© NOV 2025 | IRE Journals | Volume 9 Issue 5 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I5-1712196

Cybersecurity Challenges in Digital Music Streaming Platforms

TOMILOLA AYENI
Business Administration, University of Northampton

Abstract *- The transformation of the music industry toward streaming has accelerated the proliferation of digital music platforms, enabling millions of users to access vast catalogues on demand. However, this shift to cloud-based and mobile delivery models has concurrently expanded the exposure of the industry to cybersecurity threats. This article assesses key cybersecurity risks faced by digital music streaming platforms. Some of these risks includes credential stuffing, API vulnerabilities, data breaches of user and metadata, and the cracking of Digital Rights Management (DRM) controls. Through literature review and case examples, we identify weaknesses in platform architectures and DRM systems, and evaluate emerging ways of mitigation such as stronger encryption, two-factor authentication, and blockchain-enhanced DRM. The findings show the urgency for platforms to adopt proactive security measures and for stakeholders to prioritise user data protection and rights management innovations. The paper concludes with recommendations for better approaches and suggestions for future research.*

Keywords: Cybersecurity, Digital Rights Management, Streaming Platforms, Data Protection, Music Industry.

I. INTRODUCTION

Over the past decade the global music industry has shifted dramatically from sales of physical media and downloads toward streaming subscription models. The convenience of on-demand access via platforms such as Spotify, Apple Music and their peers, has catalyzed this transition, and with it the creative content and usage data formerly locked in physical form now resides in the cloud and is accessed via mobile devices. (Williams, A., 2022)

Due to this transition, the music industry now has a lion share of the streaming sector. This market is skyrocket to about 66.62 billion dollars by 2029, as many more people will adopt the use of streaming platforms (See figure 1).

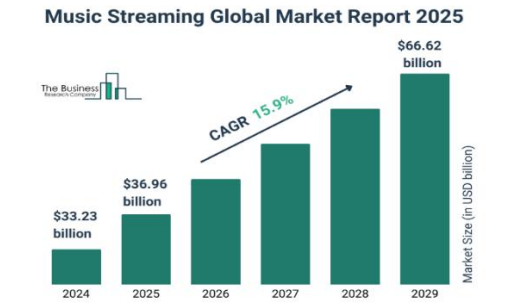


Figure 1: Music streaming global market report. Adapted from The Business Research Company.

A few of the majorly used streaming platforms by number of subscribers include Spotify, Sound Cloud, Apple Music, YouTube Music, Amazon Music, Pandora, Mixcloud Deezer, Tidal. Spotify takes the largest, with a total of 500 million subscribers, followed by Sound Cloud with 170 million subscribers, followed by Apple Music with 88 million subscribers and YouTube Music with 80 million subscribers. Also, Amazon music has a total of 75 million subscribers, Pandora has 47 million subscribers, Mixcloud has 20 million subscribers, Deezer has 16 million subscribers and Tidal has 5 million subscribers (See figure 2).

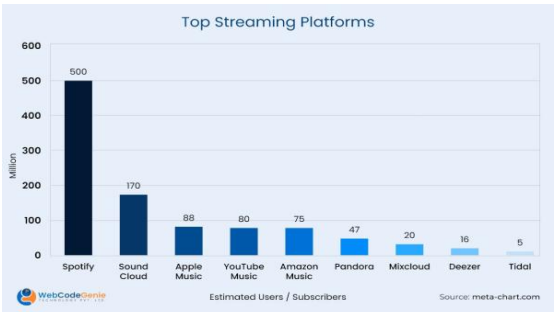


Figure 2: Top streaming platforms by number of subscribers. Adapted from WebCodeGenie Technology PVT.LTD.

However, in this environment, cybersecurity is increasingly a critical concern for the entertainment industry. Protecting the integrity of content delivery, safeguarding user data, and protecting revenue flows from disruption or abuse (Arenal et al., 2024).

© NOV 2025 | IRE Journals | Volume 9 Issue 5 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I5-1712196

The research problem addressed here is that streaming platforms are subject to a growing number of cyber threats. Including unauthorized access, piracy, data leaks, and rights infringements, which undermine consumer trust, reduce revenue for rights holders, and threaten the sustainability of the business model. The objective of this paper is to identify and analyze the most critical cybersecurity challenges faced by digital music streaming services, assess the state of platform and DRM security architectures, and provide recommendations for improved protection. The importance of this work rests in protecting creative content and user data in a digital entertainment ecosystem where scale, interconnectivity and data flows are high and rapidly evolving.

