GAN-Based Anomaly Detection for Cybersecurity: A Technology Management Framework for Legal Risk, Regulatory Compliance, and Digital Governance

[1]Dr K P N V Satyasree
Professor & Head
Department of CSE
Usha Rama College of engineering and technology,
Telaprolu, Krishna Dt, A.P
India - 521109
satyasreekpnv@gmail.com
cse.satyasree@usharama.in
[2]Bhuvan Unhelkar
Professor
Muma College of Business
University of South Florida
8350 N. Tamiami Trail Sarasota, Florida. USA.
bunhelkar@usf.edu
[3]Dr.Siva Shankar S
Professor & Hear IPR
Department of Computer Science and Engineering
KG Reddy College of Engineering and Technology
RR district
Telangana,INDIA - 501504
drsivashankars@gmail.com

Abstract
The growing complexity of cyber threats has highlighted the shortcomings of traditional signature-based IDS (intrusion detection systems) and led to the need for intelligent, adaptive, and governance-centric cybersecurity solutions. Recent developments in the field of deep learning have produced a novel technique called Generative Adversarial Networks (GANs), which has shown promise in anomaly detection by its ability to learn complex data distributions and detect previously unseen attack patterns. Research on GAN-based cybersecurity to date, however, has been mostly oriented towards enhancing the detection performance, while limited research has been conducted on organizational decision-making, legal risk management, regulatory compliance, and digital governance. This paper presents a holistic GAN Based Anomaly Detection Framework for Cybersecurity, which combines intelligent anomaly detection with technology management, legal risk assessment, regulation compliance and digital governance. The proposed framework consists of four layers that are interconnected: data acquisition and data preprocessing; anomaly detection using the GAN; technology management; and integration of legal risk and compliance. The framework integrates the Advanced Threat Protection (ATP) capabilities of

artificial intelligence with the widely adopted cybersecurity standards such as the NIST Cybersecurity Framework (CSF 2.0), ISO/IEC 27001:2022, and the General Data Protection Regulation (GDPR), which can be used for the detection of unusual network activity as well as to prioritize organizational risks, monitor compliance, report to management, and inform strategic decision making. The proposed approach is different from the traditional intrusion detection architecture, in which anomaly detection is seen as a technical task and not as a part of enterprise cybersecurity management. The study offers a cross-disciplinary conceptual framework that combines Artificial Intelligence, Cybersecurity, Technology Management, Legal and Compliance considerations, and Digital Governance to offer a basis for future implementation and empirical validation in enterprise security settings.

Keywords-*Generative Adversarial Networks (GANs), Legal Risk Assessment, Regulatory Compliance, Digital Governance, Artificial Intelligence.*

1. Introduction

Organizations are undergoing a massive digital transformation, making the modern information system larger, more complex and more interconnected. Digital technologies have enabled innovation and operational efficiency, but also added additional layers of risk to critical infrastructures against sophisticated cyber threats. Whether in finance, healthcare, government, manufacturing or Cloud Computing, organizations are increasingly becoming dependent on interrelated digital platforms, whereby cybersecurity has become a strategic priority and not just a technical issue. The traditional security methods are losing their effectiveness against the changing nature of the attacks, as new attacks can adapt, find new vulnerabilities, and evade signature-based detection methods. Therefore, intelligent and adaptive cybersecurity solutions are crucial to safeguarding the assets of any organization and continuity of business operations [2, 3].

Anomaly detection has become one of the most promising ways of detecting previously unknown or zero-day attacks that are undetectable by traditional rule-based and signature-based intrusion detection systems. Anomaly detection models learn what is considered normal network activity and detect any abnormal activity that may be a sign of malicious behaviour, unlike traditional models. In recent years, the field of artificial intelligence (AI) has made significant progress, especially in the areas of machine learning and deep learning, which have greatly enhanced cybersecurity systems' capacity to identify intricate patterns of attacks within vast network environments. These smart methods allow automated feature extraction, ongoing learning and greater accuracy in detection than traditional statistical methods [10, 11, 12].

Recently, Generative Adversarial Networks (GANs), which are known for their special ability to learn complex data distributions with adversarial training, have sparked a lot of interest. GANs were introduced by Goodfellow et al. [1] as two concurrent neural networks: a generator and a discriminator, which continually augment each other in their learning process. While GANs are primarily known for their ability to generate realistic data, their potential applications in anomaly detection, synthetic data generation, data augmentation, and cybersecurity have been shown in subsequent studies. GANs can be trained with the distribution of normal traffic, and they will be able to detect unusual observations that do not resemble any known behavior, which makes them

well suited to recognize advanced cyber attacks and solve the class imbalance issue often seen in intrusion detection problems [2]–[4].

Another key benefit of GANs for anomaly detection is that it generally enhances the learning of the system when labelled attack data is scarce. In real cyber security scenarios, much more effort is needed to acquire a full set of datasets, including all attack variants, as they continually evolve. To overcome this drawback, GANs are able to create realistic synthetic samples, complementing the training sets, and thus enhance the generalization of the models. Benchmark datasets like UNSW-NB15 and CICIDS2017 are openly available and are used to evaluate IDSs based on deep learning and offer a standardized environment for comparing model performance [5, 6]. These datasets enable the creation of intelligent security frameworks that can be used to detect known and unknown cyber threats.

