GRADUATE BUSINESS SCHOOL

# Paper: 9536 Applied Project

| | |
|---|---|
| **Student Name:** As appearing on transcripts | Haibo Shi |
| **Title of Applied Project:** | Examining Content Protection Mechanisms in Major Digital Rights Management Software: A Comparative Analysis of Technical Architectures and Implementation Strategies |
| **Major** | Master of Business Informatics |
| **Date:** | 20-Mar-2026 |

*To the best of my knowledge, this work is the student's own, meets the required academic standards, adheres to ethical principles, and has not been submitted for examination or publication elsewhere.*

| | |
|---|---|
| **Research Supervisor Name:** | Dr. Cindy Wang |
| **Date:** | 20-Mar-2026 |

# Acknowledgements

I remember to give many thanks to my Heavenly Father for bringing me to New Zealand and opening up a door to study at ICL Graduate Business School and be blessed with dedicated and professional teachers, and be blessed with warm and generous classmates to whom I have shared experiences and ideas with them along this journey.

I give thanks to the Lord Jesus Christ, who through prayer, brought this research topic upon my heart and gave me a definite sense of direction when I needed it the most. I am also equally grateful to Holy Spirit for helping me curious, and capable of understanding more as I drained the scholarly literature and persevere with it, and give me the perseverance to throw myself into it.

I hold a particular debt of gratitude to my supervisor Dr Cindy Wang whose professionalism, rigorous feedback, patient guidance was indispensable to the completion of this study. It was Dr Wang who taught me to step away from the technical description and to make a really comparative analytical argument, which was a lesson that fundamentally influenced both this paper and my development as a researcher.

I would also like to acknowledge the contribution of Florian Roudot and Mohamed Sabt of Univ Rennes whose published research into the Widevine licence-acquisition protocol provided an insight into the security architecture of Google's DRM system that was instrumental in the formulation of the vulnerability analysis in this study. Their rigorous work is a fine example of the kind of transparent, independent security research upon which studies such as this one rest.

Finally, I would like to thank my family. I am deeply grateful to my wife, Sunny Wang, who assumed the responsibility of taking care of our children to give me time to write and to my mother-in-law, Mary Zhang, who gave her generosity on a daily basis in our home and constant prayers sustained me throughout.

# Table of Contents

# Abstract

Digital Rights Management systems play an important role in protecting commercial digital content, but architectural design choices that the large systems have made between providing security robustness and user experience are understudied in the literature. This research fills this knowledge gap by conducting a qualitative comparative case study on three dominant DRM platforms, Google Widevine, Microsoft PlayReady and Apple FairPlay, by understanding how the respective architectures handle the trade-off between content protection and user accessibility and what implementation strategies enable the best optimisation of this trade-off. Guided by a post-positivist philosophy, and based on a theoretical methodology (socio-technical systems theory, access control theory), a four dimensional analytical framework of architectural design decisions, security robustness mechanisms, user experience impact factors and implementation strategies are used to systematically compare the three platforms through thematic analysis of vendor documentation, peer reviewed security research and independent assessments by technical experts in information security.

The results show that the three platforms reflect fundamentally different approaches to the security-usability dilemma at the strategic level, and are dictated by commercial agendas of the companies building and owning them, and not by the technical side of the trade-off. Widevine has a market segmentation divided by introducing a tiered architecture for sharing the trade-off expenses across users by implementing device-dependent quality restrictions. PlayReady places the onus on content providers by having a configurable policy framework with the requirement for implementation expertise. FairPlay eliminates the tradeoff from its ecosystem with its closed hardware integration and focuses costs on users that are requiring cross platform access. The analysis has also shown that implementation context such as, key management architecture, protocol design quality and organisational vulnerability response processes play a far greater role in determining in the real world security effectiveness

than choosing between cryptographic algorithms alone. Vulnerability disclosure as a key organisational factor for long-term protection outcomes mobile DRM's user experience costs are demonstrated to be associated with more than just playback quality, with issues of digital ownership and platform allegiance.

The study concludes that an optimal balance between all deployment contexts is not accomplished by any one platform, and the fusion of the industry's drift towards multi-DRM deployment with the adaptive tiering of content values, the use of forensic watermarking and help users to understand security requirements is the most effective current optimisation strategy. These findings contribute to the academic literature in that they extend the socio-technical systems theory to the analysis of DRM and to bridge a gap that has been documented in the cross-platform comparative research. For modern business behaviour, the study has some guidance about platform selection, strategies to protect in an adaptive way and how to manage security-usability trade-offs in digital content distribution.

# Chapter 1: Introduction

## 1.1 Background

Digital Rights Management (DRM) encompasses a set of access control technologies designed to govern the use and duplication of copyrighted digital content by restricting the unauthorised modification or redistribution of copyrighted digital works (Ma, 2017). These systems exploit cryptographic tools and licence controls and authentication methods to allow access to the protected content to only authorised users under some circumstances. Digital rights management (DRM) is now essential to the modern digital economy and has given intellectual property protection throughout the entertainment, publishing, software and business sectors (Ma, 2017; Acharya et al., 2025).

The DRM market is large and increasing. In 2024, it was worth USD 5.7 billion (about NZD 9.4 billion) which is projected to reach USD 13.5 billion (about 22.3 billion NZD) by 2033, at 9.5% annual growth rate (IMARC Group, 2024). This growth is caused by a number of factors. First of all, streaming platforms such as Netflix, Disney+, and Amazon Prime Video use industry-standard DRM systems (Widevine, PlayReady, and FairPlay) to protect their content libraries massively, generating massive demand for scalable protection (Rafi et al., 2023). Second, over-the-top (OTT) platforms that deliver content directly over the internet are exposed to greater security risk because content (valuations) is transmitted over open networks without the physical security provided by traditional broadcast systems (Filipe, 2016). Third, as software became more of a subscription service rather than something to buy one time, DRM did not stay limited to media, but also to business applications. Gartner (2022) revealed that the worldwide expenditure on public cloud services was Nearly $600 Billion (NZD$955 billion) just in 2023 and a lot of this software needs licence validation and anti-piracy controls. Fourth, the use of DRM by digital publishing and online education platforms to protect educational materials and e-books from unauthorised sharing practices is on the rise.

## 1.2 Research Problem

The adoption of DRM causes an inherent tension between security goals and the accessibility of users. Researchers have tried to capture this fundamental challenge in the design of security mechanisms. Only unauthorised users are to be prevented from accessing the system, but not to cause frustration for the legitimate users (Ding, 2023). As DRM is too concerned with security, there are issues for the user, such as incompatible devices, playback failure, or cumbersome login procedures. On the other hand, systems that emphasise ease of use might fail to offer the sufficient protection from sophisticated attack (Ma, 2017).

