GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(Review Article)

Check for updates

Leveraging Generative Artificial Intelligence (AI) for cybersecurity: Analyzing diffusion models in detecting and mitigating cyber threats

Ayodele R. Akinyele [1, *], Oluwole Olakunle Ajayi [2], Geoffrey Munyaneza [1], Ugochukwu H.B. Ibecheozor [3] and Nakul Gopakumar [1]

[1] Kenan-Flagler Business School, University of North Carolina at Chapel Hill, North Carolina, USA.
[2] Community and Program Specialist, UHAI For Health Inc, Worcester, Massachusetts, USA.
[3] Darden School of Business, University of Virginia, Virginia, USA.

GSC Advanced Research and Reviews, 2024, 21(02), 001–014

Publication history: Received on 13 September 2024; revised on 28 October 2024; accepted on 30 October 2024

Article DOI: https://doi.org/10.30574/gscarr.2024.21.2.0408

Abstract

Due to the increased number of cyber dangers in today's digitally connected world, more advanced and flexible security measures have had to be created. Using generative artificial intelligence (AI), especially diffusion models, to find and stop cyber threats is investigated in this study. A new type of generative models called diffusion models have shown great promise in many areas, including picture creation and natural language processing. The purpose of this study is to look at their use in cybersecurity, especially for finding strange patterns, predicting future threats, and stopping attacks as they happen. The study utilized five scientific databases and a systematic search strategy to identify research articles on PubMed, Google Scholar, Scopus, IEEE, and Science Direct relating to the topic. Furthermore, books, dissertations, master's theses, and conference proceedings were utilized in this study. This study encompassed all publications published until 2024. Through a thorough study of the diffusion model's structure and how it can be applied to cybersecurity issues, we look at how these models can improve current systems for finding threats. Additionally, we talk about their ability to add to datasets by creating fake data, which makes anomaly detection more accurate in cyberattack cases that aren't well represented. Due to their stability and ability to predict, diffusion models are seen as a useful tool for finding complex threats like advanced persistent threats (APTs) and zero-day attacks. Some problems still exist, though, such as the need for a lot of computing power, models that are hard to understand, and the fact that online threats are always changing. This article suggests avenues for future study and talks about how diffusion models might change the way cybersecurity is done.

Keywords: Cybersecurity; Artificial Intelligence; Threats; Diffusion models; Attacks

1 Introduction

Transformational technologies-based generative AI algorithms could create new material based on data trends. Generic artificial intelligence (Gupta et al., 2024) makes data instances that are very similar to real-world inputs, while traditional machine learning models focus on categorizing or predicting outcomes. According to Ajayi et al. (2024) and Davies et al. (2024), this skill changes the way people are creative in many areas, including art, music, literature, medicine, and more. In parallel, traditional machine learning models have been successfully applied in scientific domains such as health (Mudele et al., 2021a, Mudele et al., 2021b).

Generative artificial intelligence can make people more creative, make content creation easier, and improve data synthesis, which leads to new uses and better efficiency (Al Naqbi et al., 2024). Differentiated data creation is what makes diffusion models interesting as generative models. If you want to get data back from doubt, diffusion models use a gradual noise process and a learning reverse process. Popular generative models like variational autoencoders and

[*] Corresponding author: Ayodele R. Akinyele

Generative Adversarial Networks (GANs) are different from this method. Along with a discriminator, a generator in a game-theoretic framework creates accurate data and tells the difference between generated and real-world data in GANs (Salehi et al., 2020). Virtual assistants use statistical methods to store data in a hidden space for future samples. Different uses of GANs and VAEs have shown that they work, but diffusion models are more stable and produce better results, especially in situations with a lot of dimensions (Pandey et al., 2022).

They are therefore useful for making future generative jobs better. Growing as the digital world changes, online threats become a major issue. With the deployment of advanced methods by hackers to exploit system and network vulnerabilities, the frequency and severity of cyberattacks are on the rise (Jimmy, 2024). These dangers include ransomware, hacking, DDoS attacks, and advanced persistent threats (APTs) that stay hidden and keep attacking. AI-powered solutions that can find and stop threats in real time are in high demand because they are getting more complicated (Obi et al., 2024,000). Because standard security measures don't always work with cybercriminals' changing tactics, it is important to use advanced AI technologies that can learn from and respond to these changing threats (Bécue et al., 2021).

Although online threats are getting more complicated, the problem statement stresses the need for new ways to find and stop them. Regular security measures might not be able to keep up with how online threats change, leaving businesses open to harm and unprotected. Some signature-based detection systems don't pick up on new attack vectors, especially when it comes to evasion methods (Mallick and Nath, 2023) even though they can pick up on known threats.

For cybersecurity strategies to keep up with the ever-evolving threats (Sarker, 2024), they need to include creative AI. According to this study, diffusion models, a type of generative artificial intelligence, might be able to help make defence better. Finding and handling cyber risks can be made easier by looking into the unique features of diffusion models in this study. This creates new ways to find anomalies, combine data, and predict threats. In this essay, we look at diffusion models and how they can be used in cybersecurity to show how new technologies can be used to create strong security systems that can change as cyber risks alter. By showing how important advanced creative methods are for keeping digital assets safe in today's dangerous cyber world, it adds to the conversation about artificial intelligence in cybersecurity.

2 Literature Search

The study utilized five scientific databases and a systematic search strategy to identify research articles on Leveraging Generative AI for Cybersecurity: Analysing Diffusion Models in Detecting and Mitigating Cyber Threats (PubMed, Google Scholar, Scopus, IEEE, and Science Direct) (Zhao *et al*., 2020). Furthermore, there were books, dissertations, master's theses, and conference proceedings. The search terms "Cyber security" and the keywords "Generative AI," and "Diffusion model" were inputted into the search engine. An exhaustive list of abstracts was acquired and scrutinized for the present study; any publications meeting the inclusion criteria were thoroughly investigated. The review encompassed all publications published until 2024.

3 Results

3.1 What is Generative AI?

This kind of AI makes data that looks like data from the real world. Generative AI doesn't sort data or guess what it will be; it makes new text, images, sounds, and videos. Bandi et al. (2023) say that this power has changed many things by making people more creative, making things run more smoothly, and giving people useful fake data for many things. As AI gets better, it has helped singers, artists, and designers find new ways to present their work. Users of DALL-E and Midjourney can turn words into art, which gives them more ways to be creative. Based on Zhou and Lee (2024), generative AI can write scripts, make songs, and make levels for video games. This helps find new ways to play games and tell stories.

Generative AI can be used for more than just making things. It can also be used in data science and analytics. Abumalloh et al. (2024) say that companies can train machine learning models without letting private data get out by making fake datasets that look like real-world data patterns. This is very useful in healthcare, where it's important to keep patient information secret. Natural language processing (NLP) is better with generative AI because it can write like a person, translate languages, and summarize data (Obaid et al., 2021).