In spite of this technological progress, cybersecurity is no longer seen as just a technical problem. As AI-powered security systems become more prevalent, they must be deployed within a legal, regulatory, and governance framework. Organizations must perform and implement effective risk management, information security controls, ensure the protection of their personal data, as well as demonstrate compliance with international standards and regulations, such as the NIST Cybersecurity Framework (CSF) 2.0, ISO/IEC 27001:2022, and the General Data Protection Regulation (GDPR) [7]–[9]. Therefore, cybersecurity solutions must be able to deliver high accuracy of detection and enable the accountability, transparency, compliance auditing, and responsible governance of organizations.

As a technology manager, the implementation of AI-powered cybersecurity tools demands a blend of technological advancements and organizational goals, legal compliance, mitigation of operational risks, and governance frameworks. Decision makers need to consider whether intelligent detection systems can be a key asset in enhancing the resilience of an organization without compromising compliance with relevant cyber security requirements and regulatory regimes. Therefore, when combined with legal risk assessment and digital governance, anomaly detection can shift the paradigm from threat detection to proactive cyber risk management, which can aid in strategic decision making and long-term digital sustainability [2], [3], [7].

While the GAN-based architectures for intrusion detection and network anomaly detection have been widely explored in existing literature, previous works mainly target at enhancing the detection performance by algorithmic improvements. Not much focus has been placed on embedding the technology intelligence detection with technology management, legal risk assessment, regulatory compliance and digital governance. This separation impedes the use of AI-based cybersecurity solutions in organizations where operational, managerial and regulatory demands are all equally important [2], [3], [10], [11].

To solve this research gap and fill the aforementioned gap, this paper suggests a GAN-Based Anomaly Detection Framework for Cybersecurity, which combines intelligent anomaly detection with a technology management approach that incorporates legal risk assessment, regulatory compliance and digital governance. The proposed framework integrates the GAN's detection prowess with the organizational decision-support tools to enable safe, compliant, and responsible

cybersecurity management. The proposed method is designed to combine technical innovation with governance and regulatory aspects to ensure effective detection of cyber threats and responsible use of AI-based security solutions. The result of this study is believed to make a meaningful contribution to the body of knowledge on AI based cybersecurity and will enable practical application by researchers, technology managers, cybersecurity professionals and organizational policy makers

2. Related Work

As the network infrastructures are becoming more complex and the attacks are becoming more sophisticated, a lot of effort has been invested in studying new developments on machine learning and deep learning for intrusion detection systems. The growing complexity of network infrastructures and the sophistication of the attacks have motivated the study of new developments in machine learning and deep learning for the problem of intrusion detection systems. Traditional intrusion detection methods typically rely on a database of pre-compiled signatures, manually written rules or statistical thresholds. This can still be helpful for recognising attacks that have been previously seen, but these methods are less effective when attacks evolve or new attacks are encountered. Anomaly detection, based on machine learning, has thus become a key research area that can help security systems learn the network traffic behaviour and recognize activities that deviate from network traffic behaviour that is considered to be normal.

Anis et al. [13] summarized and classified the existing deep learning methods for network intrusion detection systems. Their research uncovers a growing trend towards reconstruction-based, discriminative, hybrid and generative approaches for detection of malicious network behaviour. An advantage of deep neural networks is that they can be trained to capture the complex relationship between traffic records in high-dimensional space without the need to pre-select features. Convolutional neural networks, recurrent neural networks, autoencoders, and generative models have therefore been used for various intrusion detection problems. But the review also uncovers common problems, such as class imbalance, lack of interpretability, high computational demands, data dependency, and poor generalizability across networks. The restrictions suggest that more accurate detection by itself is not enough to ensure a deep learning-based intrusion detection system can be relied upon in real organizational environments.

Network security situational awareness is also closely related to network anomaly detection. Regarding the perspective of situational awareness, Zhen et al. [14] studied machine learning based anomaly detection, and discussed the limitations, methods and future directions of the field. Their analysis shows that anomaly detection can do more than just classify a network record as normal or abnormal. It is part of a larger effort to gather security data, detect anomalies, assess threat levels, and aid in quick decision making. Different statistical methods, traditional machine learning algorithms, ensemble methods and deep learning methods have their own benefits. However, these techniques are affected by false positives, availability of adequate training data, feature representation, rapidly changing traffic flow characteristics and data quality [14]. These results validate the need for an anomaly detection framework to make the link between model output and risk assessment and organizational security decision making.

In the field of deep learning research, Generative Adversarial Networks have been given special attention due to their ability to learn a complex data distribution and synthesize realistic observations. Dunmore et al. [15] gave a thorough overview on GANs applications in the field of cybersecurity intrusion detection. As per the study, GANs have been utilized in creating synthetic attack instances, augmenting minority class, generating adversarial instances, learning features, and also in anomaly detection. Normal traffic patterns typically outnumber some classes of attacks in intrusion detection datasets. This imbalance can lead classifiers to overlook rare but security-critical attacks and delivering a majority class bias. This issue can be partly overcome by having more samples of underrepresented classes during model training, as in the case of GAN-generated samples [15].

GAN-based anomaly detection can also work on the principle of learning the normal traffic and determining if there are new observations that are not consistent with the learned normal distribution. A generator tries to produce data that is like a real network's and a discriminator tries to learn how to tell the difference between generated data and real data. This adversarial process is used to build the model, which represents the traffic distribution. Any record that varies significantly from this representation could then be considered as an anomaly. The GAN literature reviewed by Dunmore et al. [15] also notes a number of significant challenges such as training instabilities, mode collapse, inconsistent evaluation, hyperparameter sensitivity, and a potential disconnect between generated and operational network conditions. Accordingly, the ability of the intrusion detection algorithm to detect intrusions can't be validated based on synthetic-data quality or classification accuracy only.

