Security Model Against Private Data Sharing by Streaming (OTT) Platforms Using Generative Adversarial Networks

Michael Moeti, Anna-Marie Jansen van Vuuren, Joey Jansen van Vuuren and Makhulu Relebogile Langa
Tshwane University of Technology, Pretoria, South Africa

MoetiMN@tut.ac.za
Jansenvanvuurenja1@tut.ac.za
Jansenvanvuurenjc@tut.ac.za
Relebogilelanga@gmail.com

Abstract: The expansion of television streaming services has transformed media consumption, providing unparalleled convenience and access to content. Streamers frequently gather comprehensive user data, encompassing viewing patterns, individual preferences, and financial details. This data can be commercialised via collaborations with external advertisers and data brokers, thereby engendering considerable privacy violations, identity theft, and user confidence deterioration. Generative Adversarial Networks (GANs) present a promising method for improving detection techniques of data transmitted to third parties. GANs can be trained to replicate standard data flow patterns and detect anomalies that suggest unauthorised data sharing. Additionally, GANs can produce synthetic data that simulate authentic user behaviour, thereby aiding in developing resilient real-time detection models. Moreover, GANs can create sophisticated data anonymisation techniques to monitor whether user data has been shared. This paper introduces an innovative, multifaceted security and privacy model utilising GANs and deep learning methodologies to identify and alleviate these threats. It compares the GAN model against traditional Support Vector Machine and Random Forests Classifier models. Our methodology integrates anomaly detection and graphs convolutional networks with generative adversarial networks to detect dubious data-sharing activities. The proposed model illustrates the efficacy of deep learning models, specifically GANs, in identifying unauthorised data-sharing platforms.

Keywords: Streaming platforms, Data privacy, Generative adversarial networks (GANs), Anomaly detection, Unauthorized data sharing

1. Introduction

1.1 Background

In today's world, streaming services, alternatively known as over-the-top (OTT) platforms, are a popular choice for users to access a wide range of content like music, podcasts, and films with just a few clicks (Vaidya et al., 2023). Television streaming services are generally preferred by viewers because, for a small monthly fee, they have access to widely popular movies, documentaries, and series (Shah and Mehta, 2022; Polisetty et al., 2023).

The leading international streamers are Netflix, Canal+, Amazon Prime, Shahid and AppleTV+. Streamers with a strong footprint in the USA and the Global North are Hulu, tubi, Roku Channel, Peacock, Max, Paramount+ and Pluto TV (Nielsen, 2024). However, Amazon Prime has the most significant footprint in North America. With this subscription service that includes Prime Video, viewers can watch stand-alone videos by purchasing them on Amazon.com through Prime Video.

Netflix dominates Western Europe and Australasia, except China, where Tencent Video has the most significant footprint with 124 million subscribers. In North Africa and the Middle East, most viewers subscribe to the free Arab service called Shahid. In Central and West Africa, francophone Canal+ is the most popular streamer, while Showmax leads Southern and East Africa, with 15 countries listing this streaming service as holding the monopoly in their territories. Still, Netflix is the largest global streaming service, with the biggest footprint in 78 countries (Visual Capitalist, 2024). Currently, Netflix's biggest competitor for 'eyeballs', as the streamers colloquially refer to viewers, is the free online service YouTube (Statista, 2024). Therefore, we used Netflix and YouTube as our case studies in this paper.

The authors investigate using advanced generative models, specifically GANs, to develop a comprehensive security and privacy framework for detecting unauthorised data sharing on OTT platforms. We emphasise developing a comprehensive security and privacy model that combines GANs with deep learning methods to detect unauthorised data sharing, allowing for timely detection and notification of illicit activities. Thus, we propose a multifaceted security and privacy model for detecting unauthorised viewer data sharing in streaming platforms using deep learning and GANs. This model's primary function would be to protect viewers' information and thus maintain consumers' trust. In addition, the model takes advantage of GANs' adversarial learning

process to reduce false positives, improve detection accuracy, and increase the adaptability of anomaly detection systems. Furthermore, FedDGANs can improve detection models by keeping training data private.

1.2 Security Concerns

Viewers have embraced streaming platforms because the monthly subscription fee is usually cheaper or the same price as visiting a traditional cinema, and you can watch content in your home. However, this convenience and flexibility come at a cost. Viewers' privacy is often compromised as these services collect valuable viewer data to enhance the user experience (Shim et al., 2022). This includes viewing habits and preferences, device information, location data, demographic information, and payment information (Chalaby et al., 2023). While this may seem harmless, concerns have been raised about the privacy implications of this data collection, particularly regarding third-party sharing or selling of viewer data (Andreotta et al., 2021; Pekpazar et al., 2023).

This practice raises questions about who has access to this sensitive information and how this data is being used. Users can fall prey to financial scams linked to their streaming accounts, for example, getting an e-mail alerting them that their streaming account is unpaid or that it has expired, like in Figure 1 below. An unassuming viewer could type in their account details without verifying that the bill/invoice is coming from the streaming service, thus falling for the hoax, and allowing a criminal to access their banking or credit card details.