Generative AI looks for patterns in data and makes new samples based on those patterns. These models can learn the subtleties of the input data so that they can produce statistically close results by using more than one training method. Alwahedi et al. (2024) say that the fact that generative AI can copy makes it a powerful tool for progress and creativity in all those areas.

3.2 Understanding Diffusion Models

Different from other creative AI methods, diffusion models create data in a uniquely different way. Models of diffusion use probabilistic processes to create data by simulating increasing noise. In many steps, noise is slowly added to a dataset until it can't be told apart from pure noise (Zhang et al., 2023). Training the model to make the original data from the noisy version reverses the process of noise. This two-step process turns random noise into clear data instances, which lets the model make new samples (Ble, 202<). You can make diffusion models with Markov chains, where each step represents a change in the state of the data. Although the forward diffusion process messes up data, the reverse process uses samples from a learned distribution to fix it. (Wang et al., 2024) says that this method models random events using statistics and machine learning.

As compared to GANs and VAEs, diffusion models are better. Using GANs, a generator and a discriminator fight to make realistic data and tell the difference between real and generated samples. For example, Sharma et al. (2024) say that this strong adversarial training can lead to mode breakdown and generator instability with little output variety. Virtual reality encodes information into a hidden space and then takes samples from that space to make new instances. Achieving high precision makes VAEs less accurate when trying to fit complicated distributions.

These issues can be fixed by diffusion models that improve training stability and product quality. For richer and more diversified outputs, diffusion models use denoising to create more detailed data (Cao et al., 2024). Dielectric models are widely used in picture production and other fields because they are stable and good.

3.3 Applications of Diffusion Models

Diffusion models are appearing in more and more new areas, showing how flexible they are and how well they can produce good data. Yang et al. (2023) says that one of the key uses is to make images. It's amazing how creatively and accurately DALL-E 2 and Stable Diffusion can use diffusion methods to turn text into photorealistic images. These models might make pictures that have their own artistic styles and look like real things, which can help people understand difficult ideas (Patil et al., 2024).

Artificial neural networks (NLP) are testing diffusion models to see how well they can create text that makes sense and fits the situation. These models can write creatively, make content, and react like people because they understand language structures and semantics (Filippo et al., 2024). From these skills come chatbots, automated stories, and content creation for marketing and social media.

Cybersecurity uses of diffusion models go beyond these uses. As cyberattacks get smarter, fake data that shows attack routes can help find threats more quickly (La Salle, 2023). Utilizing generative cyberattack simulations, businesses can teach their AI systems to recognize and react to unusual events. In cybersecurity, diffusion models can help make strong training datasets that let systems learn from a wide range of situations, such as new or unusual threats (Sai et al., 2024).

Additionally, diffusion models are a strong and flexible creative AI technique. Their unique design, longevity, and ability to produce high-quality data make them useful tools in both the arts and cybersecurity (Jamal, 2024). As study and development go on, diffusion models are ready to stimulate new ideas and tackle tough digital problems (Shibeika and Harty, 2015).

4 The Cybersecurity Landscape

4.1 Overview of Cyber Threats

Cybersecurity is getting harder to understand and more dangerous for people, businesses, and countries. There is a different way to attack and a different effect for each type of computer threat. Admass et al. (2023) say that malware, ransomware, scams, and DDoS attacks happen all the time.

Malware is computer software that attacks, hurts, or stops working devices, networks, and computers. Malicious viruses, worms, Trojans, and spyware take advantage of weak spots in systems (Akinde et al., 2021). Ransomware has recently become popular because it locks files and asks for money to unlock them. Because this attack can stop work and cost money, cybercriminals love it (Ryan, 2021). Phishing is another common cyber threat. It looks like real email but is trying to steal your login information or bank information. Gururaj et al. (2024) say that social engineering that uses psychological tricks is especially sneaky. DDoS attacks, on the other hand, send a lot of data to a target's server, service, or network, stopping it from working and stopping services.

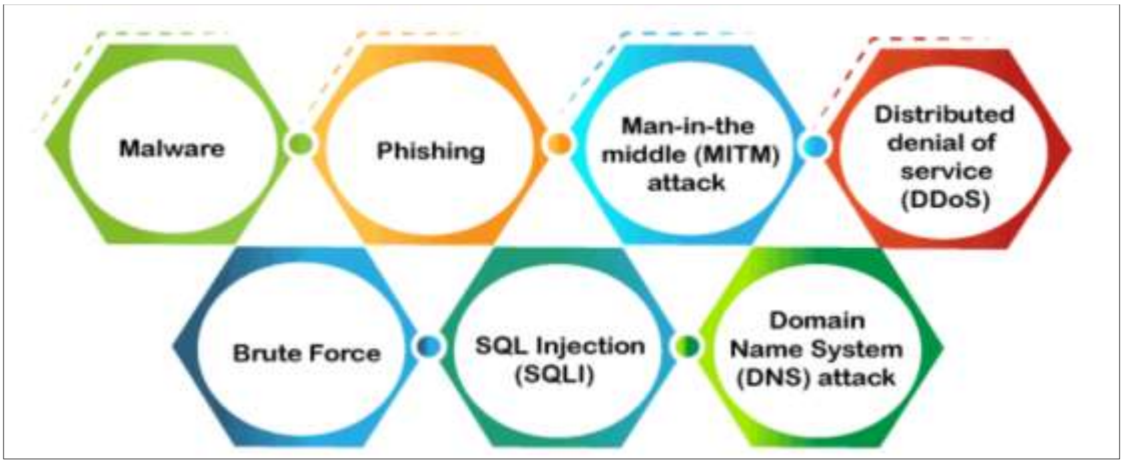
Malware
Phishing
Man-in-the middle (MITM) attack
Distributed denial of service (DDoS)
Brute Force
SQL Injection (SQLI)
Domain Name System (DNS) attack

Figure 1 Types of Cyber threats (Li and Liu, 2021)

As cybercriminals get smarter, they use APTs and zero-day attacks. Well-resourced adversaries start coordinated APTs against specific organisations or industries to steal sensitive data over time (Sfetcu, 2024). Attackers use stealth to get into systems that have been hacked without being seen. Zero-day exploits are software flaws that neither sellers nor the public know about (Waheed et al., 2024) Because there are no fixes or defenses in place at the time of the attack, these flaws could let attackers get in without permission and cause damage before any security measures are put in place. To stop these computer threats from getting smarter and more varied, we need more advanced ways to find them and stop them.