More broadly, the security of AI systems needs to be considered when implementing AI-driven cybersecurity solutions using GANs. Narula et al. [18] performed a systematic mapping study of the research topics, tools, metrics and frameworks on AI security. Their efforts have shown that AI security is about more than just employing artificial intelligence in a protective capacity; it's also about securing AI systems from attacks, misuse, and technical failures. Issues such as adversarial examples, data poisoning, model extraction, privacy leakage, insecure implementation, and insufficient testing are relevant concerns. These concerns are directly relevant to the GAN-based anomaly detection since the anomaly detection model can be a target of manipulation. An attacker can try to manipulate the traffic characteristics, pollute the training data, or exploit the weaknesses of the model's decision boundary. The resilience, transparency, reliability and operational security are, therefore, critical factors to consider when assessing an AI-powered intrusive detection system, in addition to its predictive performance [18].

Ennaji et al. [19] studied network intrusion detection systems in greater detail in terms of their adversarial vulnerabilities. The research shows how evasion and poisoning attacks can impact their study-based detection models. During an evasion scenario, the attacker changes the properties of the malicious input to make it more likely to evade. When a poisoning attack occurs, the attacker disrupts the learning process, causing the resulting model to learn incorrect patterns. These threats pose a great challenge for GAN-based cybersecurity, given that generative models can be applied in reverse for data augmentation and robustness testing, but their generative capabilities can be

used to create traffic samples that avoid detection. The two aspects of the dual-use applications of GANs thus call for proper control of the training data, access to GANs models, testing methods, monitoring, and updates of the systems [19].

Next, the use of multiple cybersecurity data views, another important development. In a comparison between single-view and multi-view deep learning techniques in cybersecurity anomaly detection, Li et al. [20] compared the two methods. Single-view models typically use one source of information or view to learn, while multi-view models use a set of complementary views, drawn from network and host information. Their results show that multiple perspectives can enhance the capability of IDSs to depict complex security events. A single traffic representation may be insufficient to identify all the attack behaviours, especially if attacks involve multiple devices, services or layers of an information system. While Multi-view learning can induce a more comprehensive picture of network conditions, it does add new challenges on data integration, computational cost, view consistency and model complexity [20].

All the reviewed studies reflect significant advancement in deep learning for IDS, situational anomaly analysis, GAN for data generation, AI security and adversarial robustness, and multi-view detection. But the current literature mainly focuses on technical goals like classification accuracy, data augmentation, representation of features, and adversarial robustness. Few efforts have been made to synthesize the outputs of anomaly detection, particularly with GANs, into technology management, legal-risk assessment, regulatory compliance and digital governance processes. Existing models may be able to detect suspicious activities, but they are unable to explain how the anomalies detected should be prioritized, documented, escalated, audited and related to organizational accountability.

This gap leads to the need for an integrated framework where GAN-based anomaly detection is one of several elements of the cybersecurity management system. It should leverage the adaptive and data-generative capabilities highlighted in [13] and [15], promote situational awareness as discussed in [14] and manifest AI security threats and adversarial attacks outlined in [18] and [19] and integrate a variety of security information as studied in [20] from a multi-view perspective. The present study thus builds on previous technical research and incorporates legal-risk assessment, regulatory compliance, technology management, and digital governance.

3. Proposed Framework

This study presents an integrated GAN-Based Anomaly Detection Framework comprising intelligent cyberattack detection, technology management principles, legal risk assessment, regulatory compliance and digital governance. The proposed framework goes beyond the traditional approach of intrusion detection systems, which are mostly dedicated to attack classification, and makes anomaly detection a decision support system that can help organizations detect cyber threats and assess the compliance requirements and governance needs. The framework aims to enhance the resilience of the organization's cybersecurity posture through the combination of technical intelligence and management and compliance-based decision making.

The proposed framework is divided in four layers: (i) Data Acquisition and Pre-processing, (ii) GAN-Based Anomaly Detection, (iii) Technology Management Layer, and (iv) Legal Risk and

Compliance Layer. Each layer has a specific role to play and the layer below it provides information to the next layer, establishing a continuous cybersecurity management process. The overall architecture of the proposed framework is shown in figure 1

A. Overall Framework

The first step of the framework is to collect network traffic from organizational information systems. The framework can be extended to enterprise network environment but it can also be used with publicly available benchmark intrusion detection datasets, including UNSW-NB15 and CICIDS2017. The raw traffic records are then cleaned up by running them through data cleaning processes to eliminate incomplete records, duplicate observations, and inconsistent data. Categorical network features are encoded to numerical representation and numerical features are normalized to lower scale variations. These processed results are then split into a training, validation, and testing subset of data to aid in the development of the model.

The cleaned dataset is then passed to the anomaly detection module using the GAN. The proposed model is based on adversarial learning, where it learns the statistical distribution of legitimate network traffic, instead of merely relying on predefined attack signatures. This allows the framework to be more sensitive to unusual behaviour that deviates from normal operational characteristics, and to be able to detect attacks which it has not seen before.

The anomaly detection results are then sent to the Technology Management Layer where technical outputs are converted into organizational risk indicators. The framework does not just provide an anomaly score, it also considers the operational significance of detected events, based on asset criticality, attack severity, and organizational priorities. Lastly, the Legal Risk and Compliance Layer identified incidents and correlated them with the relevant cybersecurity standards, regulatory requirements, and governance.