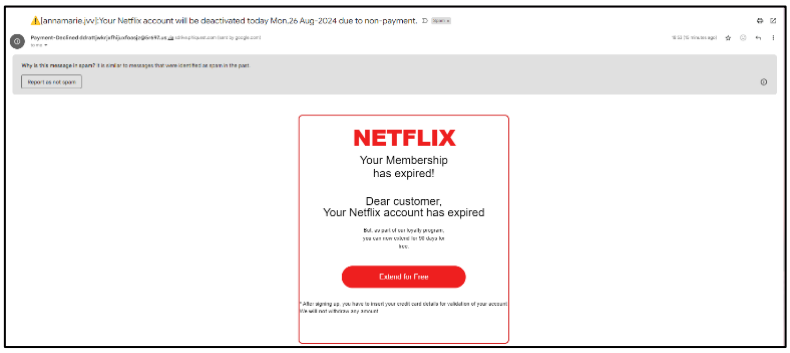

Figure 1: Example where a scammer attempts to get access to a user's bank details

Many users are unaware of the extent to which their viewing habits are being tracked and disseminated to advertisers or other companies (Pathak, 2022). This lack of transparency can erode trust between viewers and streaming services, leading to concerns about potential misuse of personal data and legal consequences. Yet, limited methods are available to ascertain if viewer data is disseminated to third-party corporations.

2. South African Streaming Services and Users' Data

2.1 Interviewing Individual Streaming Services on Data Protection: Their Perspective

The authors of this paper, hailing from South Africa, contacted the leading streaming services in their country, namely Showmax, Disney+, Netflix and eVod.[1], to interview them about their data policies and the processes they employ to safeguard their users' data. We excluded the national broadcaster, SABC+, from the survey since they are a free VOD service, and users do not need personal payment data to register for this service. Though we sent a list of five questions to these streamers and followed up with them numerous times, only one streamer responded to our query, namely Multichoice, the parent company of Showmax.[2]

Multichoice employs the company Irdeto to safeguard its satellite and streaming services. According to their spokesperson, they deploy a range of advanced tools and technologies to detect and combat piracy. As he put it, "our efforts have led to numerous successful raids and arrests across the African continent, targeting illegal streaming operations and other forms of piracy to protect MultiChoice Group's content" (Thulare, 2024). Multichoice's spokesperson elaborated further by stating:

[1] eVod is the Video-on-Demand and live streaming service of the South African free to air broadcaster, etv.

[2] Showmax recently went into a partnership with the United Kingdom's Comcast.

> *The MultiChoice Group remains dedicated to addressing piracy through strong partnerships and technological innovation, ensuring viewers can legally access authentic, high-quality content. In collaboration with enforcement and judicial agencies. MultiChoice Group is committed to safeguarding the content they invest in to provide customers and subscribers with the latest and most relevant programming.*

When probing further into the data collected from individual viewers, including the algorithms that monitor their viewing patterns, the response was as follows:

> *As part of our operations, we continuously assess security protocols to ensure that individual data is protected. At the same time, our data analysis focuses solely on understanding piracy patterns to enhance our protective measures. We gain insights that aid our anti-piracy efforts by leveraging proprietary and publicly available data supported by machine learning algorithms and artificial intelligence (Thulare, 2024).*

Without a comprehensive response from the streamers themselves, we turned to an investigative journalist who provides in-depth coverage of all the South African streaming services to various local and international news outlets. His responses are summarised in the next section.

2.2 Interviewing an Expert on South African Streaming Services: A User's Perspective

The journalist we interviewed, Thinus Ferreira, has covered the South African broadcasting industry for the last thirty years. In the last ten years, as the OTT services Showmax and Netflix entered the market, he reported on their activities. As he needs to subscribe to all of these streaming services to do his job, he argues that his data privacy and safety as a user is of enormous concern to him (Ferreira, 2024). The first concern that he raised is that streaming services keep a user's data, even after a user cancels their subscription. He uses the streamer Showmax as an example. As an experiment, he recently deleted his Showmax profile to test if they would keep his details. Since then, he has received multiple e-mails from urging him to re-subscribe, as he explains:

> *The e-mail was directly addressed to me. This means they kept my name and my e-mail address in a database. However, since I am no longer their customer, they are supposed to delete my details and NOT keep them on record. This has been a huge eye-opener as to how my personal and contact details are kept despite whatever regulations or consumer laws might exist about it in South Africa.*

A prevalent approach for streaming services, like other business organisations, is to explicitly articulate their data-sharing practices within their privacy policy or terms of service agreements (Solove, 2022). Companies may offer users the choice to opt in or opt out of data sharing, enabling them to make informed decisions regarding utilising their information (Aridor et al., 2023). But this is not always the case, as explained by Ferreira (2024):

> *Occasionally, I will get an email saying, "Our terms and conditions have been updated", but it does not specify how it was updated. When the e-mail does provide a link, and you click on it, it only shows the terms and conditions. Therefore, you do not realise how it has changed from what it was previously. In extreme cases, you are not even taken to the terms and conditions but to a generic Question & Answer page and must click further to actively go and find the information about the terms and conditions. So, you are not really helped and guided about your rights and how specifically your data is being used.*

According to Ferreira, all of the South African streamers are culprits, and there is not a single one he can highlight that has asked him for specific permission, as a subscriber, to use his personal data and viewing preferences.