The financial stakes are high. Digital video piracy causes USD 29 billion USD (NZD48 billion) estimated losses across entertainment, software and publishing every year, with more than 80% of digital piracy coming from streaming platforms (Roudot and Sabt, 2025). Beyond the loss of revenue, pirated content undermines subscription based and advertising based business models. The music industry has similar issues too, and the annual estimates of losses due to piracy range from USD 12.5 billion (or about NZD 20.6 billion) (Zwattendorfer & Tauber, 2023).

DRM also fits well in complex legal frameworks. The Digital Millennium Copyright Act (DMCA) of 1998 and the Information Society Directive of the European Union in 2001 make it a crime to bypass technological protection mechanisms and opened endless debates about what is fair use and accessibility (Samuelson, 2003). Research has proven that DRM restrictions can be barriers for users with disabilities making use of assistive technologies (Kerscher and Kawamura, 2000; Volckmann, 2024).

Despite how widespread DRM is, comparative research into a balance between security and user experience that major platforms achieve through certain design choices is limited. Previous work has addressed elements of the law and ethics (Samuelson, 2003), or has paid attention to individual implementations (Kasprowski, 2010), or has constructed theoretical models of security with no comparison to actual implementations (Coates and Abroshan, 2024). A lack of in-depth comparative

analyses of design trade-offs of several major DRM systems was noted by Rafi et al. (2023).

## 1.3 Research Questions

How do architectural design decisions in major DRM systems (Widevine, PlayReady, and FairPlay) balance security robustness with user experience, and what implementation strategies optimise this trade-off?

## 1.4 Research Objectives

**Objective 1 Comparative Analysis on DRM Architectures**

To provide a study and comparison between the architectural aspects of Widevine, PlayReady and FairPlay DRM systems, identifying certain architecture design parameters, affecting security strength and user experience.

**Objective 2: Testing of Security-User Experience Trade-Offs**

To determine the impact of security demands in individual DRM systems to user experience in different user deployment situations and device type.

**Objective 3: Optimisation Strategy identification**

To identify and evaluate implementation strategies that are used by major streaming platforms (Netsflix, Disney+, Amazon prime video) and that do an effective job balancing security requirements against user experience.

## 1.5 Motivation and Research Context

This Applied Project is based on professional experiences as a Technical Solutions Analyst at Haihaisoft which is a DRM software company. This is a good background for practical understanding of the challenges of DRM implementation, such as cross-platform, changing piracy threats and access control vs. user experience.

Whilst this professional experience informs practical understanding, the study focuses on Widevine, PlayReady, and FairPlay rather than Haihaisoft's proprietary solutions. These platforms collectively protect the majority of commercially distributed streaming content and reflect three distinct design philosophies, enabling analysis of fundamental trade-offs that transcend platform-specific details.

This study focuses specifically on how security protection balances with user experience are made in design choices in these three platforms, focusing on:

- Security level implementations (hardware versus software security protection) and its respective impact on device compatibility
- Licence management protocols and how it influences user accessibility
- Strategies for cross-platform deployment and their trade-offs
- Industry implementation patterns optimizing the security/usability balance

## 1.6 Significance of the Study

This research is significant to the fields of knowledge and practise as it addresses a documented gap in DRM literature.

**Academic Contributions**

This research responds to a significant gap in DRM research, which has mainly centred on the legal, ethical and theoretical dimensions rather than empirical technical work (Samuelson, 2003; Ding, 2023). By systematically comparing Widevine, PlayReady, and FairPlay this research makes three important contributions to the scholarship.

First, it builds upon existing single-system case studies (Kasprowski, 2010), by providing comparative empirical data for the three most popular commercial platforms, specifically the investigation of how design choices yield various security-usability trade-offs. Second, it constructs an analytical framework that is based on socio-technical systems theory (Ding, 2023), that conceptualises DRM as

systems that combine technical mechanisms, legal mechanisms, and user interactions. This theoretical perspective enables systematic analysis of the interaction between technical design decisions and business requirements and user behaviours to generate various outcomes across different platforms. The framework is based on the access control theory from the research on computer security (Ma, 2017), and models on usability-security trade-off from the research on human-computer interaction, which provide a structured set of criteria to compare DRM implementations. Third, it is a direct response to the gap noted by Rafi et al. (2023), the absence of detailed comparative studies into the internal workings, design trade-offs and practical security performance of major DRM systems.

**Practical Contributions**

The results of the research give actionable information for a number of stakeholder groups:

- DRM developers have comparative knowledge of technical approaches taken by market leaders influencing design selection on security levels of implementation, licence management protocols and cross-platform deployment strategies.
- Content distributors considering implementation of DRM are benefited from a systematic analysis of the capabilities, limitations and implementation trade-offs associated with the platforms, that is specific to the balance of security and user experience.
- Information providers (industry practitioners) are informed in an evidence-based way on multi-DRM deployment strategies as well as adaptive security approaches to maximise the security-usability balance.

This work feeds existing discourses on the effectiveness, efficiency and fairness of various implementations of DRM especially with respect to accessibility, user rights and whether protection mechanisms can keep up with evolving threats (Volckmann, 2024).

## 1.7 Structure of the Report

Chapter 1 has presented the background of the research, research problem, research question, research objectives, and research significance. Chapter 2 presents existing literature regarding DRM architectures and security-usability trade-offs. The qualitative comparative methodology is described in Chapter 3. Findings and discussion are presented in Chapter 4. Chapter 5 concludes with recommendations and directions for future research.

# Chapter 2: Literature Review

This chapter is a review of work that has been conducted on Digital Rights Management technologies, especially in the domain of content protection technologies, technical architectures and implementation strategies, which are relevant to understanding the security-usability trade-off in major DRM systems. The review starts by identifying content protection systems in a theoretical framework that allows for analysing these systems beyond the technical dimensions, and then examines the technical architectures of Widevine, PlayReady and FairPlay. It moves on to discuss encryption and key management techniques, access control and licence management systems, multi-DRM deployment strategies, written security weaknesses and economics which affect technology deployment decisions. The chapter concludes by synthesising the literature to identify research gaps that were dealt with in this study.