II. RESEARCH ELABORATIONS

The music industry is a very confiscated industry with many processes, management procedures, collective management uses and services, stakeholders and data. However, the understanding of music rights ownership, collection and streaming on a global scale, differs across countries. This is because almost all countries have specific legal and institutional structures that guides their operation along relevant issues (Arenal et al., 2024).

Generally, some of these processes include music composition and sound recording. While a few services include Hotels, Televisions, Gyms, Bars, Live music events and streaming platforms like Spotify, YouTube Music, Amazon Music and so on. For these processes to be fully executed, it involves multiple workflows of data and revenue among different stakeholders (services/uses, CMOs, and right holders for composition and sound recording) (See Figure 3).

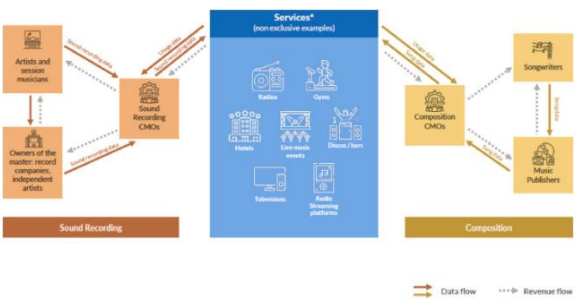


Figure 3: Music industry copyright and collective management uses and services, stakeholders, and data and revenue flows. Adapted from Sitonio and Nucciarelli (2018).

Putting a focus on streaming platforms, cyber threat remains a major issue. Some of these issues are identified below.

A. Nature of Cyber Threats in Streaming

Streaming platforms face multiple threat vectors. Credential stuffing and phishing attacks target user accounts, which may grant access to premium features or payment information. Pirated or unofficial streaming apps may serve malware or leak user data. Data breaches involving user metadata, subscription details, and behaviour logs pose a risk both to consumers and to platforms' reputations. For example, a few studies particularly stated how unofficial apps and open-source file sharing enable risks that goes beyond just simple piracy issues (Amaya Alviz, 2022). Other means with which this industry can be attacked can be found in cloud-based services and APIs. From improperly configured APIs to unsafe authentication management, or inadequate encryption, people who practice cyber fraud can retrieve user information or content without authorization. Although the study of Fan, (2022), on digital music streaming platforms reveals how that mobile distributed machine learning techniques can be used to fight cyberattacks.

B. Digital Rights Management (DRM) and Piracy Prevention

DRM remains a cornerstone for protecting digital music content, but it is also subject to security and usability challenges. DRM systems such as those used by major streaming services (e.g., AES-based encryption, license-token systems) are designed to restrict access, copying, and redistribution of content (Ghatak, et al., 2004; Fortinet Cyber Glossary, 2025). However, the evolution of streaming has changed DRM's role: as noted in recent work, the shift from copy-based to streaming-based consumption has altered the nature of rights and permissions, introducing new vulnerabilities (Scharf, 2022). In fact, a 2021 analysis discovered that digital rights management issues in a few of the Indian OTT music services made it easier to steal streamed content (Dabholkar et al., 2021). On the side of the artists, labels, and rights holders, severe repercussions like DRM cracking or circumvention may lead to illegal duplication, lost profits, and a decline in platform credibility.

C. *Platform Security Architectures*

Streaming platforms need to implement strong, secure structures to fend off threats. These structures include tokenization, secure cloud storage with very strict access, two-factor authentication, and end-to-end encryption. Examples of these are SSL/TLS for data in transit and AES for stored content. Mind you, Artificial intelligence (AI) and behavior-based anomaly detection are being used more and more to keep an eye on suspicious device or user behavior such as bots that inflate streams or misuse user login details. One promising direction is blockchain-based DRM frameworks which store watermarking and rights metadata immutably, as demonstrated in a 2024 review of "SecureRights" (Madushanka et al., 2024). The combination of strong platform architecture and intelligent detection systems is required to address both technical and behavioural threats.