> *I cannot recall anyone explaining in detail how they would handle my personal data when I signed up. I think it is about instant gratification. They want to onboard a user as fast as possible before they might lose you. They usually also allow you to subscribe for a week or a couple of days for free – like a drug dealer that might give a new user a first taste for free to get somebody hooked and will extract payments after that once the person is now addicted.*

He cautions that there is more than one option under the settings of a streaming platform. When a user subscribes, they are usually automatically or "by default" subscribed to specific user preferences, which is not necessarily in the customer's best interest, as it often concedes that a service can collect personal data from them. Consumers can choose to change this option, but many do not even consider looking at the different options since they generally trust the streaming service to look after their interests. He does concede that many organisations, even browsers like Google Chrome and Microsoft Edge, follow this approach.

Many South African organisations store the data they collect from their users on the cloud. Ferreira has independently confirmed that every service that streams in South Africa, from Netflix to Disney+, Amazon Prime Video, VIU, Showmax, and Apple TV+, stores its users' data outside South Africa's.

> *It will be stored wherever they hire their server space, and it could be anywhere – literally from the Arizona desert or India. I have only found that SABC+ collects only its users' e-mail addresses and stores this data with Discover Digital (which runs SABC+ on behalf of the SABC) which is based in South Africa.*

Ferreira also raised a concern about how the streamers tend to 'feed' him the same content based on their algorithms that determine viewing preferences. While he acknowledges that it is part of their business plan to keep users engaged, he describes it as "being kept in a content cage", (Ferreira, 2024):

> *I watched Science Fiction recently on Netflix SA. Now, their recommendation algorithm feeds me suggestions, pop-ups, and tiles of content on Sci Fi. So, I am never exposed to something different or new outside of my already established "preferences". Therefore, if you give away your personal viewing preferences, services exploit it in a dangerous way where you get more of the same unless you deliberately decide to break out of what is constantly being recommended to you. It is like with streaming services, we are living The Matrix movie.*

Streamers and viewing platforms like YouTube build a consumer profile of a viewer based on what they watch. While it is part of a strategy to keep users engaged and returning to the platform, a user might never be introduced to other content that they might enjoy since these algorithms have broken this viewer down according to "elementary choices", which Ferreira explains as follows:

> *It is like that toy for toddlers, where the triangle can only go through the triangle hole, and the block can only enter through the block shaped hole. Nothing else "fits" through these holes. The result is that these streaming recommendations, based on personal data, narrow the viewpoints and viewing diet of the user. A physical radio or television news bulletin, even one that is possibly politically influenced or biased, will still have within that bulletin, stories and reporting that the consumer did not "choose" or that does not fit their expectation – but you will still be exposed to it and hear it and see it. On a streaming service, you literally see what you want to see because the algorithm and recommendation engine feed you the eye candy you already said is the flavours you like most.*

Ferreira suggests that streaming services should have an opt-in and opt-out button for their viewing preferences. Then, a user could opt out of being 'fed' the same content repeatedly. By implementing these measures, companies can assure users that their data is managed responsibly and ethically.

Through the above interview, it has become apparent that Ferreira trusts none of the streaming services with his data and has evidence and cases that motivate his distrust. Considering that he reports for the largest online news services in the country, *News24* and *Netwerk24*, as well as large international entertainment websites like *Variety*, this does not bode well for these streamers. However, by ensuring transparency and granting users authority over their data, streaming companies can exhibit their dedication to safeguarding user privacy and cultivating trust in their brand.

3. The Suggested Solution: Using Gans to Protect User's Data and Privacy

Streaming services and OTT platforms need to institute stringent data security protocols to safeguard user information from unauthorised access or breaches. This may encompass the encryption of sensitive information, routine security assessments, and adherence to industry standards for data protection. By implementing these measures, companies can assure users that their data is managed responsibly and ethically. By prioritising user privacy and security, companies can cultivate robust relationships with their customers and uphold their reputation in the marketplace. Nonetheless, it is crucial to acknowledge that despite robust data security protocols, breaches may still transpire due to cyber threats and vulnerabilities. Consequently, companies must prioritise transparency and communication with customers during a data breach to preserve trust and credibility. To supplement these measures to ensure viewer privacy, the power of artificial intelligence (AI) and machine learning (ML) can provide practical solutions to cyber challenges (Mohamed, 2023; Salem et al., 2024). This is especially true in those complex cases where viewer data is shared with third parties through IP tracking and video traffic tracking (Kattadige et al., 2022; Anande et al., 2023).

Deep learning has recently emerged as a critical component of modern anomaly detection, with various architectures designed to deal with the high-dimensional, temporal, and heterogeneous properties of network traffic data (Roy, 2024). The advancement of innovative technologies, such as Generative Adversarial Networks

(GANs), can assist in identifying and mitigating potential breaches before their occurrence (Lu et al., 2023), thereby enhancing overall cybersecurity protocols (Borky & Bradley, 2019).