## 2.1 Digital Rights Management: theoretical foundations

Digital Rights Management is a complex socio-technical system, which is a combination of technical systems, legal frameworks, business relationships and consumer interactions (Ding, 2023). This conceptualization is based on the socio-technical systems theory which holds that the effectiveness of technology is dependent on interactions between the technical features, organisational processes and human behaviours instead of simply focusing on the technical features (Ding, 2023). This theoretical lens is needed to analyse how various architectural design choices make different trade-off decisions in between security strength and user experience, as technical choices cannot be assessed in isolation to their impact on users and business requirements (Sony & Naik, 2020).

Modern DRM systems are able to carry out a number of interconnected functions, such as access control, usage control, integration with billing systems and support for

legal enforcement (Acharya et al., 2025). Present implementations offer content in encrypted forms, and require authorised users to obtain decryption keys from licence servers (Roudot and Sabt, 2025). This architecture opens up what access control theory calls a 'reference monitor' meddling all access attempts between content providers and consumers (Ma, 2017).

The evolution of DRM over the past is a progressive attempt to balance security and usability. Early systems were based on crude approaches that favoured security over convenience for the user (Acharya et al., 2025). The Content Scramble System (CSS) for DVD protection, was one step forward but easily overcome by DeCSS illustrating a fundamental problem with the fact that content needs to be decrypted for playback leaving some possibilities for extraction (Gillespie, 2006).

Contemporary implementations have moved in a direction of providing hardware backed implementation with Trusted Execution Environments whilst at the same address usability with tiered security models. TEEs employ processor-level security capabilities which are used to isolate the cryptographic operations from the main operating system of the computer, theoretically preventing malware from accessing protected materials(Schneider et al., 2022). This evolution is what human-computer interaction research calls the security-usability trade-off: the more secure something is, the less usable it becomes, and vice versa (Ding, 2023). Understanding how various architecture approaches navigate this trade-off is the focus of this research since Widevine, PlayReady and FairPlay have each taken a different approach in applying hardware-backed security and tiered protection models. The theoretical frameworks discussed in this section thus provide the analytical lens in terms of which these architectural differences are evaluated in the following chapters in order to be able to compare the three systems not only with respect to their technical merit, but in terms of the extent to which they balance security and usability.

## 2.2 Technical architectures of major DRM platforms

This section explores the technical architectures of the three DRM platforms which have been chosen for this study: Widevine, PlayReady and FairPlay, How Different Security-Usability Trade-offs emerge through Their Respective Choices in Mechanism Design. The discussion focuses on the architectural features of the greatest immediate relevance for understanding the specific way in which each platform implements its content protection mechanisms and, therefore, for the comparative analysis that follows.

### 2.2.1 Platform Selection Rationale

Widevine, PlayReady, and FairPlay had been chosen based on 3 criteria that are directly related to the research question. First, they are collectively used to protect the majority of commercially distributed streaming content across the world, compatible with all major device ecosystems: Widevine covers Android and the Chrome environment, PlayReady covers Windows and Xbox, and FairPlay secures Apple's iOS and macOS ecosystems (Patat et al., 2022). Second, each represents a fundamentally different architectural philosophy with distinct security-usability trade-offs (Rafi et al., 2023). Third, this diversity enables comparative analysis of the relationship between protection strength and user accessibility.

### 2.2.2 Google Widevine Tiered Security Model

Widevine's architecture specifically addresses the security-usability trade-off by using a three-tier protection model, where each tier of protection represents a different set of design choices that provide a trade-off between protection and accessibility. According to Roudot and Sabt (2025), these are three levels that represent an incremental approach to security with each level providing a different level of hardware-based protection and, therefore, a different impact on the user experience and are designated Level 1, Level 2 and Level 3 security.

- Level 1 (L1) emphasises security, and performs all content processing and cryptographic functionality in hardware-based Trusted Execution Environments, carries content on secure route such as HDCP (Schneider et al., 2022). This architectural choice offers the best protection but limits the deployment to devices that have special hardware used for security, which reduces accessibility(Agarwal & Cherukuri, 2025). Content providers are capable of providing the best 4K / HDR content through L1, and only about 40% of android devices are reachable (Roudot & Sabt, 2025). This generates a very obvious trade off, better security means fewer accessible devices.
- Level (L2) is an intermediate architecture option, where cryptographic operations are restricted to the Trusted Execution Environment, but content processing and media rendering processes run outside of the Trusted Execution Environment in regular software or dedicated video hardware. Patat et al. (2022) note that L2 is implemented on devices where the full TEE-based processing is not available such as legacy devices, though Android does not natively propose L2 as a security option. This places L2 as a balance between the complete hardware-based security of L1 and the purely software-based approach of L3 - this represented a compromise between greater device compatibility and full hardware-based security of the most sensitive cryptographic functions (Roudot and Sabt, 2025).
- Level 3 (L3) actually implements the cryptography and content processing independently in software, and makes an explicit architectural decision to compromise security in favour of deployment flexibility (Roudot and Sabt 2025). L3 provides near-universality of compatibility (100% of platforms), and with limitations of the content quality to the standard definition (480p) because of security concerns. This kind of tiered structure represents the central issue of the research this is looking at, how architecture can balance security robustness with user experience.

Coates and Abroshan (2024) discuss the real-life security implications of these architectural choices. Widevine L3's implementation in software made it vulnerable to reverse engineering differential fault analysis attack, and security researcher David Buchanan demonstrated how to bypass Widevine L3 with only "a few evenings of work" by using publicly available tools (as cited in Coates & Abroshan, 2024, p. 38 ) .Content providers respond by limiting L3 to lower resolutions, building tiered user experiences with device capabilities directly determining the quality of contents you can access (Patat et al. 2022). This is proving to be a good example of how architectural choices have a direct effect on security effectiveness as well as user experience.

Last year, new research has uncovered more architectural vulnerabilities in Widevine's licence management. Roudot and Sabt (2025) described a replay attack called "Narrowbeer" on the validation of timestamps with flaws in timestamp and validation mechanisms. The vulnerability is due to architectural design flaws where the Content Decryption Module of Widevine did not check chronological consistency between the generation timestamp of the licence request and loading timestamp of the response. Attackers can manipulate these parameters to make licences that have effectively infinite expiration periods (recorded attacks were able to lengthen 24-hour licences to over 100 years) (Roudot & Sabt, 2025). More critically, unauthorised users are able to reuse harvested licences between multiple devices, turning the DRM system from a form of protection mechanism into a potential piracy enabler where small licence files can be used in a sharing context, whilst content is streamed directly from providers infrastructure (Roudot & Sabt, 2025).

### 2.2.3 Microsoft PlayReady: Enterprise Flexibility Architecture

PlayReady's architecture optimises for enterprise flexibility whilst maintaining security (ScoreDetect, 2024; Pellegrini, 2024). It allows the content providers to add granular usage rules such as geographical restrictions, time-limited access, output controls and device-specific authorisations (ScoreDetect, 2024). This policy flexibility

is suitable for enterprise scenarios where a complex access control is needed, but it results in implementation complexity.