In this layered architecture, anomaly detection is no longer just a technical task but a crucial part of cybersecurity management.

B. GAN-Based Detection Model

A Generative Adversarial Network (GAN) forms the backbone of the proposed framework, as the core intelligence. The GAN is composed of the following two neural networks: Generator (G) and Discriminator (D).

The Generator is fed randomly sampled latent vectors and generates synthetic network traffic samples similar to real network traffic. The goal of the Generator is to continually fine-tune the quality of the generated traffic in order to make it harder for the Discriminator to tell the difference between synthetic samples and real observations.

The Discriminator, on the other hand, is presented with both real network records and samples generated and tries to classify them correctly. In training, both networks play an adversarial manner. As training continues, the Generator is able to produce more realistic data distributions and the Discriminator becomes more and more capable of detecting discrepancies between the real and synthetic traffic.

After convergence the trained model is able to detect the normal network behaviour. Traffic arriving at the distribution is compared to the learned distribution, and any observations that show significant deviations are flagged as possible anomalies to be investigated further.

The proposed GAN-based detection process is as follows:

1. Collection of network traffic data.
2. Installing applicable packages.
3. Creating a data frame.
4. Training of the Generator and Discriminator.
5. Knowing where to find legitimate traffic.
6. Calculating Anomaly Score of new network traffic.
7. Classification of suspicious activities.
8. Passing identified anomalies to the management layer.

The proposed GAN framework is more adaptive to the changing attack behaviour when compared with the traditional signature-based intrusion detection systems (IDS), and less dependent on manually created attack signatures. In addition, it is able to create synthetic traffic to enhance learning when the dataset is imbalanced, meaning that there are relatively few training examples for some attack categories.

C. Technology Management Layer

Most intrusion detection work ends with the identification of malicious traffic, but this proposed system adds a special Technology Management Layer which transforms technical detection into organizational intelligence.

This layer's primary goal is to support cybersecurity managers when prioritizing threats they have identified, based on organizational impact and not just on the anomaly score. Several management indicators are considered such as asset criticality, operational dependency, business continuity needs, likelihood of exploitation, financial impact potential, and organization tolerance for risk.

Detected anomalies are classified as to the organizational level of risk which allows the security teams to distinguish between monitored events and events that are of an immediate high priority. This prioritisation is helpful for effective resource allocation and for strategic decision making in cybersecurity.

The Technology Management Layer also stores data on anomalies in past attacks to detect patterns and track overall cybersecurity trends over time. This data can help organizations assess the impact of current security measures, allocate resources efficiently, and enhance their cybersecurity strategies for the future.

The proposed framework, however, is not a technical detection system but rather serves to assist in organizational governance by linking the output of the anomaly detection process to management related cybersecurity choices.

D. Legal Risk and Compliance Integration

Cybersecurity operations in the modern era should meet both technical and legal and regulatory needs. As a result, the last step of the proposed framework combines anomaly detection with legal risk assessment and regulatory compliance.

These detected anomalies are assessed based on pre-defined compliance rules based on internationally accepted cybersecurity frameworks including the NIST Cybersecurity Framework (CSF 2.0), ISO/IEC 27001:2022 and the General Data Protection Regulation (GDPR). This mapping can help organizations identify if a detected event impacts the information confidentiality, integrity, availability, personal data protection, or organizational governance requirements.

The framework automatically creates incident reports from the compliance evaluation which include the classification of the anomaly, estimated impact on the organization, applicable regulatory control, recommended mitigation action, and legal considerations as a result. These reports are useful for cybersecurity teams in incident response and for organizational management to help them prove compliance in security audit situations.

The Legal Risk and Compliance Layer also ensures accountability by providing a log of incidents detected, management decisions, corrective actions and compliance assessments. This helps in evidence-based decision making when the organization goes under regulatory review and helps in strengthening organizational governance.

The proposed framework has two main components, technical anomaly detection and compliance evaluation, combining the two to create a bridge between artificial intelligence – driven cybersecurity and organizational governance. The resulting architecture allows for intelligent threat detection, whilst ensuring legal accountability, regulation compliance, strategic technology management and responsible digital governance.