4.2 Existing AI Solutions in Cybersecurity

In cybersecurity, where risks are always changing, AI has made it much easier to find problems and deal with them. To find bad trends, Jada and Mayayise (2023) say that deep learning and machine learning are types of AI that look at a lot of data. More complex systems that look at past data are taking the place of rule-based models that use known threat signatures. Anomaly detection systems are a big step forward in defence artificial intelligence, say Jada and Mayayise (2023). They're supposed to find odd behaviour that could mean there was a breach. The algorithms used in behavioural analytics help companies that use them find users who are acting in strange ways. Deep learning-based systems that collect threat intelligence look at a lot of different sources of data to find new holes and ways to attack.

Defence AI models have a lot of issues, even though they can be useful. The issue of accuracy remains important, despite the potential of artificial intelligence to lower false positives (Kaur, 2023). Bad labelling can keep threats from being found or set off alarms when security staff are already worn out. The study by Oyinloye et al. (2024) inquires whether AI models can adapt to new dangers. Because hackers are always changing how they do things, AI systems need to be able to spot patterns and draw conclusions from small groups of data. To find new ways to fight threats that aren't already known, you need to be able to adapt (Bordeanu, 2024). The fact that models of artificial intelligence can be described makes defense even harder. In important situations, experts need to know how a model makes choices because the wrong readings can lead to very bad outcomes (Sindiramutty et al., 2024). AI models and deep learning systems often behave like "black boxes," which makes it tough to understand how they decide what to do (Rudin, 2019).

4.3 Why We Need Generative AI in Cybersecurity

Generative artificial intelligence needs to be a part of cybersecurity tactics because cyberthreats are getting more complicated. Traditional detection systems that use AI have a hard time keeping up with how quickly hacks change, so models need to be able to adapt and generalize well. As Abdulhussein (2024) says, generative AI, especially when used with diffusion models, might be able to solve these problems well.

Generative artificial intelligence programs make fake data that looks like real-world dangers. This feature makes it easier to create large and detailed training sets, which can help machine learning systems recognize different attack paths, even ones that are new or haven't been seen before (Pezoulas et al., 2024). Generative AI models are getting better, which helps make security better and gives organizations better tools to prepare for possible future risks. De Azambuja et al. (2023) use to plan cyberattacks.

Artificial intelligence models that generate new ideas must be able to change to the constantly changing world of cybersecurity. Kaur et al. (2023) say that these models can be taught to recognize and stop new attack methods, which makes security strong and effective. The utilisation of synthetic attack data allows organisations to thoroughly assess and confirm the effectiveness of their security systems, thereby enhancing their defensive measures and reaction protocols (Steingartner et al., 2023). Being that cyberthreats are so complicated, it is important to use new and flexible ways to find them. Gupta et al. (2024) say that generative artificial intelligence could change the way cybersecurity is done because it can create coherent data and react to different environments. Generative models allow organisations to enhance their ability to spot and react to threats, thereby fortifying their cybersecurity frameworks in a challenging digital landscape (Dhoni and Kumar, 2023).

5 Detecting and Mitigating Cyber Threats with Diffusion Models

5.1 How Diffusion Models Work in Detecting Cyber Threats

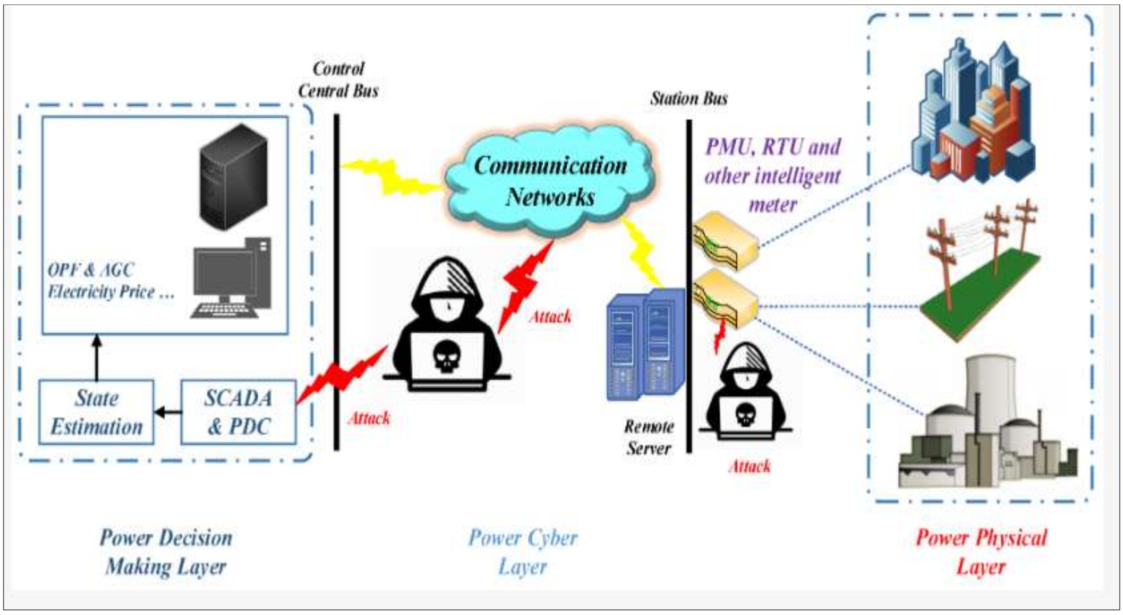

Figure 2 How Cybersecurity works (Almalaq et al., 2022)

Diffusion models are changing cybersecurity, especially finding strange things. Seeing strange behaviour can be a sign of cyber threats like unauthorized entry, data theft, or system intrusions. They can learn complex data distributions and spot "normal" behaviour in a dataset, making diffusion models powerful (Shyaa et al., 2024).

In anomaly detection, network traffic, user behaviours, and system logs are used to train diffusion models. The model learns to recognize complicated patterns of behaviour during training. Understanding normal operational metrics is easier when you teach the model to make fake samples that match this trend (Veres and Moussa, 2019). As new data comes into the model, it can check it against the rules that were already set. Security experts are aware of possible threats when there are big changes from the norm. Furthermore, to finding problems, diffusion models can improve datasets and create fake data (Wang et al., 2021). Lack of data for new or rarely occurring types of attacks hurts defence. By making new cyber threats, generational diffusion models improve threat detection algorithms and add to training datasets. This method gets AI systems ready to find both common and unusual ways to fight (Chougule, 2024). By making fake data that mimics both normal and abnormal behaviours, diffusion models make machine learning systems stronger. To make detection systems work better, the model can come up with believable versions of a rare attack based on what it knows about existing data (Truong et al., 2024). With this proactive cybersecurity method, businesses can get ready for threats before they happen.