PlayReady supports a variety of Windows devices as well as Xbox consoles, smart televisions, and embedded systems (ScoreDetect, 2024). However, Roudot and Sabt (2025) report client identity compromise from some implementations of PlayReady, a case in point that architectural flexibility can add vulnerabilities not present in more restrictive approaches.

### 2.2.4 Apple FairPlay: Closed Ecosystem Architecture

FairPlay is the most restrictive in terms of the architectural approach as it tightly integrates content protection into Apple's hardware and software (ScoreDetect, 2024). This closed ecosystem design is favourable for security as it uses hardware-backed security and at the same time has severe usability constraints. FairPlay is an Apple-only service (iOS devices, macOS computers, Apple TV) which eliminates cross-platform attack vectors by having control over the environment, but reducing the portability of content in a dramatic way (Rafi et al., 2023).

Volckmann (2024) suggests this architectural integration embeds platform lock-in strategies in ostensibly security-focused designs raising questions about the aim of restrictions in terms of content protection or commercial interests. Content purchased from FairPlay protected services cannot be accessed outside of Apple's ecosystem, causing friction for users who need a cross-platform solution. This represents the far end of the spectrum between security and usability, for maximum security, full ecosystem control, there is no user flexibility at all.

### 2.2.5 Key Differences Between Architectural Approaches

The three DRM platforms being studied are all based on quite different design philosophies, each influenced by the ecosystem in which it emerged. Widevine's tiered security architecture prioritises wide deployment flexibility so that content

providers can target a wide range of devices with different levels of protection, although this is necessarily a source of weakness in their software-based implementations, as documented by Patat et al. (2022). PlayReady, by contrast, is geared towards enterprise-scale policy control and cross-platform compatibility, and provides granular licence management features such as key rotation and output protection that allow content providers to have fine-grained authority over how content is consumed (Coates & Abroshan, 2024). FairPlay runs in Apple's closed hardware and software environment, and this enables it to take advantage of device-level security features like the Secure Enclave to provide a well-contained and consistent security, but this comes with the limited compatibility outside of Apple devices. As noted by the authors (Rafi et al., 2023) none of the three systems offer a full arsenal of security features independently; each leaves some aspects of content protection to be carried out by the content provider: this means that the overall security-usability balance is determined not only by the DRM platform itself, but also by the choices made by the organisations implementing it. These differences are reflective of different trade-offs instead of one optimal approach, Widevine focuses on reach over uniform security, PlayReady focuses on flexibility versus implementation complexity, and FairPlay focuses on environmental control versus openness (Rafi et al., 2023). Understanding how each platform addresses these trade-offs is the key to the comparative analysis presented in the following chapters.

## 2.3 Encryption Methodologies and Key Management

Cryptographic protection serves as the root mechanism for the DRM content protection and the choice of encryption algorithm and key management practices dictates the security robustness as well as implementation complexity(Tiwari et al., 2025). This section focuses on the effects of encryption and key management architectural choices in order to understand how they produce various security-usability trade-offs.

The majority of modern DRM platforms use Advanced Encryption Standard (AES) using 128-bit and/or 256-bit keys to encrypt content (CyberSecurity News, 2024; Rehman et al., 2021). AES supports good theory strength with computation rate applicable to real-time decryption during playback (Lu, 2023). However, the practical security of AES-based DRM is completely dependent on the key management practices rather than algorithm strength. This presents an important architectural challenge, namely how to deliver decryption keys to client devices without allowing them to be accessed by unauthorised parties.

The basic architectural weakness is related to the requirements of symmetric encryption. Any device that is approved to play protected content must have access to the decryption key in a readable format, which provides the main attack surface that the adversaries exploit (Masoud & Ali, 2015). Keys stored in device memory when playing are susceptible to extraction via debugging tools, memory dumps or run-time analysis (CyberSecurity News, 2024). Keys embedded in device firmware are vulnerable to reverse engineering attacks in which attackers take apart software binaries to find key-handling logic. The contradictory nature of ensuring legitimate users the keys to play and protecting legitimate users from unauthorised access are the core technical challenges of DRM (Ding, 2023). This contradiction has a direct relationship with the security-usability trade-off, stronger key protection is usually less accessible.

Hardware-based storage of keys in Trusted Execution Environments is an alternative architectural approach, which tries to solve the software vulnerabilities by segregating cryptographic operations in processor-protected memory areas not accessible from the main operating system. Modern processors from Intel, AMD, ARM, and other manufacturers include extensions for security that make it possible to implement TEE functionality, which provides isolated execution environments where sensitive operations can be performed without interacting with potentially compromised software (Bitmovin, n.d.; Hoang et al. 2023). This architectural choice is a good

choice for improved security, however it limits deployment to devices with specialised hardware, which has a direct impact on user accessibility.

Token-based authentication is an alternative method, with the modern DRM systems generating temporary access tokens with time and geographical limitations instead of distributing long lived cryptographic keys (CyberSecurity News, 2024). Industry implementations include millisecond-level expiration periods and binding to IP addresses for access control protection. However, the Narrowbeer attack on Widevine proves that even advanced token-based systems have fundamental vulnerabilities when the mechanisms for timestamp validation do not have logical consistency (Roudot and Sabt, 2025).

## 2.4 Access Control and Licence Management Frameworks

Beyond the cryptographic protection, DRM systems have comprehensive licence management systems for how, when, where and for what the authorised users can access the protected content. These frameworks are used to map the business requirements and to map the policies into technical enforcement mechanisms, which have a direct impact on the user experience. Contemporary platforms of DRM support different licencing models those of subscription access, rental period with set time of expiration, geo restrictions that allow regional distribution deals, device limitations that limit the number of simultaneous playback sessions, output restriction that prevents transmitting high quality content to devices that are not authorised, (BuyDRM, n.d., ScoreDetect, 2024). Each licencing model represents architectural choices between business needs for a product and user convenience.

Licence servers form the authority server parts of DRM architectures, with responsibility for user authentication, entitlement validation, issuing of content decryption keys and enforcement of use policies. When people are trying to view protected content, their devices connect to licence servers, and provide authentication information and ask for permission. According to Pellegrini (2024), providing detailed analysis of DRM licence management systems and servers: validate these credentials

against subscriber databases, check that users have proper entitlements for content requested and respond with encrypted licence packages including decryption keys and content usage policy specifications. ScoreDetect (2024), commercial DRM analytics platform explains how the Content Decryption Module on client devices receive these licence packages, extract the decryption keys, apply certain usage policies on the system, and coordinate with media playback components to decrypt and render content (Roudot & Sabt, 2025).