GAN establishes a precise deep-learning method for solving complex problems (Elsayed et al., 2024; Sun et al., 2023). According to (Brandão Lent et al., 2024; Hyun Yoon & Ku Kim, 2023; Lim et al., 2024), GANs perform well against traditional models such as Support Vector Machines (SVM) and Random Forests (RF), due to their additional layers of networks. This detection can be accomplished through various mechanisms, such as privacy-preserving frameworks, federated learning, and sophisticated data analysis techniques. Transformational deep learning architectures like GANs have significant implications for anomaly detection since GANs have two neural networks: the generator and the discriminator. These two networks compete to outperform each other. The generator creates synthetic data that looks like real data, while the discriminator classifies it (Haque, 2021; Lin et al., 2020). Iterative training improves both networks: the generator produces realistic samples, and the discriminator distinguishes authentic and generated data. The GAN training alternates generator and discriminator optimisation. Initially, the generator generates data that the discriminator can easily spot as fake. However, as the generator updates its parameters, it generates data that the discriminator finds harder to detect. In contrast, the discriminator updates its parameters to better distinguish real from generated data (Truong-Huu et al., 2020). Implementing advanced solutions and taking a proactive stance on security creates a more robust foundation for customer trust and loyalty (Salem et al., 2024).

Determining data sharing with third parties requires a multifaceted approach encompassing an understanding of previously mentioned approaches. Streaming and OTT services must adhere to their own stipulated privacy policies, and those employed by these companies must be aware of the ethical considerations surrounding data sharing. Lastly, they need to know the technological frameworks that enable this process.

4. Security and Privacy Model to Detect Unauthorised Data Sharing in OTTs

GANs are useful for detecting unauthorised data sharing, especially in addressing data imbalance and discovering new methods. Traditional fraud detection models use supervised learning methods that require lots of labelled data. In the OTT domain, abnormal traffic flows far exceed normal ones, creating highly imbalanced datasets that hinder conventional models. GANs generate synthetic network traffic flow data to equilibrate training datasets and improve anomaly detection models.

GANs are effective in generating synthetic data (Bobadilla & Gutiérrez, 2024; Madarasingha et al., 2022). In the context of data sharing detection, the ability of GANs to generate synthetic data that mimics real network traffic is of immense value (Anande et al., 2023). Network traffic data for data sharing commonly exhibit characteristics that are either highly subtle or entirely novel, making them difficult to detect using traditional models that rely on predefined patterns. By simulating both legitimate traffic flow and irregular traffic flow, GANs create a rich, diverse training dataset that enables data sharing detection models to learn the intricate behaviours of data sharing without being constrained by the availability of labelled traffic flow data (Chang et al., 2021). This capability positions GANs as an ideal solution for anomaly detection in the dynamic and high-stakes OTT environment, where unauthorised data-sharing strategies continuously evolve (Adenubi & P. Oduroye, 2024). However, they also present risks related to the potential leakage of sensitive information from the training datasets (Saxena & Cao, 2021). To address these risks, the Federated Differentially Private Generative Adversarial Networks (FedDPGAN) framework can be introduced to maintain user privacy while still enabling generative modelling and using Wasserstein GAN principles (Kundroo & Kim, 2023; Zhang et al., 2021).

Identifying viewer data sharing by streaming platforms with third-party marketers can be efficiently accomplished using FedDPGANs and deep learning techniques, especially when integrated with privacy-preserving methods and FL frameworks. The integration of these technologies guarantees viewers' data security while facilitating valuable insights into data-sharing practices. As depicted in Figure 1, we provide a step-by-step overview of how we applied GANs for detecting unauthorised data sharing:

Step 1: Training on Normal Data:

- We train the GAN using one of the NetTiSA (Network Time Series Analysed) dataset (Koumar et al., 2024), which consists of a collection of datasets with DNS over HTTPS traffic.
- The generator then learns to produce synthetic samples that mimic normal data distribution, while the discriminator is trained to distinguish between real and synthetic data.

Step 2: Generation of Synthetic Data:

- After training, we use the trained generator to produce a set of synthetic data samples. These synthetic samples should ideally resemble the normal instances present in the training data.

Step 3 Anomaly Detection:

- We combine the synthetic data generated by the GAN with the original standard network flow data.
- We then use a traditional anomaly detection technique (time series analysis) to identify instances that deviate significantly from the expected distribution of normal network traffic flow.
- Instances that are dissimilar to both the real and synthetic data are considered potential.