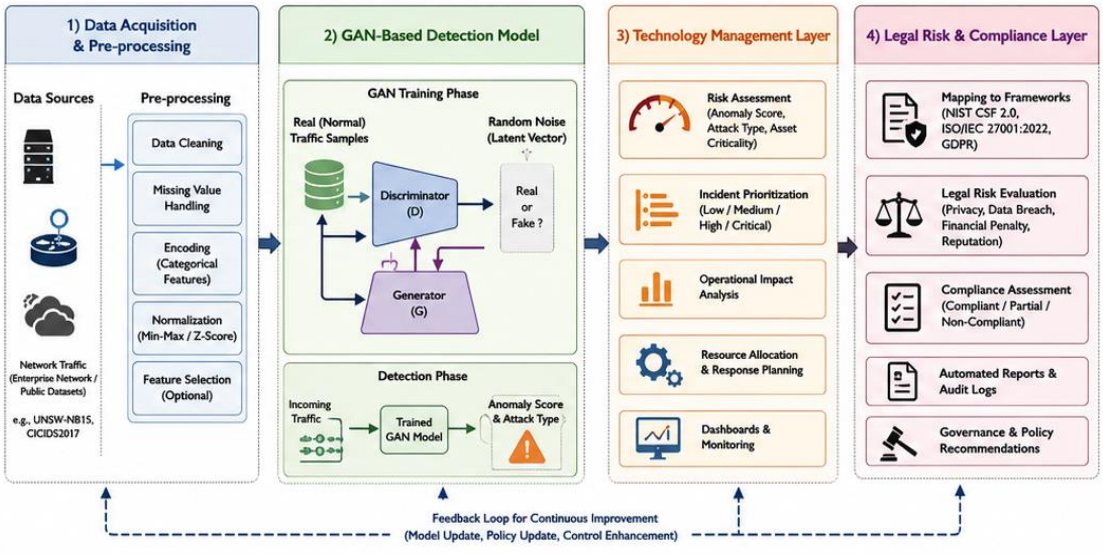

Figure 1: Overall Proposed Framework for GAN-Based Cybersecurity Anomaly Detection Integrated with Technology Management, Legal Risk, Regulatory Compliance, and Digital Governance.

Figure 1. Overall Proposed Framework for GAN-Based Cybersecurity Anomaly Detection Integrating Technology Management, Legal Risk, Regulatory Compliance, and Digital Governance.

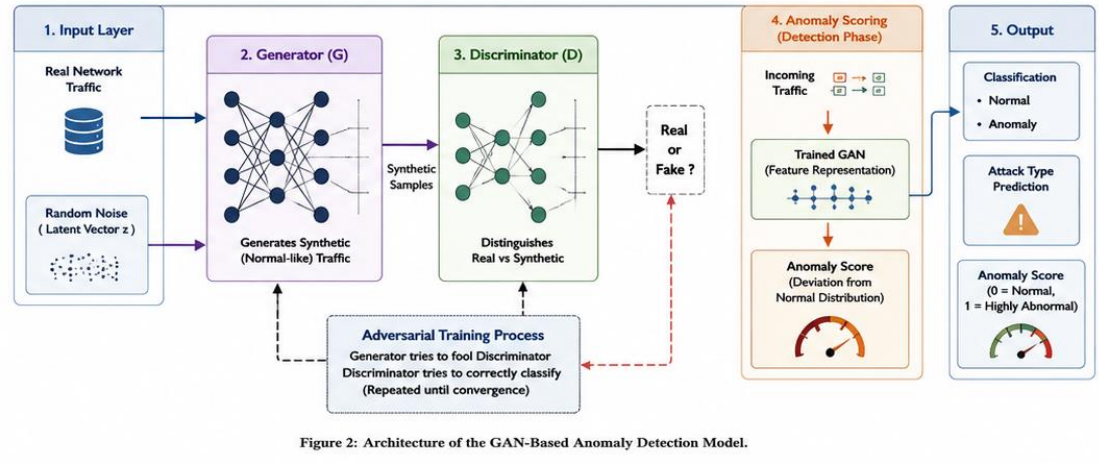

Figure 2. GAN-Based Detection Architecture Showing Data Pre-processing, Generator, Discriminator, Anomaly Scoring, Risk Assessment, and Compliance Decision Flow.

4. Result and Discussion

The proposed framework highlights the integration of technology management, legal risk evaluation, regulatory compliance, and digital governance with Generative Adversarial Network (GAN) -based anomaly detection, creating a holistic approach to cyber security management. The approach taken in this paper is a departure from the traditional intrusion detection research which focuses on classification accuracy, and rather puts forward a new framework of anomaly detection as a strategic decision support system that can be used to help organizations make technical, managerial, and regulatory decisions. In this section, the proposed framework is analyzed in terms of its architecture, management, and governance aspects and its potential benefits to current cybersecurity practice

A. Framework Analysis

The proposed architecture is composed of four layers of functionality that are interconnected and provide for the intelligent management of cybersecurity. The first layer handles data acquisition and pre-processing, cleaning and normalising the raw network traffic, encoding and structuring it into a format that is appropriate for deep learning analysis. The preprocessing in this stage boosts the consistency of the data and prepares the network traffic to be used for GAN-based learning.

The second layer is based on the GAN model for anomaly detection. The adversarial learning mechanism allows the generator and discriminator to learn the complex characteristics of the legitimate network traffic, which in turn enables the framework to detect abnormal behavioural patterns that are different from what is considered a normal operating mode. The proposed framework is expected to outperform the conventional signature-based detection systems in terms of adaptability to new behaviors because detection decisions are made based on the distribution of behaviours that have been learned, rather than on manually written attack signatures.

The third layer adds technology management features that are not found in typical intrusion detection systems. The framework does not provide anomaly scores themselves, but rather transforms technical observations into management-oriented indicators that can assist the organization's decision making process. This layer incorporates risk prioritization, incident

classification, operational impact assessment, and cybersecurity resource allocation. Security managers thus get actionable information rather than just a bunch of technical alerts.

This last layer links identified threats to law and regulations. Security incidents are assessed based on internationally recognised cyber security standards and governance frameworks, allowing organisations to link identified threats to compliance, and risk management frameworks. The integration improves accountability and aids in making informed decisions throughout the cybersecurity lifecycle.

In general, the above-mentioned architecture shows that the anomaly detection should not be a standalone operation, but should be integrated into the overall cyber security governance ecosystem.

B. Technology Management Perspective

One of the more significant contributions of the proposed framework is related to technology management. The current work on GANs and IDS focuses mainly on optimizing the detection performance of the algorithm. While these studies have great technical value, relatively little focus has been placed on organisational decision making following AOD.