Device authentication mechanisms are used to limit access to specifically authorised devices. The three platforms have different approaches. Widevine has hardware-based identifiers for L1 and session tokens for L3. PlayReady includes domain-based licencing allowing for multi-device access. FairPlay utilises persistent identifiers in Apple's Secure Enclave, which is the hardest to bypass (Rafi et al., 2023). There have been previous research into the device binding in individual platforms but not between their impacts on the security-usability trade-off, a gap directly pertinent to this study.

## 2.5 Multi-DRM Methods and Cross-Platform Deployment

The fragmentation of DRM landscape across incompatible platforms has led to the emergence of strategies of multi-DRM, which allows the content providers to access audiences across different device ecosystems while ensuring protection. This section discusses implementation strategies executed to deal with cross-platform deployment issues, and this is relevant to the third research objectivity.

Content distributors who cater to users across iOS devices, Android smartphones, Windows computers, web browsers, smart televisions, and gaming consoles are faced with a very real necessity of supporting multiple DRM technologies at a time. No one DRM platform has universal device support and requires parallel implementations (ScoreDetect, 2024). This creates a complexity in implementation, both in terms of costs, and user experience.

Multi-DRM service providers such as Axinom DRM, Intertrust ExpressPlay, and Verimatrix Multi-DRM provide integrated solutions that abstract the complexity away from content providers using unified interfaces for multi-DRM technologies (ScoreDetect, 2024). These platforms usually support the three dominant DRM systems (Widevine, PlayReady, and FairPlay), which allow content providers to encrypt content once, and create platform-specific licence packages dynamically based on the capabilities of the requesting devices. Cloud-based multi-DRM solutions offer an added benefit such as scalability to manage demand peaks, geographical dispersion of licence servers since this lowers latency, and centralized management of encryption keys and policies for use (ScoreDetect, 2024).

However, implementations of multi-DRM create additional complexity and possible security weaknesses. Each of the supported DRM platforms is a different attack surface with unique weaknesses. Content that is encrypted for multiple platforms may be available via the weakest-protected way, as opposed to the strongest. Key management is much more complicated when orchestrating cryptographic materials in multiple DRM systems using different architectural assumptions and security models. Licence server implementations must enforce the policies correctly across platforms with different sets of capabilities and constraint models(H. S., 2024). The likelihood of having to maintain an operational overhead of expertise in multiple DRM technologies and having to monitor security advisories for multiple platforms all represent ongoing burdens for content protection teams. These problems in implementation are directly related to an understanding of what strategies optimise the security-usability trade-off in real-world deployments.

## 2.6 Security Vulnerabilities and Attack Vectors

Understanding content protection mechanisms used by Widevine, PlayReady and FairPlay requires not only to look at their security features but also at their vulnerabilities and limitations. This part is a review of main types of attack vectors which represent a threat to contemporary DRM systems, and it establishes a

framework in which to evaluate the relative resiliency of DRM systems against threats based on their architectural differences.

Security research has repeatedly shown that all modern DRM implementations are vulnerable to attack by the dedicated attacker who has the necessary technical resources (Rafi et al., 2023). Understanding primary attack vectors highlights shortcomings in protection mechanism today.

Software-based client-side DRM implementations present substantial attack surfaces for reverse engineering. Adversaries can use disassemblers and debugging tools to analyse Content Decryption Module binaries, identify key management logic, and extract decryption keys from memory during playback (CyberSecurity News, 2024). Knowledge gained from analysing one version can frequently be adapted to bypass subsequent versions unless fundamental architectural changes are implemented.

Licence manipulation attacks are not directly against cryptographic protections, but are aimed at policy enforcement mechanisms. The Narrowbeer vulnerability against Widevine is a sample of this class of attacks, a vulnerability that exploited some logical flaws in the validation of timestamps to produce licences with arbitrarily extended validity periods (Roudot & Sabt, 2025). Such attacks ignore the strength of cryptography altogether and succeed by analysing protocol state machines and finding the lack of adequate validation logic. Licence sharing and replay attacks allow unauthorised users to access content by re-using licence materials acquired from legitimate subscribers, turning DRM systems from mechanisms that protect content to a potential piracy facilitation infrastructure (Roudot & Sabt, 2025), proving how architectural vulnerabilities can break whole protection systems independent of the strength of the cryptography.

## 2.7 Economic Constraints and Their Role in Implementation Strategies

The architectural and implementation choices made within DRM systems do not exist in an economic vacuum, rather, economic considerations have a big influence on the way that content providers design, deploy, and maintain technical protections. Understanding these economic dimensions is therefore necessary in order to put into perspective the implementation strategies analysed in this study because cost structures and market incentives determine the extent to which organisations tend to focus more on security robustness as opposed to user experience and vice versa.

Implementation and maintenance of DRM systems are large ongoing investments. Licensing fees, integration development, multi-platform testing, and security monitoring involve financial burdens that might be prohibitive for smaller content providers (Zhang and Zhang, 2023). These costs have a direct affect on implementation strategy, with resource constrained organisations preferring simpler single drm solutions. Additionally, major content studios often have specific technical protections that are contractual requirements which constrain options for implementation, whether mandated systems offer an optimal security-usability balance (Wu et al., 2019).

Economic analysis also sheds light on the effects of implementation decisions for end users. Research analysing the digital content markets indicate that overly restrictive protection mechanisms may have a deleterious effect on consumer value and ironically have a corrosive effect by increasing the incentives to pirate rather than decreasing it (Oestreicher-Singer and Sundararajan 2010). Studies of the music industry found that "the less rigid DRM restrictions are and the more flexible consumption is allowed, the more legitimate sales increase and not less" (Volckmann, 2024), adding further weight to the argument that implementation strategies that emphasise user experience do not have to come at the expense of revenue protection. Although these are based on different market contexts, in particular of music as opposed to video streaming, the implications of these results are nevertheless that the security-usability trade-off has real economic implications and that implementation strategies that ignore user experience may end up undermining the commercial goals

that DRM systems are intended to serve.

## 2.8 Gap in Research and Reasonableness

This literature review has examined the architectures, encryption mechanisms, access control systems, security vulnerabilities, and economic factors affecting DRM deployment. The remaining gap concerns how architectural design decisions across the three major platforms affect the security-usability balance, and which implementation strategies best optimise it.