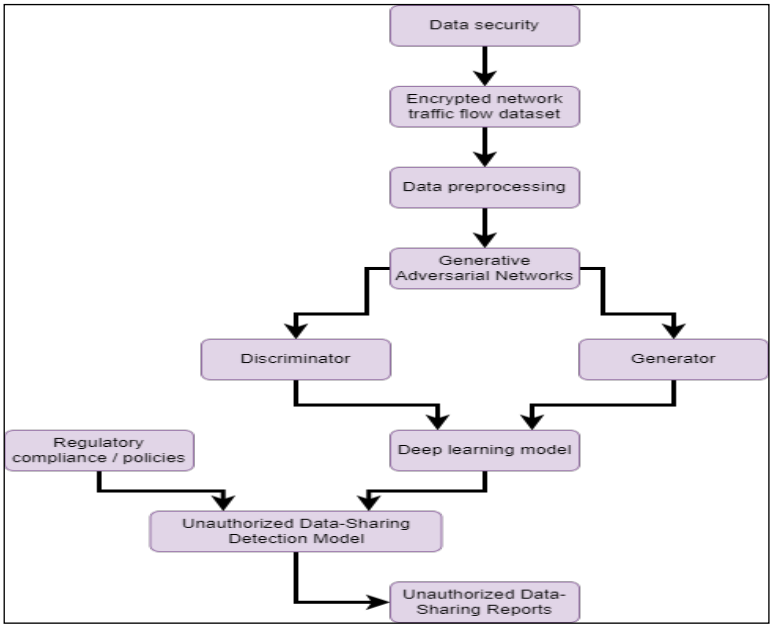

Figure 2: Unauthorized data-sharing detection model process

5. Development of the Model

5.1 Dataset

The dataset used in this study, “Collection of datasets with DNS over HTTPS traffic” (Koumar et al., 2024), contains essential network traffic features such as SRC_IP, DST_IP, SRC_PORT, DST_PORT, PACKETS, BYTES, and DURATION. Each feature provides critical insights into the data flow between network nodes, helping to establish a baseline pattern for expected traffic flows.

5.2 Normal Pattern Identification

To define a baseline for normal dataflows, we calculated the statistical averages for key metrics (e.g., mean, standard deviation, and range of PACKETS and BYTES) for typical flows between source and destination IPs. These metrics provided a reference point to distinguish between benign and anomalous data flows in encrypted multimedia streams. A heatmap in Figure 2 the frequency of common dataflows across source-destination pairs illustrates the network's standard patterns and frequent data routes.

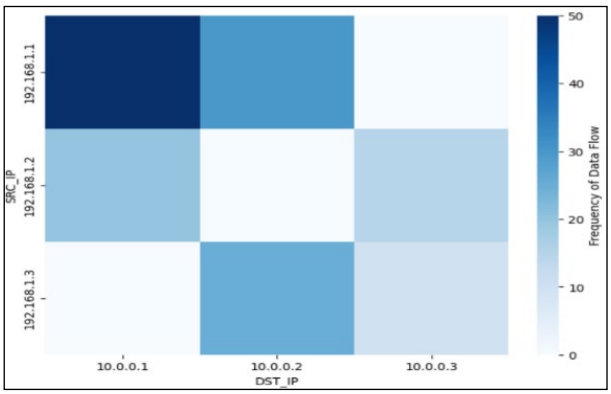

Figure 3: Frequency of common dataflows across source-destination pairs

5.3 GAN Model Setup and Training

The next step was to use the GAN deep learning algorithms to detect anomalies. The GAN comprised of two components:

- Generator: Learns to create synthetic data flows that resemble the usual pattern.
- Discriminator: Evaluates data flows to distinguish between real and synthetic flows, flagging anomalies when they deviate from the expected baseline.

Training Procedure*:* The GAN was trained using only standard data flow patterns, allowing the generator to mimic typical traffic while the discriminator identified outliers. Using average pooling, flattening, and fully connected layers enabled the model to prevent overfitting and improve generalisation to diverse network traffic types.

Equation*:* The pooling layer operation, represented in Equation 1 were used to calculate the mean of inputs within the pooling window to reduce data dimensionality while retaining crucial information:

Equation 1: Pooling layer operation equation.

$$Z_{i,j} = \frac{1}{k' \times s'} \sum_{m=0}^{k'-1} \sum_{n=0}^{s'-1} Y_{i,j \times s'+n}$$

This training technique allowed the GAN to generalise patterns effectively, minimising false positives and ensuring reliable anomaly detection.

5.4 Evaluation of the Model

The next step was the evaluation stage. The model's effectiveness was evaluated using four key metrics as shown below: Overall Accuracy, Precision, Recall, and F1 Score, as seen in Equation 2. These metrics provide a comprehensive understanding of the model's performance, balancing the rate of true positives against false positives. Figure 3 show the graphical representation of the results of the GAN model. These results indicate that the model accurately distinguishes between normal and anomalous data flows, demonstrating strong robustness across multiple network conditions.

Equation 2

$\text{Precision} = \frac{TP}{TP + FP}$	$\text{Recall} = \frac{TP}{TP + FN}$	$\text{F1 Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$

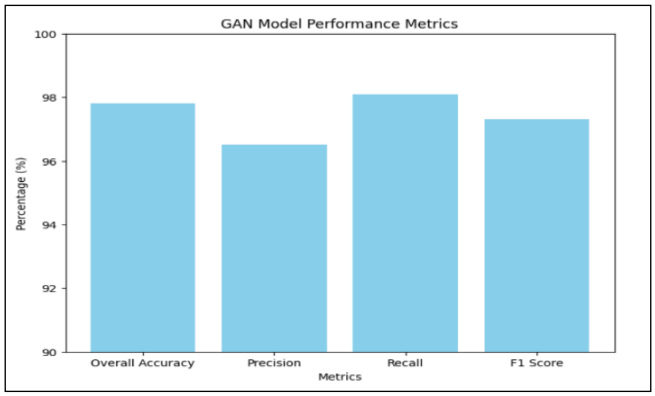

Figure 4: Performance metrics of the GAN model

5.5 Results of Anomalous Flow Detection

After training, we tested the GAN discriminator on new data flows. The model successfully identified deviations from the baseline as anomalies, with minimal false positives. Figure 4 presents a time series plot showing detected anomalies over time, where spikes indicate detected deviations from the usual pattern. This visualisation illustrates the model's sensitivity in real-time anomaly detection.

