World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Movie streaming platforms, cyber threats and data privacy

Tomilola Ayeni *

Department of Business Administration, University of Northampton, Northampton, United Kingdom.

World Journal of Advanced Research and Reviews, 2025, 28(02), 2140-2142

Publication history: Received 08 October 2025; revised on 19 November 2025; accepted on 21 November 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.2.3901

Abstract

It is undeniable that online movie streaming platforms have had an impact on the entertainment industry, causing a global on-demand access to movies. However, this digital shift has also expanded exposure to cyberattacks and data-privacy risks. This short communication reviews major threats facing movie-streaming services, including account hijacking, API vulnerabilities, DRM bypass, unauthorized third-party apps, and extensive user-data collection practices. This article draws insight from recent studies and incident reports, highlighting the loopholes in security and privacy governance, particularly among smaller streaming providers. A stronger access control, zero trust architectures, and open data handling policies are some suggestions that could reduce the cyber threat in this sector.

Keywords: Digital Piracy; DRM; Data Privacy; Cybersecurity; Movie Streaming Platforms

1. Introduction

Upon the development of movie streaming platforms like Netflix, Amazon Prime Video and Hulu, the way that people watch movies has evolved significantly. Although more convenient, this model poses serious privacy and cybersecurity issues. Through this movie streaming services, sensitive consumer data like payment details, viewing habits or even intellectual property are available. So, it is easy for cyber attackers to take advantage of platform inconsistency. Either for monetary gain, piracy, or mass data collection.

From the evaluation of recent studies, there are serious privacy risks because publicly accessible viewing metadata and app usage patterns can disclose user demographics or personal preferences [1]. In addition to this, there is increase in in cyber threat as cloud storage, smart TVs, mobile apps, and content delivery networks (CDNs) become increasingly in use. This article will identify major cyber and privacy threats in the online movie streaming industry and recommends practical ways to reduce it.

2. Major Cybersecurity and Privacy Risks

2.1. Account Hijacking and Credential Theft

Streaming accounts are frequently compromised through phishing, credential-stuffing, and password reuse. Stolen accounts are resold on dark-web markets or used to bypass regional content restrictions. Because movie-streaming services store payment cards and subscription data, these breaches create significant consumer-protection concerns [11].

* Corresponding author: Tomilola Ayeni

2.2. Malware, Pirated Apps and Add-Ons

Unofficial movie-streaming apps and browser add-ons often distribute malware while promising free access to premium content. Multiple cybersecurity investigations [8] show that such apps harvest personal data, passwords, or device information. Users may unknowingly grant dangerous permissions.

2.3. DRM Bypass and Content Piracy

Digital Rights Management (DRM) systems protect films from illegal copying or redistribution. However, with the use of screen recording tools, DRM systems can be bypassed due to weak encryption or insecure APIs. Research demonstrates that poorly implemented DRM exposes both the movie files and user data [2, 3, 7]. Tricomi et al., (2022) [4] applied similar findings to game assets but the same mechanisms apply to movie DRM vulnerabilities.

2.4. Gathering Too Much Information

The engagement metrics, device information, geo-positions, and view histories are recorded by streaming services. This gives rise to comprehensive behavioral profiling being produced. As Mekovec (2022) [1] points out, improper use and sharing might lead to one's personal habits, family life, and preferences being revealed.

2.5. Third-Party Advertising and Tracking SDKs

Third-party analytics and ad SDKs can accompany applications involving mobile live streaming. The SDK can store information about consumers across multiple platforms and applications. The consumers' information can become visible to third-party advertisers without required consent if management is inadequate regarding consumers' privacy information.

Limited Compliance on Small Platforms

An issue with smaller movie streaming services is that they do not have strong encryption, notification mechanisms, and comprehensive notions about ensuring customer privacy protection. Larger movie services have more demanding security guidelines [9]. Risks are introduced into this environment.

3. Platform Security Practices and Existing Defenses

Leading platforms currently use

- Multi-factor authentication (MFA)
- Encrypted Streaming (AES and TLS)
- Secure Content Delivery Networks
- Behavior monitoring to identify irregular transactions on accounts
- Watermarking and better DRM

However, smaller platforms tend to face issues while implementing these measures because they lack resources.