Patat et al. (2022) and Delaune et al. (2024) described Widevine's architecture and how it implements cryptographic algorithms in great detail, whilst Roudot and Sabt (2025) revealed the details of certain vulnerabilities in Widevine's licence acquisition process. These are all interesting studies that provide good insights into how Widevine works and where it has its weaknesses, but are limited to one platform and do not discuss how its design decisions compare with PlayReady and FairPlay. Rafi et al. (2023) provided the first cross-platform security comparison of all three systems, however, their work was carried out in a security-oriented manner and did not address the impact of architectural decisions on the end-user experience. Comparative studies as part of a wider DRM literature, e.g., e-book DRM system study by Oestreicher-Singer and Sundararajan (2010), are limited to specific content domains and do not cover architectural variations, which are relevant for video streaming platforms.

# Chapter 3: Methodology

## 3.1 Introduction

This chapter introduces the methodological approach adopted for answering the research question concerned with the balance between security robustness and user experience in architectural design decisions used in major DRM platforms. Given the proprietary nature of commercial DRM systems, this research takes the form of a qualitative comparative case study with a document analysis and secondary data synthesis based on a post-positivist philosophy. The chapter describes the philosophical basis, research approach and design, data collection procedures, analytical framework and ethical considerations.

## 3.2 Research Philosophy

Research philosophy includes the basic assumptions that a researcher makes about the nature of reality and knowledge, which constitute the epistemological foundation for all the methodological choices that are made (Tripathi et al., 2024; Saunders et al., 2019). This research takes a post-positivist epistemological approach, which recognises the existence of objective reality whilst recognising that knowledge is always constrained by the limits of observation and measurement (Tripathi et al., 2024). Post-positivism acknowledges that all observation is theory-laden and that knowledge claims must be held tentatively, subject to revision as evidence accumulates (Han and Liu, 2024). Post-positivist researchers acknowledge that prior knowledge, theoretical frameworks, and contextual factors influence observation, whilst retaining their commitment to systematic evidence collection and logical reasoning (Tripathi et al., 2024; Saunders et al., 2019).

This investigation takes a post-positivist philosophy because the nature of DRM systems as closed source, commercially proprietary technologies require an epistemological approach that is at the same time committed to systematic analysis, and honest about the limits of what can be known from available evidence. This position is in line with DRM research realities in a number of ways. First, DRM protection mechanisms have the form of objective technical artefacts with measurable properties that can be systematically studied. Second, the access of researcher groups to the full details of the implementation process is limited by commercial confidentiality, leaving knowledge gaps to be inferred from observable behaviours. Third, security vulnerabilities arise that conflict with vendor claims that necessitate epistemological humility regarding vendor documentation. Fourth, implementation details change as software updates occur, which are not necessarily made public, and this means that knowledge claims are like snapshots in time and do not represent permanent truths (Han & Liu, 2024).

The post-positivist approach allows the recognition that the professional experience of the researcher in DRM industry sets interpretive frameworks for how technical documentation is assessed. Rather than considering this background as Bias that should be eliminated, in post-positivist philosophy domain expertise is seen as facilitating complex interpretation but requires reflexive awareness of the influence of prior knowledge in analysis (Han & Liu, 2024). This study therefore adopts the framework of systematic comparison and explicit analytical criteria based on socio-technical systems theory (Ding, 2023) and access control theory (Ma, 2017) in order to ensure that interpretations remain well-grounded in documented evidence. Triangulation of several independent sources also helps mitigate the risk of bias because significant claims must be supported by multiple sources of documentation, academic research, and independent security analyses.

## 3.3 Research Approach

This investigation takes a mainly deductive strategy where the author starts from known theoretical frameworks and applies them to empirical evidence (Saunders et al., 2019). The security-usability trade-off, socio-technical systems theory and access control theory supply well-developed conceptual foundations against which the architectural choices of Widevine, PlayReady and FairPlay are systematically measured. The aim is not to create new theory but to apply the existing theory constructs to a comparative technical analysis not before carried out in this way (Yin, 2018).

The research approach was initiated by an overview of DRM literature for theoretical constructs that describe protection mechanisms and security-usability trade-offs as well as architectural patterns. These constructs such as socio-technical systems theory (Ding, 2023), access control theory (Ma, 2017), encryption standards, key management protocols and devices authentication mechanisms provided analytical dimensions against which the three platforms were systematically compared.

In addition to this deductive framework, the research includes inductive elements where the empirical examination revealed technical details that were not anticipated by existing theoretical frameworks (Saunders et al., 2019). For example, the discovery of the Narrowbeer vulnerability against Widevine's timestamp validation (Roudot & Sabt, 2025) involved inductive reasoning in order to understand how this implementation flaw is related to the broader principles of temporal validation and impacts on the security-usability trade-off. The research method therefore takes what Saunders et al. (2019) describe as an abductive approach in which there is an iteration between theory-driven deductive analysis and empirically-driven inductive insight.

## 3.4 Research Design

Research design translates the research question into a planned investigation linking philosophical assumptions with practical data collection and analysis decisions (Yin,

2018). The following subsections outline the methodology choice, comparative case study structure, and time horizon.

### 3.4.1 Methodology choice

This study has adopted qualitative research methodology. Qualitative methodology was selected for this study for several reasons (Yilmaz, 2013). First, the research question is concerned with "how" architectural design decisions balance competing requirements, and thus interpretive analysis rather than statistical measurement is needed (Yin, 2018). Second, the phenomena under investigation are complex socio-technical systems and need to be understood in their context rather than variables need isolating them. Third, available data is mostly in the form of technical documentation, which are texts rather than numbers. Fourth, the aim of the research is to develop comprehensive comparative understanding rather than test predetermined hypothesis (Yilmaz, 2013).

### 3.4.2 Research strategy

This study takes the form of comparative case study where each of the DRM platforms is considered as a bounded case for systematic study (Yin, 2018). Case study methodology can be used for the study of complex technical systems in which the context of implementation has a significant influence on the results. Each platform is running in different technological ecosystems (Android/Chrome, Windows/Xbox, iOS/macOS) serving different market segments with unique security requirements and usability expectations (Rafi et al., 2023).

The comparative dimension offers the possibility of systematically to look for similarities and differences between platforms. The three platforms are based on different philosophies for their design: Widevine focuses on cross-platform portability with tiered security models, PlayReady focuses on enterprise flexibility with granular policy control and FairPlay focuses on in-depth ecosystem integration to maximise protection (Rafi et al., 2023). This architectural diversity enables to study the relative

influence of the design choice on the relative strength between the robustness of security and quality of user experience.