5.2 Case Study: Diffusion Models in Malware Detection

In the area of malware detection, diffusion models show that they can find and deal with new types of malwares (Elingiusti et al., 2018). As software gets smarter, and threats get more complicated, old static signature-based methods are losing their power. Instead of using fingerprints, diffusion models look at how malware acts and can be used in several situations (Ashawa and Morris, 2021).

It is possible for diffusion models to be taught on datasets that contain both good and bad software behaviour. By looking at how legal applications behave and comparing them to malware patterns, the model can successfully find malware, even new versions that may come up (Karyotis and Khouzani, 2016). For example, diffusion models can look at the parallels and differences between a new type of ransomware and other types of malwares that are already out there. New research suggests that diffusion models can effectively find malware that acts in strange ways. When observed behaviours are used to make fake malware samples, an accurate training environment can be created that helps the model understand new malware strains (Amer et al., 2021). It is possible to make malware identification faster and more accurate by using diffusion models. The model finds patterns in how malware acts, which lets it prioritize alerts based on how important they are. This makes incident reaction more effective (Jacob, 2022). The model can let the officials know when a new strain of malware shows signs of being a high-risk variant. This speeds up the response and prevention efforts.

5.3 Diffusion Models for Real-Time Threat Mitigation

The power of diffusion models to make predictions could help protect against real-time cyber threats. According to Gonaygunta (2023), these algorithms are always looking for problems in the streams of arriving data and alerting security staff to possible threats. Real-time deviation spotting lets businesses act quickly on new risks, often before they do a lot of damage. Diffusion models help find dangers early and stop attacks before they happen. To keep services running, security teams can handle, or shift network traffic spikes caused by DDoS. Because quick responses are so important, these predictive skills help vital infrastructure and financial institutions (Islam et al., 2022).

Diffusion models can be used to guess threats and attack trends. These algorithms look at data from past attacks and observations from the present to find trends that suggest hackers might use new attack methods (Apruzzese et al., 2022). Businesses can improve their security and get ready for new threats when they know this. Cybersecurity systems that use predictive analytics make it easier to find threats and make choices (Nassar and Kamal, 2021). Diffusion models help security teams figure out the best way to send resources to high-risk areas. Threat mitigation makes security better and more flexible so it can change to new cyber threats.

5.4 Diffusion Models in Dealing with Advanced Persistent Threats (APTs)

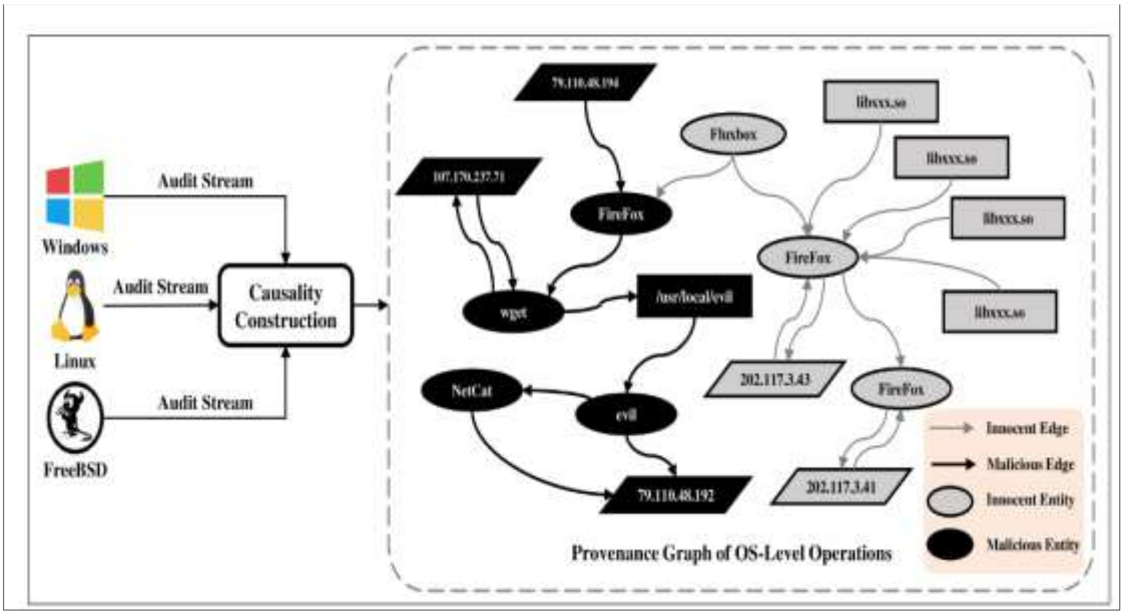

Figure 3 An Overview of Provenance Graph-Based APT Audit Approach (Wang et al., 2024)

Advanced Persistent Threats, or APTs, are a big threat to cybersecurity because they are very smart and take a long time to target specific companies. APTs get into systems and hide for a long time by being quiet, patient, and using advanced techniques (Sfetcu, 2024). By looking at huge amounts of data and finding trends related to APTs, diffusion models can find and lower APT risks. To find APTs correctly, diffusion models need to be trained on datasets that are known to be safe (Benabderrahmane et al., 2024). These models can find small signs of APT activity, like moving networks laterally, seeing strange access patterns, and finding ways to steal data that regular security systems miss. It could lead to a review if an employee looks at private files when they're not at work.

When looking for an APT, diffusion models may be able to pick up on network lateral motions early on. Once attackers get into a network, they often move around it looking for information or entry permissions (Karam, 2022). By finding the right user behaviour, training diffusion models helps security teams find lateral movement. This let’s help be given quickly, before big problems happen (Gragg, 2003). Models of diffusion map APT TTPs. By looking at past data and simulating attack situations, these models help companies understand APTs and build defences against them (Wang, 2020). Companies can use predictive analysis to make security measures that are resistant to APTs.

6 Challenges in Implementing Diffusion Models in Cybersecurity

6.1 Data Privacy and Security

Data security and privacy make it harder for cybersecurity diffusion ideas to work. Diffusion models need a lot of data, such as personal information (PII), financial records, and secret information about an organization. People worry about their privacy when it comes to these private data because leaks or unauthorized access could hurt people and businesses (Li and Liu, 2021). Law and morality make things more difficult. The GDPR and CCPA put limits on how businesses can use sensitive information. These rules cover things like openness, agreement, and erasure of data processing, which could make it harder for businesses to use AI safely (Dos Santos, 2020). Because of problems with not following the rules, companies might not want to share data used to train models and find it hard to create AI-based security solutions (Wall, 2021).

When private data is used to train AI algorithms, it raises ethical questions. Companies need to deal with who owns the data, getting informed agreement, and biases in the dataset. If you train diffusion models on biased or uniform data, they might keep their biases and miss threats. So, cybersecurity groups that use diffusion models need to deal with risks to data privacy and security (Tatineni, 2019).