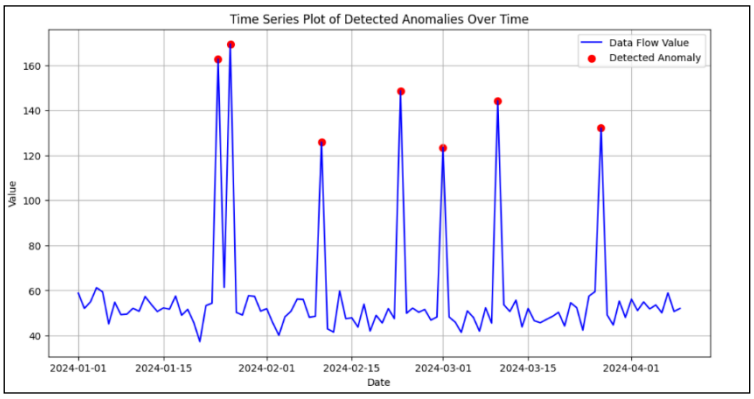

Figure 5: Time Series Plot of Detected Anomalies over time

5.6 Result

The datasets provide a large and unique combination of labelled traffic. The generated DoH and labelled real-world HTTPS traffic provide the ground truth data for training network classifiers and evaluating their performance. Moreover, packet capture is used for IP flow-based traffic analysis, detection, and classification to experiment with novel traffic features. In using real-world data to test the detection algorithm, we applied FedDPGAN to test the flow of streaming on a single device, ensuring that the streaming device's data remains secure and unexposed to the model. This was used to improve understanding of DoH behaviour and other HTTPS traffic phenomena in a large-scale network environment. The plot in Figure 5**.** shows the accuracy of over 100 epochs. The accuracy starts low and gradually increases as the model is trained on more data. The curve eventually plateaus, indicating that the model has reached its maximum accuracy for the given dataset and training parameters.

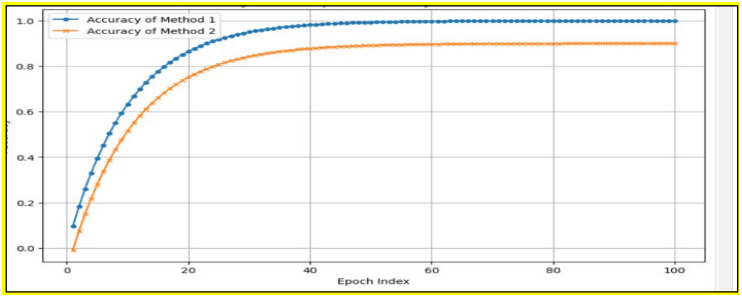

Figure 6: Accuracy of the Proposed Anomaly Detection Method

5.7 Comparative Analysis with Benchmark Models

To validate the model's performance, we compared it with traditional classifiers, notably Support Vector Machine (SVM) and Random Forests (RF), from the results of Suresh et al. (2024) and Pekar and Jozsa (2024)..Suresh et al. (2024)and Pekar and Jozsa (2024) respectively, where both revealed high-performance metrics on large-scale datasets; however, Fig 5 only shows the proposed GAN-based anomaly detection (Method 1) and SVM (Method 2) since the performance results of SVM against RF were almost similar. Based on the large-scale dataset, this paper's performance metrics surpass them, although it has used a different large-scale dataset. The results shown in Table 1 are represented in Figure 6 The GAN model achieved the highest accuracy and F1 score, surpassing traditional models by over 4%, indicating its superior capability in identifying abnormal flows in complex, encrypted networks and DNS over HTTPS traffic environments.

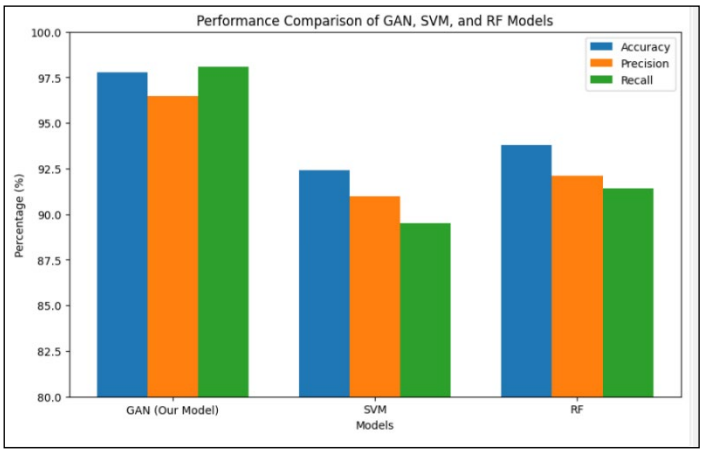

Figure 7: Performance comparison of GAN, SVM, and RF

Table 1 below shows these models' comparative accuracy and F1 scores against the GAN-based model.