This research involves in comparative case study analysis with document analysis being the most important means of data collection (Bowen, 2009). Given the philosophy of post-positivism described in Section 3.2, and the abductive approach described in Section 3.3, the starting point for this strategy is theoretically informed criteria, which are applied across the three platforms, whilst allowing for the possibility that what comes out of the data may require these criteria to change. Widevine, PlayReady and FairPlay are all proprietary system and closed source, therefore there is no way to directly access their internal workings. The analysis is therefore based on a mix of vendor documentation, technical standards, published security research and independent assessments to construct the comparative evaluation.

### 3.4.3 Time Horizon

A cross-sectional time horizon is used in this study, where the focus would be on the actual situation of each platform, instead of focusing on longitudinal development (Saunders et al., 2019). This is suitable given the focus of the research question on the impact of current design decisions on the security-usability trade-off. DRM platforms are updated on a regular basis and implementation details may change post the period covered in this study.

## 3.5 Data Collection

Data collection was made exclusively from secondary sources, due to proprietary character of the commercial implementations of DRM, rendering the possibility of primary empirical research through source code analysis or controlled security testing

impossible. The research included synthesis of evidence from multiple categories of documents that provided perspectives on characteristics of DRM implementation that are relevant to understanding the security-usability trade-offs.

### 3.5.1 Data Type

The data is completely of qualitative secondary data in textual form (Bowen, 2009). This includes technical specifications, implementation guides, academic research publications, security vulnerability reports, industry analyses and technical blog posts. The textual nature fits then the methodology of qualitative research, which requires an interpretative analysis, not statistics.

### 3.5.2 Sampling technique

Document selection followed a purposive sampling method, a non-probability approach whereby researchers select sources most likely to yield rich and relevant information aligned with the research objectives (Ahmed, 2024; Bowen, 2009). This strategy is especially suitable for qualitative research dealing with specialised technical systems where the population of relevant sources is inherently limited.

In this study, the use of purposive sampling was undertaken in two levels. At the platform level, Widevine, PlayReady, and FairPlay were chosen because they have (collectively) the dominant share of commercial content protection in video streaming, and because each represents a fundamentally different philosophy of its architecture. Widevine's tiered security model, PlayReady's granular policy framework, and FairPlay's ecosystem-integrated approach are all quite different schemes of compromises between security and usability that, together, represent a purposive sample spanning the range of design strategies currently in use. At the document level, sources were chosen based on their ability to shed light on the ways in which the architectural decisions of each platform were made and what consequences those decisions have for security robustness and end-user experience. Technical documentation published by Google, Microsoft, and Apple formed the foundation of

the corpus because these are the main ways that each vendor expresses his or her own design rationale.

#### 3.5.2.2 Sample Size

Document collection process continued until theoretical saturation was reached, i.e., when additional sources supported existing findings rather than adding new information relevant to the analytical framework (Bowen, 2009; Saunders et al., 2019). The final corpus was 12 documents from four categories of source material. Three vendor specification documents and technical standards published by Google, Microsoft and Apple gave authoritative descriptions of the intended platform functionality. There were five peer-reviewed academic publications regarding security architectures and vulnerabilities of each platform. Two separate security research reports, including analyses produced using formal verification and penetration testing, provided an outside review of platform robustness. Two industry white papers focused on DRM implementation strategies and content protection practises for the streaming world. These categories were chosen in order to support the triangulation approach discussed in Section 3.2 so that the claims made about each platform were based on convergent evidence from multiple independent sources rather than vendor documentation alone (Yin, 2018).

The coverage was not distributed equally between the three platforms. Widevine got the highest number of material available because of the larger volume of academic and security research published about Google's system (Patat et al., 2022; Delaune et al., 2024; Roudot and Sabt, 2025). FairPlay had quite a few independent sources in which it can detect which is recognised as a limitation of this study (Rafi et al., 2023).

### 3.5.3 Source categories and Selection Criteria

Documentation - Primary sources were official technical specifications from Google, Microsoft and Apple and the descriptions of intended functionality and security models are authoritative.

Secondary sources included academic publications with peer review on theoretical frameworks and security vulnerabilities for example Ding, 2023; Ma, 2017; supplemented by industry white papers as well as technical assessments.

Rigorous source evaluation criteria were used to make inclusion decisions (Bowen, 2009): (1) Credibility: Peer-reviewed publications and official vendor documentation had top priority; (2) Currency: materials and resources dating from 2017-2025 were given top priority; (3) Relevance: materials directly relating to architectural decisions or security-usability trade-offs were selected; (4) Corroboration: significant claims were expected to be substantiated by multiple independent sources.

### 3.5.4 Search Strategy and Collection Procedures

Document identification was done according to systematic search procedures in Google Scholar, IEEE Xplore, ACM Digital Library, ScienceDirect and SpringerLink by using keyword combinations relating to DRM architecture, security-usability trade-offs and platform-specific implementations.

Seminal publications (Ma, 2017; Ding, 2023), further materials (Webster and Watson, 2002) complemented by official developer portals and the Common Vulnerabilities and Exposures database were identified.

Collection came to halt when theoretical saturation was reached, when new sources found to be not adding new architectural characteristics, but only confirming existing results (Bowen, 2009). This multi-source approach meant that triangulation, whereby claims made in vendor documentation have been either confirmed or disputed through independent security research (Yin, 2018) was possible.

## 3.6 Data Analysis

The analytical framework that was used was a thematic comparison organised by dimensions developed in the research question, research objectives and theoretical

frameworks. The focus of the analysis was to understand how architect design decisions create various trade offs between security robustness and user experience.

### 3.6.1 Development of Analytical Framework

Two theoretical viewpoints drove the development of frameworks. Socio-technical systems theory (Ding, 2023) sees DRM as a combination of technical mechanisms and organisational processes as well as user interaction. Access control theory (Ma, 2017) provides frameworks for understanding authentication, authorisation and policy enforcement. Together, these theories informed the development of four analytical dimensions looking at the technical implementations, as well as the socio-technical consequences.

Framework development started in the literature review where the dissection of existing DRM research identified recurring themes on the balance between protecting and usability in DRM protection mechanisms. Following the hybrid thematic analysis approach described by Fereday and Muir-Cochrane (2006), these themes were organised systematically in an analytical framework that comprises four main dimensions as follows:

**Dimension 1:** Architectural Design Decisions looks at the structural decisions that influence the security-usability trade-off such as: security model architecture, approach to ecosystem integration, and scalability strategies. This dimension addresses Research Objective 1 as it studies the effects of design choices on security robustness and user experience.