6.2 Computational Resources

Cybersecurity diffusion models are hard to use because training big models is very time-consuming and computer intensive. As Munoz (2023) says, GPUs or TPUs are needed for diffusion models that work with large datasets or complicated designs. This system can be hard for businesses that are small or don't have a lot of money. It takes time, energy, and tools to train a diffusion model. Li et al. (2023) say that training deep learning models takes a long time because they need to be changed and improved a lot. Businesses might not use these advanced technologies because they need a lot of resources, and their IT goals may not be compatible. The cloud, which can grow or shrink based on needs, can help businesses fix these problems. Cloud-based options are hard to use because of problems with data security, managing vendors, and following rules (Padhy, 2011). More computer resource-intensive diffusion models need to be used in defence.

6.3 Explainability and Trust in AI Systems

Diffusion models and cybersecurity solutions that are powered by AI make it harder to understand and trust. Interpreting model decisions is the main job. Afroogh et al. (2024) say that diffusion models and many other deep learning systems are "black boxes," which makes it hard to understand the findings. Lack of openness can make people less likely to trust a system, especially when mistakes could have very bad results.

Cybersecurity decision-makers must figure out what model results mean. It's not okay for security teams to follow a model's advice if they don't know why it saw a threat or an unusual event. AI-enhanced security could be limited by a lack of faith, which could slow down responses or reject model results (Villadiego, 2020). Organizations should prioritize AI systems that can be explained to build trust and human control. With openness frameworks, security teams can put model decisions in their proper context (Hamon et al., 2020). By showing model output effects, feature importance analysis helps people trust AI-driven protection solutions more. As Binhammad et al. (2024) say, giving human operators knowledge that they can understand will improve how AI systems and security staff work together and how they respond to cyber threats.

6.4 Evolving Nature of Cyber Threats

Because cyber dangers change over time, it can be hard to use cybersecurity diffusion models. According to Safitra (2023), cybercriminals are always changing their methods, which makes it hard to use diffusion models to find and deal with new threats. Without new data and threat intelligence, models may become useless when hackers hit without warning. Companies need to find ways to use methods of sharing that include ongoing learning. According to Labu and Ahammed (2024), feedback loops can teach the model again with new threat data so that it can change to new attack patterns.

Threat intelligence streams give organizations information about flaws, exploits, and malware in real time. During training, this information helps diffusion models find new threats and strange things. Putting together threat intelligence data is hard because companies must make sure it is correct, up-to-date, and useful (Li and Liu, 2021).

7 Case Studies and Applications

7.1 Case Study 1: Diffusion Models in Network Intrusion Detection

The diffusion models in network intrusion detection tools have made security better. Invasions of a network include getting in without permission, stealing data, and DDoS attacks. It's possible that old breach detection systems won't be able to find new ways to attack. In comparison, diffusion models use data to find strange network traffic patterns (Ullah et al., 2024). A lot of data sets showing how networks usually act in different situations were used to train diffusion models. The size, frequency, source and destination IP addresses, and protocol types of packets are used by this model to learn regular traffic trends. Tang et al. (2023) says that after training, the software mimics network behavior to find intrusions. The model was tried for port scans, DDoS attacks, and advanced invasions in a controlled setting. This diffusion model found these dangers while limiting alerts from harmless events like normal maintenance or changes in how users behave (Tidjon, 2020).

Alert fatigue from high false positive rates limits cybersecurity teams' ability to react to serious assaults (Mikkelsen and Seljåsen, 2024). Diffusion models make intrusion detection more accurate and efficient, so security pros can focus on real threats instead of false alarms (Apruzzese et al., 2022). This example shows how diffusion models make networks safer, which is why they are important for modern defence.

7.2 Case Study 2: Diffusion Models for Phishing Detection

Phishing still takes important data from businesses, but the methods used are getting smarter. Diffusion models look at and make examples of phishing emails and websites to help with detection (Harrison et al., 2016). In a recent case study, researchers used real and fake emails to train a spread model. Phishing was found with the help of language, URLs that looked sketchy, and sender names that didn't make sense. Using fake emails, the model added new and different types of phishing to the training set (Das, 2021a).

It worked to use the diffusion model to sort emails. It was the algorithm that was better at finding phishing emails than keyword recognition and heuristic analysis (Salloum et al., 2022). Gallo et al. (2024) say that the diffusion method looks at email structure, metadata, and content to find phishing before people see any harmful content.

The model also worked even as hacking methods changed, the study found. The screening system stays useful even as attackers get better thanks to the diffusion model's ability to make new phishing samples (Frauenstein and Flowerday, 2020). This feature protects people and cuts down on fake emails sent to end users, which makes the job of IT and security experts easier (DeWitt, 2007).

8 Future of Generative AI and Diffusion Models in Cybersecurity

8.1 Emerging Trends

In the field of cybersecurity, generative AI, especially diffusion models, will grow as new technologies are developed and threats change. These days, popular mixed models use both reinforcement learning and diffusion learning. By trying things out and learning from them, reinforcement learning makes it easier for diffusion models to find danger in real time (Zhang et al., 2021).

Diffusion models can learn from their mistakes and spot problems with the help of reinforcement learning. Using blockchain technology, security solutions could keep data safe, handle it in a clear way, and model interactions. Khan et al. (2021) says that decentralized blockchains can keep track of and protect diffusion model input data from being changed.

In cybersecurity, this is important because trust in data changes how well models work. As Daah et al. (2024) say, blockchain can protect model changes and data access, encouraging a team-based hacking approach that puts responsibility and openness first. Putting together anomaly detection systems that look for and deal with threats using a variety of models, such as diffusion models, is becoming more common. Figuring out how networks work with model information helps businesses find and lower cyber threats (Dey, 2022). These improvements show that generative AI will help make cybersecurity strategies that work better and change as needed.

8.2 The Role of Policy and Regulation

Using generative AI in defence needs rules and laws. Guidelines for ethical and legal AI use in this area need to be set up by the government and regulated. (Humphreys et al., 2024) says that companies that sell cybersecurity solutions that use AI must follow rules about privacy, algorithmic bias, and responsibility. To solve generative AI's problems, lawmakers, AI researchers, and cybersecurity experts need to work together. This can encourage the use of sensible cybersecurity diffusion models by creating best practices for model training, data handling, and risk assessment (Fui-Hoon Nah et al., 2023). A discussion with relevant parties can show the dangers of generative AI and suggest ways to reduce them.

Allowing users and stakeholders to trust AI models requires that they can be explained and understood. For cybersecurity experts to be able to analyse diffusion model results (Díaz-Rodríguez et al., 2023), AI decision-making transparency requirements are mandatory. According to these rules, cybersecurity AI apps should be fair and not favour some people over others. Lawmakers need to change their rules to deal with the new problems that generative AI technology brings to this quickly changing world (Petersen et al., 2022). To ethically use generative AI, stakeholders must encourage creativity and ethics in cybersecurity rules.