D. *Legal and Ethical Concerns*

The cybersecurity issues in streaming are not only technical in nature. Which is the reason for legal structures like the General Data Protection Regulation (GDPR) in the EU or the California Consumer Privacy Act (CCPA) in the US to ensure streaming platforms are obligated to handle user data, breach notification, and consent properly. Platforms must balance providing personalised services with respecting user privacy rights. Meanwhile, rights holders must ensure DRM systems do not in an unreasonably manner restrict legitimate user rights (e.g., fair use, device portability). Literature on DRM highlights consumer-rights concerns and regulatory pressure (Dhingra, 2017).

E. *Case Study Example*

As a focal example, consider the study of "Cyberattacks Defence in Digital Music Streaming Platforms" (2022) which used mobile distributed machine learning to detect attack patterns (Fan, 2022). While the paper focuses on detection architecture, it exposes key real-world risks that streaming platforms face. Another commentary highlights how music artists and platforms are now defending against cyber-attacks as streaming volumes rise. (SteelToad OP, 2023) Lessons learned: evolving attacker models (bots, automation), the importance of continuous monitoring, and the need for layered security rather than relying solely on DRM.

III. RESULTS AND FINDINGS

Having done a thorough Stan thesis of different literatures as well as case studies, this section presents the emerging results that consolidates the current issues in the music industry as regard cybersecurity.

1) Threat categories: It was discovered that streaming platforms are at great risk of identity theft attacks like phishing and stuffing, exploitation of personal content and piracy through DRM bypass. Aside that, data breaches like user metadata and subscription records, as well as automated fraud like streams made by bots are still very prevalent.
2) DRM vulnerabilities persist: Although encryption and licensing strategies are still in place, many platforms especially in emerging streaming markets, do not fully incorporate DRM strategies. This poor implementation, weakens their security measures and makes it possible to extract user content (Dabholkar et al., 2021).
3) Comparative platform practices: While major streaming services invest heavily in security (authentication, monitoring), smaller or regional platforms may lack resources, thereby raising risk exposure.
4) Emergent technologies improving defense: AI-driven behaviour analytics, blockchain-based DRM frameworks as in "SecureRights," and cloud tokenisation architectures provide promising enhancements.
5) User-data privacy remains a core challenge: Data collected by streaming services (listening behaviour, social integration) creates sensitive user profiles whose theft or misuse leads to reputational and regulatory risks. (British Music ASL).
6) Need for layered security: The findings underscore that DRM alone is insufficient; a multi-layer defence (platform architecture, users authentication, analytics, legal/compliance) is required.

A proposed figure would illustrate "Major Cyber Threats to Music Streaming Platforms (2020 - 5025)" with categories such as credential attacks,

© NOV 2025 | IRE Journals | Volume 9 Issue 5 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I5-1712196

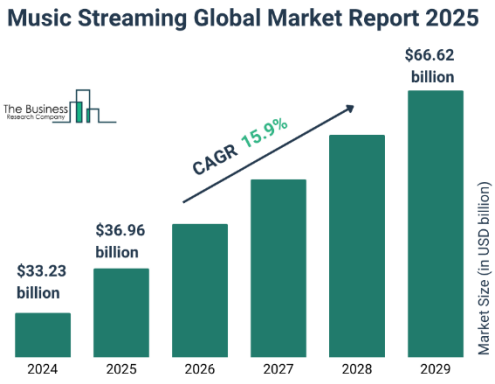
bot/stream fraud, DRM bypass, data breach — and approximate prevalence or impact ranking.