In the proposed framework anomaly detection results are no longer just classification results but also organize intelligence. Every anomaly is assessed on the basis of its impact on the organization's operations and systems, allowing the cybersecurity manager to prioritize incidents based on organ impact, not just on the model's confidence.

The proposed technology management layer enables a variety of managerial activities, such as incident prioritization, investment planning in cybersecurity, operational risk assessment, optimizing security resources, and supporting strategic decision making. Combining technical detection and organisational management processes, the framework helps decision-makers distribute scarce cybersecurity resources to the highest priority threat.

The other benefit of the proposed framework would be its ability to keep track of past anomalies detected. By analyzing historical data, organizations can gain insights into common attack patterns, assess long-term security performance, and plan for future security measures more effectively. This information is also used for continuous improvement and organisation's Cyber Security Maturity evaluations.

This new approach to cybersecurity moves beyond strictly technical security and creates better linkages between artificial intelligence, corporate governance, and technology management strategies.

C. Legal Risk and Regulatory Compliance

In today's organizations there are increasingly complex legal and regulatory environments that can have significant legal, financial and reputational ramifications from cybersecurity incidents. Thus, any effective anomaly detection system should enable it to not just detect technical incidents, but also to provide legal accountability and comply with regulations.

The proposed framework includes an exclusive legal risk assessment process for assessing detected anomalies based on the applicable cyber security regulatory requirements and

organizational security policies. Every detected incident is analyzed to assess its impact on information confidentiality, integrity, availability, protection of privacy and compliance with rules. It aims to enable compliance with globally recognised cybersecurity frameworks such as the NIST Cybersecurity Framework (CSF 2.0), ISO/IEC 27001:2022 and the General Data Protection Regulation (GDPR). Connecting outputs of anomaly detection to these frameworks helps organizations document cybersecurity incidents, help with compliance reporting, and enhance audit readiness.

In terms of governance, the framework ensures accountability by keeping structured records of the incident(s) detected, risks associated with the incident(s), management responses to risks, corrective actions, and compliance status. The records are helpful in internal security reviews and external compliance reviews.

Therefore, this approach combines both technical detection and organizational governance and legal risk management, thus facilitating the responsible use of AI in cybersecurity operations.

D. Comparative Analysis

The proposed framework is compared with some of the most representative cybersecurity methods reported in the literature that are based on the GAN. Previously, the effectiveness of GANs in anomaly detection, synthetic data generation and intrusion detection has been successfully demonstrated. Most of the existing methods are however still technically based and are not very likely to embed organizational management, legal compliance or digital governance into their design.

Table 1. Comparative Analysis of Existing GAN-Based Approaches and the Proposed Framework

Feature	Existing GAN-Based Models	Proposed Framework
GAN-based anomaly detection	✓	✓
Synthetic data generation	✓	✓
Detection of unknown attacks	✓	✓
Technology management integration	✗	✓
Organizational decision support	Limited	✓
Legal risk assessment	✗	✓
Regulatory compliance mapping	Limited	✓
Digital governance integration	✗	✓
Audit support	Limited	✓
Comprehensive cybersecurity management	✗	✓

The comparison highlights that the proposed framework does not introduce a new GAN architecture, but rather combines intelligence into anomaly detection with organizational governance. This multi-disciplinary view will broaden the use of GAN-based cybersecurity to enterprise-wide cybersecurity management

E. Digital Governance Implications

Digital governance is an integral part of today's cybersecurity landscape as organisations need to ensure that their intelligent systems are transparent, accountable and operate in line with their goals. The proposed framework helps to improve digital governance by defining clear connections between anomaly detection, organizational decisions making, legal compliance and management accountability.

The framework introduces governance processes that enable documentation, reporting, monitoring and continual improvement rather than viewing cybersecurity incidents as individual technical incidents. Structured information is provided to security managers which is used in policy implementation, compliance checks and risk based decision making.

Moreover, the incorporation of governance aspects fosters the responsible use of AI, ensuring transparency in cybersecurity efforts. Organizations can thus better show compliance with regulations and at the same time increase their operational resilience and stakeholder confidence.

F. Discussion

The proposed framework does not only fill in some of the important research gaps highlighted in the literature, but it also considers a number of other insights and experiences gathered from the review. First, it takes the concept of anomaly detection beyond traditional intrusion detection and applies principles of technology management to the cyber security decision-making process. Second, it embeds the legal risk assessment and regulatory compliance process into the anomaly detection process itself, not as a separate organizational process. Thirdly, it introduces Digital Governance as a fundamental part of the Cyber security management with the use of AI.

The framework brings together a multidisciplinary architecture that merges artificial intelligence, cybersecurity, technology management, legal compliance, and governance in a single model, offering a unique perspective from an academic standpoint. This integration opens the door to future exploration of Explainable AI, automated compliance checks, cybersecurity maturity analysis, and AI-driven governance models.

On an industry level, the proposed framework has been seen as having value as it provides practical guidance for organisations as they look to improve their cybersecurity posture and meet regulatory expectations. The architecture offers a framework to structure the integration of the intelligent anomaly detection in existing security operation, governance policies and organizational risk management practices.

While the framework provides a comprehensive conceptual architecture, some limitations need to be noted. The present study will be based around the design and embedding of the framework, with no empirical testing of the framework through implementation. The proposed architecture can be subjected to testing with benchmark intrusion detection datasets, different GAN variants,

computational efficiency analysis and evaluation of explainable AI approaches to enhance transparency and managerial trust in the future.