9 Conclusion

Diffusion models can change how cyber threats are found and how they are dealt with. Cyber threats that are complicated and broad need creative solutions. Diffusion models change the way cybercrime is stopped by using high-quality data and real-time anomaly spotting. Generative AI, especially diffusion models, can help businesses do more than just use signatures to find things. Even small changes in behaviour that could be signs of an attack can be picked up by synthetic data. With a better and more data-driven method to detection accuracy and false positives, cybersecurity teams can focus on what's important. Lastly, generative AI and diffusion models in cybersecurity start a new age of being proactive about stopping threats. Companies can plan better and take fewer risks when they understand this technology. If we use these new ideas, cybersecurity might get better, which would make the internet safer for people and companies. Learning about diffusion models helps us make the future of safety more stable, flexible, and useful.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdulhussein, M. (2024). The Impact of Artificial Intelligence and Machine Learning on Organizations Cybersecurity. Liberty University.

[2] Abumalloh, R. A., Nilashi, M., Ooi, K. B., Tan, G. W. H., & Chan, H. K. (2024). Impact of generative artificial intelligence models on the performance of citizen data scientists in retail firms. *Computers in Industry*, *161*, 104128.

[3] Admass, W. S., Munaye, Y. Y., & Diro, A. (2023). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 100031.

[4] Afroogh, S., Akbari, A., Malone, E., Kargar, M., & Alambeigi, H. (2024). Trust in AI: Progress, Challenges, and Future Directions. *arXiv preprint arXiv:2403.14680*.

[5] Ajayi, O. O., Wright-Ajayi, B., Mosaku, L. A., Davies, G. K., Moneke, K. C., & Adeleke, O. R. Enhancing Infectious Disease Management in Nigeria: The Role of Artificial Intelligence in Diagnosis and Treatment. *Clin Case Rep Int. 2024; 8, 1670*.

[6] Ajayi, O. O., Wright-Ajayi, B., Mosaku, L. A., Davies, G. K., Moneke, K. C., Adeleke, O. R., ... & Mudele, O. (2024). Application of satellite imagery for vector-borne disease monitoring in sub-Saharan Africa: An overview. *GSC Advanced Research and Reviews*, *18*(3), 400-411.

[7] Akinde, O. K., Ilori, A. O., Afolayan, A. O., & Adewuyi, O. B. (2021). Review of computer malware: detection and preventive strategies. *Int. J. Comput. Sci. Inf. Secur.(IJCSIS)*, *19*, 49.

[8] Al Naqbi, H., Bahroun, Z., & Ahmed, V. (2024). Enhancing work productivity through generative artificial intelligence: A comprehensive literature review. *Sustainability*, *16*(3), 1166.

[9] Almalaq, A., Albadran, S., & Mohamed, M. A. (2022). Deep machine learning model-based cyber-attacks detection in smart power systems. *Mathematics*, *10*(15), 2574.

[10] Alwahedi, F., Aldhaheri, A., Ferrag, M. A., Battah, A., & Tihanyi, N. (2024). Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. *Internet of Things and Cyber-Physical Systems*.

[11] Amer, E., Zelinka, I., & El-Sappagh, S. (2021). A multi-perspective malware detection approach through behavioral fusion of api call sequence. *Computers & Security*, *110*, 102449.

[12] Apruzzese, G., Andreolini, M., Ferretti, L., Marchetti, M., & Colajanni, M. (2022). Modeling realistic adversarial attacks against network intrusion detection systems. *Digital Threats: Research and Practice (DTRAP)*, *3*(3), 1-19.

[13] Apruzzese, G., Andreolini, M., Ferretti, L., Marchetti, M., & Colajanni, M. (2022). Modeling realistic adversarial attacks against network intrusion detection systems. *Digital Threats: Research and Practice (DTRAP)*, *3*(3), 1-19.

[14] Ashawa, M., & Morris, S. (2021). Analysis of mobile malware: a systematic review of evolution and infection strategies.

[15] Bandi, A., Adapa, P. V. S. R., & Kuchi, Y. E. V. P. K. (2023). The power of generative ai: A review of requirements, models, input–output formats, evaluation metrics, and challenges. *Future Internet*, *15*(8), 260.

[16] Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*, *54*(5), 3849-3886.

[17] Benabderrahmane, S., Hoang, N., Valtchev, P., Cheney, J., & Rahwan, T. (2024). Hack me if you can: Aggregating autoencoders for countering persistent access threats within highly imbalanced data. *Future Generation Computer Systems*, *160*, 926-941.

[18] Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L. H. (2024). The Role of AI in Cyber Security: Safeguarding Digital Identity. *Journal of Information Security*, *15*(02), 245-278.

[19] BLE, Z. A. I. (2023). Generative adversarial networks for ambient music creation: enhancing creative installations with AI-driven soundscapes.

[20] Bordeanu, O. C. (2024). From Data to Insights: Unraveling Spatio-Temporal Patterns of Cybercrime using NLP and Deep Learning (Doctoral dissertation, UCL (University College London)).

[21] Brooks, C. (2024). Inside Cyber: How AI, 5G, IoT, and Quantum Computing Will Transform Privacy and Our Security. John Wiley & Sons.

[22] Cao, H., Tan, C., Gao, Z., Xu, Y., Chen, G., Heng, P. A., & Li, S. Z. (2024). A survey on generative diffusion models. *IEEE Transactions on Knowledge and Data Engineering*.

[23] Chen, M., Mei, S., Fan, J., & Wang, M. (2024). An overview of diffusion models: Applications, guided generation, statistical rates and optimization. *arXiv preprint arXiv:2404.07771*.

[24] Chougule, A. U. (2024). Artificial intelligence enabled vehicular vision and service provisioning for advanced driver assistance systems (ADAS) (Doctoral dissertation, BITS PILANI, Pilani campus).

[25] Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing zero trust models in the financial industry through blockchain integration: A proposed framework. *Electronics*, *13*(5), 865.

[26] Das, R. (2024). Generative AI: Phishing And Cybersecurity Metrics. CRC Press.

[27] Davies, G. K., Ajayi, O. O., Wright-Ajayi, B., Mosaku, L. A., Moneke, K. C., Adeleke, O. R., ... & Mudele, O. (2024). Unravelling the complexity of environmental exposures and health: A novel exposome-centered framework for occupational and environmental epidemiology. *GSC Advanced Research and Reviews*, *19*(1), 026-032.

[28] De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics*, *12*(8), 1920.

[29] DeWitt, A. J. A. G. (2007). *Usability issues with security of electronic mail* (Doctoral dissertation, Brunel University, School of Information Systems, Computing and Mathematics).