IV. CONCLUSION

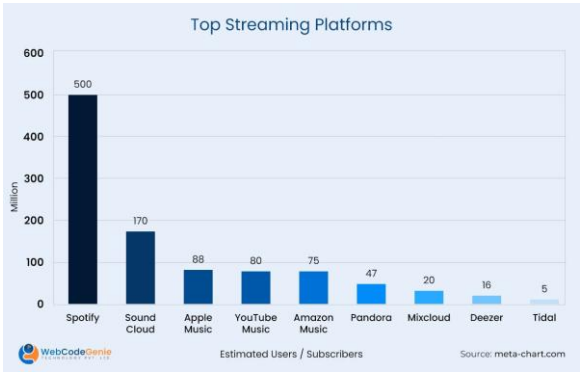
This article has shown that digital music streaming platforms operate in a high-risk cybersecurity environment. Numerous sources of threat are created by the level of access, the sensitivity of user and rights-holder data, and the importance of constant delivery of content. Although, DRM's function as a protective measure is still significant, it is no longer enough on its own. Platforms must adopt comprehensive security strategies: robust encryption and authentication, behavioural monitoring and anomaly detection, blockchain-enhanced rights management, and strong data-privacy governance. Furthermore, user education (e.g., promoting strong passwords, two-factor authentication) and transparent security policies will help build trust. Rights holders and platform providers should collaborate on threat intelligence sharing and standardised fraud detection frameworks. Future research should explore the effectiveness of AI-driven detection systems in streaming fraud, and the application of decentralised ledger technologies (blockchain) for rights management at scale. As the entertainment industry continues to evolve, cyber-resilience must also continue to become stronger in order to ensure the sustainability and growth of streaming platforms.

V. APPENDIX

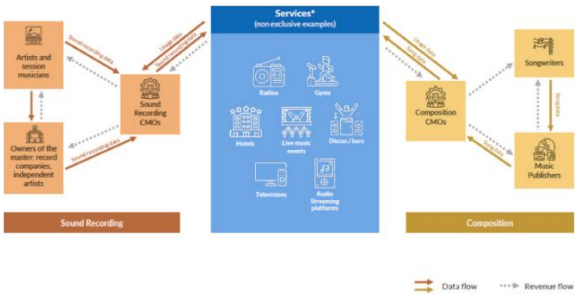
1.



2.



3.



REFERENCES

[1] Fan, G., 2022. Cyberattacks Defense in Digital Music Streaming Platforms by Mobile Distributed Machine Learning. *Computational Intelligence and Neuroscience*, *2022*(1), p.1701266.

[2] Sitonio, C. and Nucciarelli, A., 2018. The impact of blockchain on the music industry.

[3] Scharf, N., 2022. The evolution and consequences of digital rights management in relation to online music streaming. *Legal Studies*, *42*(1), pp.61-80.

[4] Missing Profits – Music Artists Defense Against Cyber Attacks, SteelToad OP; 2023. Available at https://www.steeltoad.com/missing-profits-music-artists-defense-against-cyber-attacks/?utm_source=chatgpt.com#sources

[5] "Digital rights management (DRM) – What it is, how it works, use cases," Fortinet Cyber Glossary, 2025 Cyber Glossary, 2025 Cyber Glossary, 2025 Cyber Glossary, 2025. Available: What Is DRM? Digital Rights Management Explained | Fortinet

[6] Dhingra, M., 2017. Digital rights management & its consumer concerns. *International Journal of Engineering Research & Technology*, *6*(3), pp.438-441.

[7] "Music Streaming Platforms and Data Privacy Concerns," ASL-Inter Interactive blog, 2023. Available: https://www.asl-inter.com/music-streaming-platforms-and-data-privacy-concerns/

[8] Ghatak, P., Tripathi, R.C. and Chakravarti, A.K., 2004. Digital Rights Management: An integrated secure digital content distribution technology. *Journal of Intellectual Property Rights*, *9*(4), pp.13-31.

[9] Dabholkar, A., Kakarla, S. and Saha, D., 2021. Looney tunes: Exposing the lack of DRM protection in indian music streaming services. *arXiv preprint arXiv:2103.16360*.

[10] Williams, A., 2022. Digital Streaming Services. *Geo. L. Tech. Rev.*, *6*, p.322.

[11] Madushanka, T., Kumara, D.S. and Rathnaweera, A.A., 2024. SecureRights: A blockchain-powered trusted DRM framework for robust protection and asserting digital rights. *arXiv preprint arXiv:2403.06094*.

[12] Arenal, A., Armuna, C., Ramos, S., Feijoo, C. and Aguado, J.M., 2024. Digital transformation, blockchain, and the music industry: A review from the perspective of performers' collective management organizations. *Telecommunications Policy*, *48*(8), p.102817.

[13] Sitonio, C. and Nucciarelli, A., 2018. The impact of blockchain on the music industry.

[14] Amaya Alviz, How is cybersecurity affecting the music industry?, Medium; 2022. Available at: How is cybersecurity affecting the music industry? | by Amaya Alviz | Medium