Table 1 Common Incidents in Movie-Streaming Platforms

Threat Type	Example Impact	Mitigation Approach
Credential reuse	Account theft, unauthorized access	MFA, password-reset flows
Pirated / modded apps	Malware, data theft	App verification, user alerts
DRM bypass	Illegal redistribution of films	Stronger encryption, watermarking
Insecure API endpoints	Data leakage	API authentication, rate limits

4. Discussion

Internet security on movie sharing services is more than merely safeguarding movie files themselves. The issue here is that movie consumption behavior is being gathered, stored, and analyzed. This is problematic because smaller movie services fail to embrace strong privacy guidelines. This is putting consumers' personal information at risk.

The biggest contradiction within this sector is present in DRM protection mechanisms because they involve exposing information about personal devices while aiming to safeguard property rights. This counteracts one's property rights, which includes having one's personal information secured on the device they purchased.

To enhance resilience, care providers can

- Implement zero trust architecture to verify each device and each session.
- Implement privacy by design (data minimization and anonymity)
- Increase transparency, such as publishing handling and notice processes.
- Educate consumers on how to identify phishing attacks and avoid downloading unofficial applications.
- Establish collaborative threat intelligence networks to identify any organized attacks or pirate rings [12].

5. Conclusion

Despite movie streaming services revolutionizing entertainment, they continue to attract attention from hackers aiming to steal money or access exclusive content. The article focuses on discussing vital threats such as login account manipulation, digital rights management bypass, malware dissemination, and mass information harvesting, while discussing measures such as implementing zero-trust architectures, better DRMs, precise privacy policies, and raising consumer knowledge to diminish these hazards to a great degree. Being a much more crucial priority, this article is dedicated to cybersecurity to secure movie fans and creative assets with growing movie streaming services.

References

[1] Dasgupta, D., 2022. Privacy: A myth in online gaming ?. International Journal of Advanced Mass Communication and Journalism.

[2] Patat, G., Sabt, M. and Fouque, P.A., 2022, May. Exploring widevine for fun and profit. In 2022 IEEE Security and Privacy Workshops (SPW) (pp. 277-288). IEEE.

[3] Patat, G., Sabt, M. and Fouque, P.A., 2023. Your DRM can watch you too: Exploring the privacy implications of browsers (mis) implementations of widevine EME. arXiv preprint arXiv:2308.05416.

[4] Tricomi, P.P., Facciolo, L., Apruzzese, G. and Conti, M., 2023, April. Attribute inference attacks in online multiplayer video games: A case study on Dota2. In Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy (pp. 27-38).

[5] NowSecure (2025). OTT App Security: What Streaming Developers Must Know in 2025. https://www.nowsecure.com/blog/2025/05/14/ott-app-security-what-streaming-developers-must-know-in-2025/

[6] StreamingMedia (2025). Best Practices for Premium Video Streaming – Content Protection. https://www.streamingmedia.com/Articles/Editorial/Featured-Articles/Best-Practices-for-Premium-Video-Streaming-Part-6-Content-Protection-130269.aspx

[7] Setplex (2025). Why DRM Video Protection Is Essential for Streaming Security. https://setplex.com/blog/drm-video-protection-overview/

[8] Doverunner (2025). Top OTT App Security Challenges and Solutions. https://doverunner.com/blogs/top-ott-app-security-challenges-and-solutions/

[9] Verimatrix (2024). Anti-Piracy Insights: Token Sharing and Unauthorized Streaming Access. https://www.verimatrix.com/anti-piracy/

[10] GuardianDigital (2025). OTT Platform Breaches: Understanding Risks and Restoring User Trust. https://guardiandigital.com/content/ott-platform-data-breach-response

[11] Enciphers (2023). How We Halted Piracy of DRM-Protected Video Content. https://www.enciphers.com/case-study/how-we-uncovered-halted-the-piracy-of-drm-protected-content