[30] Dey, A. (2022). Datascience in support of cybersecurity operations: Adaptable, robust and explainable anomaly detection for security analysts (Doctoral dissertation, Ecole nationale supérieure Mines-Télécom Atlantique).

[31] Dhoni, P., & Kumar, R. (2023). Synergizing generative ai and cybersecurity: Roles of generative ai entities, companies, agencies, and government in enhancing cybersecurity. *Authorea Preprints*.

[32] Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, 101896.

[33] Dos Santos, A. P. (2020). The Impact of Artificial Intelligence on Data Protection: A Legal Analysis.

[34] Elingiusti, M., Aniello, L., Querzoni, L., & Baldoni, R. (2018). Malware detection: A survey and taxonomy of current techniques. *Cyber threat intelligence*, 169-191.

[35] Filippo, C., Vito, G., Irene, S., Simone, B., & Gualtiero, F. (2024). Future applications of generative large language models: A data-driven case study on ChatGPT. *Technovation*, *133*, 103002.

[36] Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & security*, *94*, 101862.

[37] Fui-Hoon Nah, F., Zheng, R., Cai, J., Siau, K., & Chen, L. (2023). Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration. *Journal of Information Technology Case and Application Research*, *25*(3), 277-304.

[38] Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers & Security*, *139*, 103671.

[39] Gonaygunta, H. (2023). Factors Influencing the Adoption of Machine Learning Algorithms to Detect Cyber Threats in the Banking Industry. University of the Cumberlands.

[40] Gragg, D. (2003). A multi-level defense against social engineering. *SANS Reading Room*, *13*, 1-21.

[41] Gupta, R., Nair, K., Mishra, M., Ibrahim, B., & Bhardwaj, S. (2024). Adoption and impacts of generative artificial intelligence: Theoretical underpinnings and research agenda. *International Journal of Information Management Data Insights*, *4*(1), 100232.

[42] Gururaj, H. L., Janhavi, V., & Ambika, V. (Eds.). (2024). *Social Engineering in Cybersecurity: Threats and Defenses*. CRC Press.

[43] Hamon, R., Junklewitz, H., & Sanchez, I. (2020). Robustness and explainability of artificial intelligence. *Publications Office of the European Union*, *207*, 2020.

[44] Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, *40*(2), 265-281.

[45] Humphreys, D., Koay, A., Desmond, D., & Mealy, E. (2024). AI hype as a cyber security risk: the moral responsibility of implementing generative AI in business. *AI and Ethics*, 1-14.

[46] Islam, U., Muhammad, A., Mansoor, R., Hossain, M. S., Ahmad, I., Eldin, E. T., ... & Shafiq, M. (2022). Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. *Sustainability*, *14*(14), 8374.

[47] Jacob, S. (2022). Enhancing cyber attack prevention and detection using application process tracing.

[48] Jada, I., & Mayayise, T. O. (2023). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, 100063.

[49] Jamal, S. (2024). Applications of Predictive and Generative AI Algorithms: Regression Modeling, Customized Large Language Models, and Text-to-Image Generative Diffusion Models.

[50] Jimmy, F. N. U. (2024). Cyber security Vulnerabilities and Remediation Through Cloud Security Tools. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 129-171.

[51] Karam, R. (2022). Automatic detection of business data anomalies with deep learning and application to the ADS-B protocol (Doctoral dissertation, Université Bourgogne Franche-Comté).

[52] Karyotis, V., & Khouzani, M. H. R. (2016). Malware diffusion models for modern complex networks: theory and applications. Morgan Kaufmann.

[53] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804.

[54] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804.

[55] Khan, A. A., Khan, M. M., Khan, K. M., Arshad, J., & Ahmad, F. (2021). A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. *Computer Networks*, *196*, 108217.

[56] La Salle, A. (2023). On Stochastic Modeling Applications to Cybersecurity: Loss, Attack, and Detection (Doctoral dissertation, Arizona State University).

[57] Labu, M. R., & Ahammed, M. F. (2024). Next-Generation cyber threat detection and mitigation strategies: a focus on artificial intelligence and machine learning. *Journal of Computer Science and Technology Studies*, *6*(1), 179-188.

[58] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

[59] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

[60] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

[61] Li, Y., Gao, H., Gao, Y., Guo, J., & Wu, W. (2023). A survey on influence maximization: From an ml-based combinatorial optimization. *ACM Transactions on Knowledge Discovery from Data*, *17*(9), 1-50.

[62] Mallick, M. A. I., & Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News*, *190*(1), 1-69.

[63] Mikkelsen, A., & Seljåsen, T. (2024). *Mindful balancing: Avoiding Alert Fatigue in Security Operation Centers* (Master's thesis, University of Agder).

[64] Mudele, O., Frery, A. C., Zanandrez, L. F. R., Eiras, A. E., & Gamba, P. (2021a). Dengue vector population forecasting using multisource earth observation products and recurrent neural networks. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 14, 4390-4404.

[65] Mudele, O., Frery, A. C., Zanandrez, L. F. R., Eiras, A. E., & Gamba, P. (2021b). Modeling dengue vector population with earth observation data and a generalized linear model. Acta Tropica, 215, 105809.

[66] Munoz, R. (2023). A Study on Diffusion Probabilistic Models for Image Generation.

[67] Nassar, A., & Kamal, M. (2021). Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies. *Journal of Artificial Intelligence and Machine Learning in Management*, *5*(1), 51-63.

[68] Obaid, A. J., Bhushan, B., & Rajest, S. S. (Eds.). (2023). Advanced applications of generative AI and natural language processing models. IGI Global.

[69] Obi, O. C., Akagha, O. V., Dawodu, S. O., Anyanwu, A. C., Onwusinkwue, S., & Ahmad, I. A. I. (2024). Comprehensive review on cybersecurity: modern threats and advanced defense strategies. *Computer Science & IT Research Journal*, *5*(2), 293-310.

[70] Oyinloye, T. S., Arowolo, M. O., & Prasad, R. (2024). Enhancing Cyber Threat Detection with an Improved Artificial Neural Network Model. *Data Science and Management*.

[71] Padhy, R. P., Patra, M. R., & Satapathy, S. C. (2011). Cloud computing: security issues and research challenges. *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, *1*(2), 136-146.

[72] Pandey, K., Mukherjee, A., Rai, P., & Kumar, A. (2022). Diffusevae: Efficient, controllable and high-fidelity generation from low-dimensional latents. *arXiv preprint arXiv:2201.00308*.

[73] Pandey, K., Mukherjee, A., Rai, P., & Kumar, A. (2022). Diffusevae: Efficient, controllable and high-fidelity generation from low-dimensional latents. *arXiv preprint arXiv:2201.00308*.