Table 1: Models' comparative accuracy and F1 scores against the GAN-based model

Model	Accuracy	Precision	Recall
GAN (Our Model)	97.8%	96.5%	98.1%
SVM	92.4%	91.0%	89.5%
RF	93.8%	92.1%	91.4%

5.8 Analysis of Results: Insights and Implications

As shown in this paper, GANs and deep learning can revolutionise the detection of unauthorised data sharing. These advanced machine-learning methods have improved the precision, efficacy, and reactivity of anomaly detection systems. GANs can generate synthetic datasets to improve detection model training, making institutions more resilient to advanced cyber threats. A security and privacy model for detecting unauthorised data sharing on OTT platforms uses GANs and deep learning models, showing their adaptability to complex network data flow patterns. These systems can significantly reduce false positives while maintaining precision and recall, improving operational efficiency. Adversarial training has also successfully detected network data flow anomalies, allowing institutions and consumers to respond quickly to data violations.

The dynamic nature of data-sharing tactics necessitates a continual evolution of a multifaceted security and privacy model for detecting unauthorised data sharing in OTT platforms to maintain consumers' privacy and data security. Adversarial training is pivotal in enhancing the system's robustness and adaptability to new fraud tactics. By incorporating adversarial examples into the training process, the models can better understand the subtle nuances of fraudulent activities and learn to identify them more accurately.

Adversarial training's iterative nature allows the model to adapt to fraud changes in real time. The framework can update its training dataset with transactional data as new fraudulent strategies emerge, keeping the model current with scammer's movements. The system can improve over time by recording and analysing fraud alert results like confirmed fraud and false alarms. This feedback can improve algorithm precision and recall by adjusting hyperparameters and feature selections.

6. Conclusion and Recommendation

The security of OTT streaming is critical in any anomaly detection model, requiring strong measures to safeguard against various threats, including adversarial attacks, data manipulation, and system vulnerabilities. An extensive security strategy must be incorporated into the unauthorised data-sharing detection model to guarantee resilience against these potential threats. Furthermore, the model must be engineered to endure adversarial assaults that aim to exploit weaknesses in the machine learning models. Adversarial training methods can be utilised to enhance the training dataset with adversarial examples—deliberately constructed inputs intended to deceive the model. Exposing the unauthorised data-sharing detection system to these perturbations during training enables the model to identify and counteract such threats, thereby improving its resilience against advanced unauthorised data-sharing strategies.

More investigation into innovative adversarial methods will be essential for safeguarding data in streaming from emerging threats. As fraudulent tactics advance, the capacity of models to adapt and mitigate these strategies will be crucial for preserving the integrity of financial transactions. This involves examining the incorporation of anomaly detection models that employ unsupervised learning to recognise previously unobserved fraudulent patterns. Implementing AI-driven anomaly detection systems significantly impacts the future of data security, privacy compliance, and customer trust within the OTT sector. Enhancing the efficacy of a comprehensive security and privacy model for detecting unauthorised data sharing on streaming platforms can mitigate risks related to fraudulent activities and improve the overall customer experience. Timely and precise fraud identification mitigates customer impact, enhancing loyalty and trust in streaming services.

References

Adenubi, A. O., & P. Oduroye, A. (2024). Data security in big data: challenges, strategies, and future trends. *INTERNATIONAL JOURNAL OF RESEARCH IN EDUCATION HUMANITIES AND COMMERCE, 05*(02), 01-15. https://doi.org/10.37602/ijrehc.2024.5201

Anande, T. J., Al-Saadi, S., & Leeson, M. S. (2023, 2023/03/28). Generative adversarial networks for network traffic feature generation. *International Journal of Computers and Applications, 45*(4), 297-305. https://doi.org/10.1080/1206212x.2023.2191072

Bobadilla, J., & Gutiérrez, A. (2024, 2024/02). Wasserstein GAN-based architecture to generate collaborative filtering synthetic datasets. *Applied Intelligence, 54*(3), 2472-2490. https://doi.org/10.1007/s10489-024-05313-4

Borky, J. M., & Bradley, T. H. (2019). Protecting Information with Cybersecurity. In *Effective Model-Based Systems Engineering* (pp. 345-404). Springer International Publishing. https://doi.org/10.1007/978-3-319-95669-5_10

Brandão Lent, D. M., da Silva Ruffo, V. G., Carvalho, L. F., Lloret, J., Rodrigues, J. J. P. C., & Lemes Proença, M. (2024). An Unsupervised Generative Adversarial Network System to Detect DDoS Attacks in SDN. *IEEE Access, 12*, 70690-70706. https://doi.org/10.1109/access.2024.3402069

Chang, Q., Yan, Z., Qu, H., Zhang, H., Baskaran, L., Zhang, S., & Metaxas, D. (2021). Federated Synthetic Learning from Multi-institutional and Heterogeneous Medical Data.

Elsayed, S., Mohamed, K., & Madkour, M. A. (2024). A Comparative Study of Using Deep Learning Algorithms in Network Intrusion Detection. *IEEE Access, 12*, 58851-58870. https://doi.org/10.1109/access.2024.3389096

Ferreira, T. (2024, 30 September). *Does South African streaming services do enough to protect my data? A journalist's perspective* [Interview].

