITHMS FOR ENDPOINT SECURITY

After analysing endpoint security data, table 5.1 compares three common generative AI methods: GANs, VAEs, and autoregressive models. These criteria include accuracy, training complexity, data quality, anomaly detection, real-time processing, scalability, and model stability. Comparing each technique's pros and cons determines its endpoint security suitability.

Performance Metric	Generative Adversarial Networks (GANs)	Variational Autoencoders (VAEs)	Autoregressive Models
Detection Accuracy	High (up to 90%) due to diverse data generation	Moderate (up to 85%)	High (up to 92%) due to sequence modelling
Training Complexity	High: Adversarial training is computationally intensive and unstable	Moderate: Easier to train than GANs	High: Requires significant resources for long sequences
Data Generation Quality	High: Produces realistic and high-quality data	Moderate: May produce blurry reconstructions	High: Generates realistic sequential data
Anomaly Detection	Moderate: Effective with synthetic data generation	High: Good for detecting anomalies in complex data	High: Effective for sequential data anomalies
Real-time Processing	Low: Computationally intensive, not suitable for real-time	Moderate: Can be adapted for near real-time	Low: Sequential processing can be slow
Scalability	Moderate: Scales with hardware improvements	High: Less resource-intensive	Moderate: Scalability depends on sequence length
Model Stability	Low: Prone to mode collapse and training instability	High: Stable training process	Moderate: Requires careful tuning

Table 5.1: Comparison of Different Generative AI Techniques and Algorithms for Endpoint Security

Autoregressive models are most suitable for endpoint security because they can detect anomalies in sequential data accurately. They excel in analysing user behaviour and network traffic patterns, which is crucial for detecting complex threats. However, their complex training and real-time data processing limits necessitate careful planning and resource allocation.

V.DISSCUSSION

Generative AI in endpoint security can improve cyber threat identification and mitigation. With sophisticated malware, phishing assaults, and insider threats, traditional endpoint security methods typically fall behind. Advanced generative AI models like GANs, VAEs, and autoregressive models generate synthetic data, model complicated behaviours, and simulate attack patterns.

Comparing GANs, VAEs, and autoregressive models shows their pros and cons. GANs generate realistic, high-quality data, making them ideal for malware detection and phishing simulation. Their real-time applicability and scalability are limited by their high training difficulty, instability, and computing needs. Despite these challenges, their diverse data can improve endpoint security.

Probabilistic data encoding makes VAEs good at anomaly identification and log analysis. They are more suitable for real-time applications than GANs due to their consistent training process and low processing needs. However, generated data is usually lesser quality than GAN data, which can limit applications that require high-quality outputs.

Autoregressive models accurately recognize and model sequential data like user behaviour and network traffic patterns. This makes them effective for detecting insider threats and network breaches. However, their computational intensity and delayed data production hinder real-time processing and scalability. However, their capacity to record sequential data dependencies makes them useful for endpoint security.

The performance measurements show that each generative AI method has strengths and weaknesses. GANs and autoregressive models identify well, with autoregressive models performing better in sequential data situations. VAEs are ideal for situations that require constant performance without excessive processing load due to their moderate detection accuracy and good stability.

CONCLUSION AND FUTURE SCOPE

In this research, generative AI techniques improved endpoint security. Cyber threats are challenging traditional endpoint security, requiring innovative solutions. GANs, VAEs, and autoregressive models increase threat identification and mitigation in novel ways. Each model has pros and cons. GANs produce high-quality data and enhance training datasets but struggle with training complexity and real-time application. Despite lower data quality, VAEs are stable and detect anomalies. Autoregressive models are good in sequential data analysis and can detect insider threats and network breaches, but they are computationally intensive.

Comparative research and debate show that the optimum generative AI technique varies on security needs, computational resources, and threats. Endpoint security solutions can be strengthened, adapted, and improved by incorporating these methods.