[74] Patil, S., Patil, S., Sitapure, S., Patil, M., & Shelke, M. V. (2024). Text-Guided Artistic Image Synthesis Using Diffusion Model. *International Research Journal on Advanced Science Hub*, *6*(06), 157-166.

[75] Petersen, E., Potdevin, Y., Mohammadi, E., Zidowitz, S., Breyer, S., Nowotka, D., ... & Herzog, C. (2022). Responsible and regulatory conform machine learning for medicine: a survey of challenges and solutions. *IEEE Access*, *10*, 58375-58418.

[76] Pezoulas, V. C., Zaridis, D. I., Mylona, E., Androutsos, C., Apostolidis, K., Tachos, N. S., & Fotiadis, D. I. (2024). Synthetic data generation methods in healthcare: A review on open-source tools and methods. *Computational and Structural Biotechnology Journal*.

[77] Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature machine intelligence*, *1*(5), 206-215.

[78] Ryan, M. (2021). *Ransomware Revolution: the rise of a prodigious cyber threat* (Vol. 85). Berlin/Heidelberg, Germany: Springer.

[79] Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, *15*(18), 13369.

[80] Sai, S., Yashvardhan, U., Chamola, V., & Sikdar, B. (2024). Generative ai for cyber security: Analyzing the potential of chatgpt, dall-e and other models for enhancing the security space. *IEEE Access*.

[81] Salehi, P., Chalechale, A., & Taghizadeh, M. (2020). Generative adversarial networks (GANs): An overview of theoretical model, evaluation metrics, and recent developments. *arXiv preprint arXiv:2005.13178*.

[82] Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access*, *10*, 65703-65727.

[83] Sarker, I. H. (2024). Introduction to AI-Driven Cybersecurity and Threat Intelligence. In *AI-Driven Cybersecurity and Threat Intelligence: Cyber Automation, Intelligent Decision-Making and Explainability* (pp. 3-19). Cham: Springer Nature Switzerland.

[84] Sfetcu, N. (2024). Advanced Persistent Threats in Cybersecurity–Cyber Warfare. MultiMedia Publishing.

[85] Sfetcu, N. (2024). Advanced Persistent Threats in Cybersecurity–Cyber Warfare. MultiMedia Publishing.

[86] Sharma, P., Kumar, M., Sharma, H. K., & Biju, S. M. (2024). Generative adversarial networks (GANs): Introduction, Taxonomy, Variants, Limitations, and Applications. *Multimedia Tools and Applications*, 1-48.

[87] Shibeika, A., & Harty, C. (2015). Diffusion of digital innovation in construction: a case study of a UK engineering firm. *Construction management and economics*, *33*(5-6), 453-466.

[88] Shyaa, M. A., Ibrahim, N. F., Zainol, Z., Abdullah, R., Anbar, M., & Alzubaidi, L. (2024). Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems. *Engineering Applications of Artificial Intelligence*, *137*, 109143.

[89] Sindiramutty, S. R., Tan, C. E., Lau, S. P., Thangaveloo, R., Gharib, A. H., Manchuri, A. R., ... & Muniandy, L. (2024). Explainable AI for Cybersecurity. In *Advances in Explainable AI Applications for Smart Cities* (pp. 31-97). IGI Global.

[90] Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry*, *13*(4), 597.

[91] Tang, B., Lu, Y., Li, Q., Bai, Y., Yu, J., & Yu, X. (2023). A diffusion model based on network intrusion detection method for industrial cyber-physical systems. *Sensors*, *23*(3), 1141.

[92] Tatineni, S. (2019). Ethical Considerations in AI and Data Science: Bias, Fairness, and Accountability. *International Journal of Information Technology and Management Information Systems (IJITMIS)*, *10*(1), 11-21.

[93] Tidjon, L. N. (2020). *Formal modeling of intrusion detection systems* (Doctoral dissertation, Institut Polytechnique de Paris; Université de Sherbrooke (Québec, Canada)).

[94] Truong, V. T., Dang, L. B., & Le, L. B. (2024). Attacks and Defenses for Generative Diffusion Models: A Comprehensive Survey. *arXiv preprint arXiv:2408.03400*.

[95] Ullah, F., Turab, A., Ullah, S., Cacciagrano, D., & Zhao, Y. (2024). Enhanced Network Intrusion Detection System for Internet of Things Security Using Multimodal Big Data Representation with Transfer Learning and Game Theory. *Sensors*, *24*(13), 4152.

[96] Veres, M., & Moussa, M. (2019). Deep learning for intelligent transportation systems: A survey of emerging trends. *IEEE Transactions on Intelligent transportation systems*, *21*(8), 3152-3168.

[97] Villadiego, R. (2020). Decision Making in Cybersecurity. Lumu Technologies, Available online at https://lumu. io/wpcontent/uploads/2020/10/en_wp_decision-making-in-cybersecurity. pdf.

[98] Waheed, A., Seegolam, B., Jowaheer, M. F., Sze, C. L. X., Hua, E. T. F., & Sindiramutty, S. R. (2024). Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure.

[99] Wall, A. M. (2021). Guidelines for artificial intelligence-driven enterprise compliance management systems (Doctoral dissertation).

[100] Wang, X. (2020). Modeling and Analysis of Advanced Persistent Threats in Cyber Space (Doctoral dissertation).

[101] Wang, Y., Liu, H., Li, Z., Su, Z., & Li, J. (2024). Combating Advanced Persistent Threats: Challenges and Solutions. *IEEE Network*.

[102] Wang, Z., Xie, W., Wang, B., Tao, J., & Wang, E. (2021). A survey on recent advanced research of CPS security. *Applied Sciences*, *11*(9), 3751.

[103] Yang, L., Zhang, Z., Song, Y., Hong, S., Xu, R., Zhao, Y., ... & Yang, M. H. (2023). Diffusion models: A comprehensive survey of methods and applications. *ACM Computing Surveys*, *56*(4), 1-39.

[104] Zhang, C., Zhang, C., Zheng, S., Zhang, M., Qamar, M., Bae, S. H., & Kweon, I. S. (2023). A survey on audio diffusion models: Text to speech synthesis and enhancement in generative ai. *arXiv preprint arXiv:2303.13336*.

[105] Zhang, W., Valencia, A., & Chang, N. B. (2021). Synergistic integration between machine learning and agent-based modeling: A multidisciplinary review. *IEEE Transactions on Neural Networks and Learning Systems*, *34*(5), 2170-2190.

[106] Zhao, Y., Liu, Z., & Wu, J. (2020). Grassland ecosystem services: a systematic review of research advances and future directions. *Landscape Ecology*, *35*, 793-814.

[107] Zhou, E., & Lee, D. (2024). Generative artificial intelligence, human creativity, and art. *PNAS nexus*, *3*(3), pgae052.