Haque, A. (2021, 2021/05/18). EC-GAN: Low-Sample Classification using Semi-Supervised Algorithms and GANs (Student Abstract). *Proceedings of the AAAI Conference on Artificial Intelligence, 35*(18), 15797-15798. https://doi.org/10.1609/aaai.v35i18.17895

Hyun Yoon, J., & Ku Kim, H. (2023, 2023/07). Why do consumers continue to use OTT services? *Electronic Commerce Research and Applications, 60*, 101285. https://doi.org/10.1016/j.elerap.2023.101285

Koumar, J., Hynek, K., Pešek, J., & Čejka, T. (2024, 2024/02). NetTiSA: Extended IP flow with time-series features for universal bandwidth-constrained high-speed network traffic classification. *Computer Networks, 240*, 110147. https://doi.org/10.1016/j.comnet.2023.110147

Kundroo, M., & Kim, T. (2023, 2023/10). Federated learning with hyper-parameter optimization. *Journal of King Saud University - Computer and Information Sciences, 35*(9), 101740. https://doi.org/10.1016/j.jksuci.2023.101740

Lim, W., Yong, K. S. C., Lau, B. T., & Tan, C. C. L. (2024, 2024/04). Future of generative adversarial networks (GAN) for anomaly detection in network security: A review. *Computers & Security, 139*, 103733. https://doi.org/10.1016/j.cose.2024.103733

Lin, Z., Khetan, A., Fanti, G., & Oh, S. (2020, 2020/05). PacGAN: The Power of Two Samples in Generative Adversarial Networks. *IEEE Journal on Selected Areas in Information Theory, 1*(1), 324-335. https://doi.org/10.1109/jsait.2020.2983071

Lu, T., Wang, L., & Zhao, X. (2023, 2023/05/22). Review of Anomaly Detection Algorithms for Data Streams. *Applied Sciences, 13*(10), 6353. https://doi.org/10.3390/app13106353

Madarasingha, C., Muramudalige, S. R., Jourjon, G., Jayasumana, A., & Thilakarathna, K. (2022, 2022/04). VideoTrain++: GAN-based adaptive framework for synthetic video traffic generation. *Computer Networks, 206*, 108785. https://doi.org/10.1016/j.comnet.2022.108785

Nielsen. (2024, August 2024). *July Exhibits Rare Upswing in TV Viewing, Amplified by Streaming and First Days of Summer Olympics, according to Nielsen's The Gauge™*. Retrieved 12 September from https://www.nielsen.com/news-center/2024/july-exhibits-rare-upswing-in-tv-viewing-amplified-by-streaming-and-first-days-of-summer-olympics-according-to-nielsens-the-gauge/

Pekar, A., & Jozsa, R. (2024). Early-Stage Anomaly Detection: A Study of Model Performance on Complete vs. Partial Flows. *arXiv preprint arXiv:2407.02856*.

Roy, S. (2024). *A comprehensive Survey on Network Traffic Anomaly Detection using Deep Learning*. https://doi.org/10.13140/RG.2.2.32071.30884

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024, 2024/08/04). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data, 11*(1). https://doi.org/10.1186/s40537-024-00957-y

Saxena, D., & Cao, J. (2021, 2021/05/08). Generative Adversarial Networks (GANs). *ACM Computing Surveys, 54*(3), 1-42. https://doi.org/10.1145/3446374

Statista. (2024, June 2024). *Leading streamers worldwide across major streaming platforms in June 2024, by average viewers*. Retrieved 18 August from https://www.statista.com/statistics/1482635/top-streamers-by-average-viewers/

Sun, H., Plawinski, J., Subramaniam, S., Jamaludin, A., Kadir, T., Readie, A., Ligozio, G., Ohlssen, D., Baillie, M., & Coroller, T. (2023). A deep learning approach to private data sharing of medical images using conditional generative adversarial networks (GANs). *PLOS ONE, 18*(7), e0280316-e0280316. https://doi.org/10.1371/journal.pone.0280316

Suresh, K., Velmurugan, K. J., Vidhya, R., & Kavitha, V. (2024). Deep Anomaly Detection: A Linear One-Class SVM Approach for High-Dimensional and Large-Scale Data. *Applied Soft Computing*, 112369.

Thulare, I. (2024, 27 September 2024). *Irdeto and Multichoice Responds to Security and Privacy Questions* [Interview].

Truong-Huu, T., Dheenadhayalan, N., Pratim Kundu, P., Ramnath, V., Liao, J., Teo, S. G., & Praveen Kadiyala, S. (2020, 2020/10/06). *An Empirical Study on Unsupervised Network Anomaly Detection using Generative Adversarial Networks* Proceedings of the 1st ACM Workshop on Security and Privacy on Artificial Intelligence, http://dx.doi.org/10.1145/3385003.3410924

Visual Capitalist. (2024, June 2024). *Mapped: The Most Popular Video Streaming Service by Country*. Retrieved 17 August from https://www.visualcapitalist.com/cp/mapped-the-most-popular-video-streaming-service-by-country/

Zhang, L., Shen, B., Barnawi, A., Xi, S., Kumar, N., & Wu, Y. (2021). FedDPGAN: Federated Differentially Private Generative Adversarial Networks Framework for the Detection of COVID-19 Pneumonia. *Information systems frontiers : a journal of research and innovation, 23*(6), 1403-1415. https://doi.org/10.1007/s10796-021-10144-6