The proposed framework proves that effective cybersecurity goes beyond just being able to detect anomalies. The seamless integration of AI, organizational strategy, legal compliance, and digital governance are essential for sustainable cybersecurity management. The integrated architecture of these complementary dimensions provides a solid basis for intelligent, accountable and governance-oriented cybersecurity management that can tackle the challenges of today's digital ecosystems.

Figure 3: Technology Management Decision-Making Workflow Following GAN-Based Anomaly Detection

Figure 3. Technology Management Decision-Making Workflow Following GAN-Based Anomaly Detection.

Figure 4: Legal Risk Assessment and Regulatory Compliance Mapping within the Proposed Cybersecurity Framework

Figure 4. Legal Risk Assessment and Regulatory Compliance Mapping within the Proposed Cybersecurity Framework.

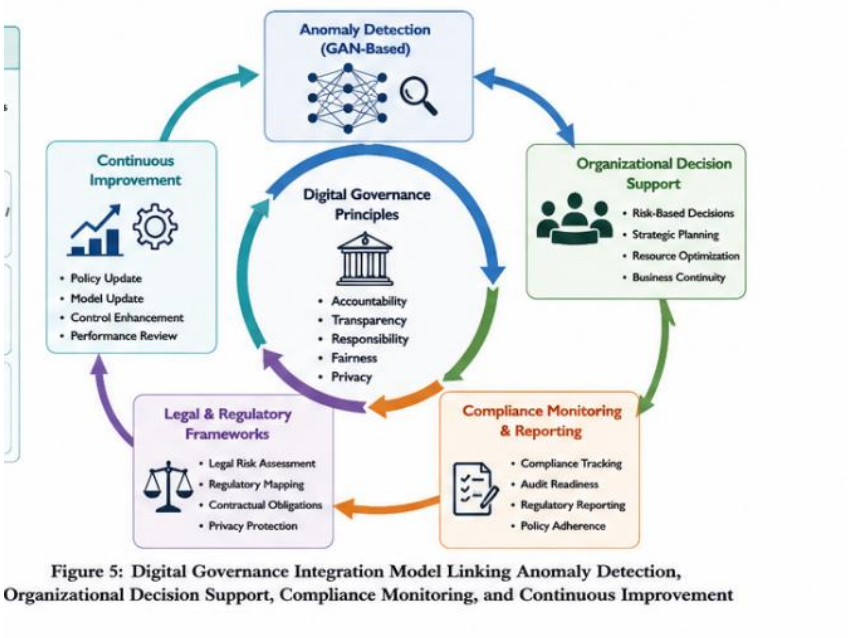

Figure 5. Digital Governance Integration Model Linking Anomaly Detection, Organizational Decision Support, Compliance Monitoring, and Continuous Cybersecurity Improvement.

5. Conclusion

The present paper introduced a novel GAN-Based Anomaly Detection Framework for Cybersecurity, bringing together Artificial Intelligence and technology management, legal risk assessment, regulatory compliance, and digital governance to the field of cybersecurity. The sophistication and complexity of cyber threats are growing, making traditional signature-based intrusion detection systems (IDS) more difficult to use and update to detect previously unknown attacks and adapt to a constantly changing network. To overcome these drawbacks, the proposed framework introduces Generative Adversarial Networks (GANs) as the foundation of the intelligence for anomaly detection, and it is extended from the technical threat detection into the strategic cybersecurity management level.

The proposed framework is unique in that it has a multidisciplinary approach. The framework doesn't just classify attacks but creates a clear relationship between intelligent detection, organizational decision making, legal accountability and governance processes. With technology management integrated, anomalies discovered can be prioritized based on the impact on the organization, need for business continuity, and resource availability. At the same time, the legal risk assessment and compliance layer maps the cybersecurity incidents to internationally accepted frameworks, such as the NIST Cybersecurity Framework (CSF 2.0), ISO/IEC 27001:2022 and the General Data Protection Regulation (GDPR) to ensure regulatory compliance and enhance organizational accountability.

The proposed architecture also plays a crucial role in digital governance, fostering transparency, traceability, and evidence-based cybersecurity management. Compliance mapping, audit documentation, and governance-focused reporting make anomaly detection a holistic

organizational ability. This holistic strategy helps security managers, technologists, and policy makers to make decisions and ensure compliance with legal and regulatory obligations.

The framework also fills an important gap in the research literature. A number of research works are studied on intrusion detection and anomaly detection using GAN but few of them have integrated technology management, legal risk and governance into a single cyber security framework. The proposed study aims to offer a conceptual basis for the design of intelligent cybersecurity solutions that emphasize technical efficacy and organizational resilience, leveraging these complementary domains.

The suggested framework is only a conceptual model and thus has some limitations. This study is not empirical-based; it does not aim at implementation or benchmarking of the performance of the framework. Therefore, a quantitative assessment with intrusion detection datasets is not included. The restriction allows for future work to test the framework with publicly accessible data, compare various architectures of GANs, measure the computational cost of the framework, study methods of explainable AI, and test the framework under real conditions of enterprise cyber security.

The framework can also be expanded in future studies to include federated learning, explainable AI, AI large language models, blockchain-based audit solutions, and automated compliance check solutions. These improvements may lead to greater scalability, transparency, interoperability, and trustworthiness, contributing to the secure digital transformation of various sectors of the business.