Future scope

Future research should focus on many crucial areas to increase endpoint security with generative AI:

- **Improving GAN Training Stability and Efficiency:** Develop strategies to stabilize and minimize GAN computational needs for real-time applications.
- **Enhancing VAE Data Quality:** Design methods to improve VAE data fidelity.
- **Optimizing Autoregressive Model Computational Requirements:** Reduce computational needs for scalability and real-time processing.
- **Integration with Other AI-driven Security Measures:** Use generative AI with AI-driven frameworks for comprehensive defensive tools.
- **Real-world Implementation and Continuous Evaluation:** Test models in real-world settings to gain actionable insights.
- **Exploring Hybrid Models:** Combining GANs, VAEs, and autoregressive approaches could improve endpoint security performance and resilience.

Improvements in these areas will lead to more strong and adaptable endpoint security solutions that can combat growing cyber threats. Cybersecurity can improve digital asset and infrastructure protection by using generative AI.

REFERENCES

[1] Symantec. (2023). Internet Security Threat Report.
[2] Goodfellow, I., Bengio, Y. and Courville, A., 2016. *Deep learning*. MIT press.
[3] Hu, W. and Tan, Y., 2022, November. Generating adversarial malware examples for black-box attacks based on GAN. In *International Conference on Data Mining and Big Data* (pp. 409-423). Singapore: Springer Nature Singapore.
[4] Saxe, J. and Berlin, K., 2017. eXpose: A character-level convolutional neural network with embeddings for detecting malicious URLs, file paths and registry keys. *arXiv preprint arXiv:1702.08568*.
[5] McAfee. (2022). McAfee Labs Threats Report.
[6] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A. and Bengio, Y., 2014. Generative adversarial nets. *Advances in neural information processing systems*, *27*.
[7] Kingma, D.P. and Welling, M., 2013. Auto-encoding variational bayes. *arXiv preprint arXiv:1312.6114*.
[8] Van den Oord, A., Kalchbrenner, N., Espeholt, L., Vinyals, O. and Graves, A., 2016. Conditional image generation with pixelcnn decoders. *Advances in neural information processing systems*, *29*.
[9] Radford, A., Metz, L. and Chintala, S., 2015. Unsupervised representation learning with deep convolutional generative adversarial networks. *arXiv preprint arXiv:1511.06434*.
[10] Mirsky, Y., Doitshman, T., Elovici, Y. and Shabtai, A., 2018. Kitsune: an ensemble of autoencoders for online network intrusion detection. *arXiv preprint arXiv:1802.09089*.

[11] An, J. and Cho, S., 2015. Variational autoencoder based anomaly detection using reconstruction probability. *Special lecture on IE, 2*(1), pp.1-18.

[12] Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T. and Song, D., 2018. Robust physical-world attacks on deep learning visual classification. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 1625-1634).

[13] Al-Dujaili, A., Huang, A., Hemberg, E. and O'Reilly, U.M., 2018, May. Adversarial deep learning for robust detection of binary encoded malware. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 76-82). IEEE.

[14] Mehdi Gholampour, P. and Verma, R.M., 2023, April. Adversarial robustness of phishing email detection models. In *Proceedings of the 9th ACM International Workshop on Security and Privacy Analytics* (pp. 67-76).

[15] Pol, A.A., Berger, V., Germain, C., Cerminara, G. and Pierini, M., 2019, December. Anomaly detection with conditional variational autoencoders. In *2019 18th IEEE international conference on machine learning and applications (ICMLA)* (pp. 1651-1657). IEEE.

[16] Cesario, E., Catlett, C. and Talia, D., 2016, August. Forecasting crimes using autoregressive models. In *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 795-802). IEEE.

[17] Corsini, A., Yang, S.J. and Apruzzese, G., 2021, August. On the evaluation of sequential machine learning for network intrusion detection. In *Proceedings of the 16th International Conference on Availability, Reliability and Security* (pp. 1-10).