To conclude, the proposed structure shows that efficient cyber security is not just about accurate anomaly detection. Sustainable cyber resilience is only possible when intelligent detection capabilities are integrated into the technology management, compliance, organizational governance and strategic decision support. The proposed framework provides a holistic framework for future AI-powered cybersecurity management systems and helps foster more secure, compliant, and governance driven digital ecosystems.

References

1. I. Goodfellow *et al.*, "Generative Adversarial Nets," in *Proc. Advances in Neural Information Processing Systems (NeurIPS)*, Montreal, Canada, 2014, pp. 2672–2680.
2. A. Dunmore, J. Jang-Jaccard, F. Sabrina, and J. Kwak, "A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection," *IEEE Access*, vol. 11, pp. 76071–76094, 2023, doi: 10.1109/ACCESS.2023.3296707.
3. W. Lim, K. Y. S. Chek, B. T. Lau, and C. T. C. Lin, "Future of Generative Adversarial Networks (GAN) for Anomaly Detection in Network Security: A Review," *Computers & Security*, vol. 139, Art. no. 103733, 2024, doi: 10.1016/j.cose.2024.103733.
4. M. Ring, D. Schlör, D. Landes, and A. Hotho, "Flow-Based Network Traffic Generation Using Generative Adversarial Networks," *Computers & Security*, vol. 82, pp. 156–172, 2019.
5. N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems," in *Proc. Military Communications and Information Systems Conference (MilCIS)*, Canberra, Australia, 2015.
6. I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in *Proc. ICISSP*, 2018.

7. NIST, *Cybersecurity Framework (CSF) 2.0*, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2024.
8. International Organization for Standardization, *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*, Geneva, Switzerland, 2022.
9. European Parliament and Council of the European Union, "Regulation (EU) 2016/679 (General Data Protection Regulation)," *Official Journal of the European Union*, vol. L119, pp. 1–88, 2016.
10. V. G. S. Ruffo, D. M. B. Lent, M. Komarchesqui, V. F. Schiavon, M. V. O. de Assis, L. F. Carvalho, and M. L. Proença Jr., "Anomaly and Intrusion Detection Using Deep Learning for Software-Defined Networks: A Survey," *Expert Systems with Applications*, vol. 256, Art. no. 124982, 2024.
11. A. Dhadhania, J. Bhatia, R. Mehta, S. Tanwar, R. Sharma, and A. Verma, "Unleashing the Power of SDN and GNN for Network Anomaly Detection: State-of-the-Art, Challenges, and Future Directions," *Security and Privacy*, vol. 7, no. 1, e337, 2024.
12. S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Hoboken, NJ, USA: Pearson, 2021.
13. F. M. Anis, M. Alabdullatif, S. Aljbli, and M. Hammoudeh, *"A Survey on the Applications of Deep Learning in Network Intrusion Detection Systems to Enhance Network Security," IEEE Access*, vol. 13, pp. 185357–185373, 2025, doi: 10.1109/ACCESS.2025.3624952.
14. L. Zhen, N. H. Kamarudin, V. J. Kok, and F. Qamar,*"Anomaly Detection Model in Network Security Situational Awareness Based on Machine Learning: Limitation, Techniques, and Future Trends," IEEE Access*, vol. 13, pp. 126084–126129, 2025, doi: 10.1109/ACCESS.2025.3589620.
15. A. Dunmore, J. Jang-Jaccard, F. Sabrina, and J. Kwak, *"A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection," IEEE Access*, vol. 11, pp. 76071–76094, 2023, doi: 10.1109/ACCESS.2023.3296707.
16. F. M. Anis, M. Alabdullatif, S. Aljbli, and M. Hammoudeh, "A Survey on the Applications of Deep Learning in Network Intrusion Detection Systems to Enhance Network Security," *IEEE Access*, vol. 13, pp. 185357–185373, 2025, doi: 10.1109/ACCESS.2025.362495.
17. L. Zhen, N. H. Kamarudin, V. J. Kok, and F. Qamar, "Anomaly Detection Model in Network Security Situational Awareness Based on Machine Learning: Limitation, Techniques, and Future Trends," *IEEE Access*, vol. 13, 2025, doi: 10.1109/ACCESS.2025.3589620.
18. S. Narula, M. Ghasemigol, J. Carnerero-Cano, A. Minnich, E. Lupu, and D. Takabi, "Exploring Research and Tools in AI Security: A Systematic Mapping Study," *IEEE Access*, vol. 13, pp. 84057–84080, 2025, doi: 10.1109/ACCESS.2025.3567195.

19. S. Ennaji, F. de Gaspari, D. Hitaj, A. Kbidi, and L. V. Mancini, "Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects," *IEEE Access*, vol. 13, pp. 148613–148645, 2025, doi: 10.1109/ACCESS.2025.3600984.

20. M. Li, Y. Qiao, and B. Lee, "A Comparative Analysis of Single and Multi-View Deep Learning for Cybersecurity Anomaly Detection," *IEEE Access*, vol. 13, pp. 83996–84012, 2025, doi: 10.1109/ACCESS.2025.3564066.

21. Dunmore, J. Jang-Jaccard, F. Sabrina, and J. Kwak, "A Comprehensive Survey of Generative Adversarial Networks (GANs) in Cybersecurity Intrusion Detection," *IEEE Access*, vol. 11, pp. 76071–76094, 2023, doi: 10.1109/ACCESS.2023.3296707.