**Dimension 2:** Security Robustness Mechanisms analyses technical mechanisms providing content protection such as cryptographic implementations, authentication mechanisms and vulnerability profiles. This dimension supports Research Objective 2 because it addresses the issue of how the security mechanisms affect the robustness of the system, but may have impact on usability.

**Dimension 3:** User Experience Impact Factors looks at the impact that technical decisions have regarding user accessibility such as compatibility across devices, playback performance, authentication friction and content portability. There is a direct link to Research Objective 2 in this dimension.

**Dimension 4:** Implementation Strategies looks at practical implementation strategies between security and usability including multi-DRM implementation strategies, adaptive security strategies, and content tiering strategies. This dimension responds to Research Objective 3.

### 3.6.2 Coding and Comparison Procedures

The contents of the documents were analysed using systematic coding procedures based on the framework for thematic analysis presented by Braun and Clarke (2006) and further developed by Naeem et al. (2023). The coding progression was a two-cycle structure following the design by Saldana (2021), and progressed from initial open coding of the data to focused coding and the identification of themes followed by cross-platform comparisons.

**Phase 1:** Initial Familiarisation & open Coding. The first stage was reading through the document corpus in order to familiarise oneself with the content and recognise parts of text dealing with architectural decisions, security mechanisms, usability impacts or ways of implementation (Braun & Clarke, 2006). These segments were labelled based on descriptive codes including 'security_levels', 'device_support', 'compatibility_restrictions', 'vulnerability_impact', and 'adaptive_security'. Table 1 provides an illustrative example of how initial codes were generated from the source documents during this phase.

**Table 1**

*Illustrative Coding Example from Document Analysis*

| Source Document | Data Extract (Example) | Initial Code | Dimension |
|---|---|---|---|
| Patat et al. (2022) | Widevine L1 performs all cryptographic operations within TEE; L3 uses software-only implementation | security_levels | 1. Architectural Design |
| Roudot and Sabt (2025) | Narrowbeer attack exploited timestamp validation flaws to extend licence validity indefinitely | vulnerability_impact | 2. Security Robustness |
| Volckmann (2024) | FairPlay content inaccessible outside Apple ecosystem; restrictions exceed security requirements | compatibility_restrictions | 3. User Experience |
| ScoreDetect (2024) | Multi-DRM providers abstract complexity through unified interfaces supporting all three platforms | adaptive_security | 4. Implementation |

*Note. Representative examples from the initial open coding phase illustrating how document extracts were assigned codes mapped to the four analytical dimensions.*

**Phase 2:** Focused Coding. The first codes were then re-arranged into platform-specific categories, resulting in parallel coding structures for Widevine, PlayReady and FairPlay (Saldana, 2021). This stage produced comparison matrices where the rows were the analytical themes and the columns were the platforms allowing a like-for-like comparison between the three cases.

**Phase 3:** Thematic Analysis. Patterns were analysed across platform in each of the analytical dimensions (Braun & Clarke, 2006). For architectural design decisions, the comparison revealed the three-tier model of Widevine, which explicitly balances security depth with accessibility, the flexible policy framework of PlayReady which balances enterprise requirements for fair play with more complexity, and FairPlay which is a closed ecosystem which goes for maximum protection at the expense of portability. For security robustness, there were differences in hardware security utilisation and vulnerability patterns between three systems, the analysis found. For the sake of user experience, comparison emphasised the trade off between content quality and cross platform compatibility. For implementation strategies, the analysis

revealed how the various platforms optimise their trade-offs using implementation strategies such as multi-DRM deployment and adaptive security measures.

**Phase 4:** Evaluation of the Evidence Quality. Throughout the process of coding and comparing, the quality of evidence was continually determined following principles of document analysis (Bowen, 2009). Claims that were supported by only one source were considered tentative. Where contradictions arose between sources these were investigated rather than resolved by default. Findings independently confirmed by two or more sources of evidence were deemed high confidence evidence. The progression from the raw data to themes therefore involved a method of structured progression from initial familiarisation and open coding of the segments of the document, followed by focused coding (in which codes were organised into categories relevant to the specific platforms), and then thematic analysis (in which cross-platform patterns in each analytical dimension were found) (Braun and Clarke, 2006; Saldana, 2021). The resultant themes, which are presented in Chapter 4, arose directly from this systematic coding process, and are based on the documented evidence-base.

## 3.7 Ethical Considerations

This investigation followed established ethical principles for security research (Association for Computing Machinery, 2018). No original penetration testing or vulnerability discovery was conducted; the study relied solely on publicly available information. All referenced security vulnerabilities were disclosed through responsible channels by the original researchers (Roudot and Sabt, 2025). Ethical approval was obtained from the ICL Research Ethics Committee (ICLREC) before data collection commenced.

Comparative analysis to identify platform weaknesses could be of theoretical help to malicious actors. This was balanced against security through obscurity which provides illusory protection, and strong architectures require transparency and

independent scrutiny (Schneier, 2000). The study emphasises an architectural analysis as opposed to circumvention instructions.

To help ensure the objectivity of research, analysis was conducted using only documented evidence from independent sources, comparison frameworks used identical evaluation criteria for comparison within a platform, and results were reported without advocacy for a specific platform adoption. Data handling was straightforward, relying solely on publicly accessible secondary data, which raises no privacy concerns regarding individuals or organisations (British Computer Society, 2022)

# Chapter 4: Findings and Discussion

## 4.1 Introduction

This chapter reports the results of the comparative analysis of Google Widevine, Microsoft PlayReady, and Apple FairPlay, which answers the research question of how architectural design choices in major DRM systems trade off security robustness with user experience. The analysis is based on the above-described four-dimensional analytical framework built in Section 3.6.1, which is conducted using systematic thematic analysis of vendor documentation, academic research, as well as independent security assessments.

The analysis is based on the corpus of documents outlined in Chapter 3, coded segments of which are organised by focused coding into platform-specific comparison matrices in terms of the four analytical dimensions. The findings are a product of systematic coding and cross-case comparisons and the findings from individual studies are referenced as supporting evidence, but not as the major forces in the analysis.

The analytical framework has four major dimensions, which directly address research objectives set in Chapter 1. Dimension 1, Architectural design decisions (Section 4.2) relates to Research Objective 1 by analysing and comparing structural components of each platform to determine specific design features that affect platform security strength and user experience. Dimension 2, Security robustness mechanisms (Section 4.3) and Dimension 3, User experience impact factors (Section 4.4) collectively serve to address Research Objective 2, i.e. the effect of security requirements on user experience in different deployment scenarios. Dimension 4, Implementation strategies (Section 4.5), relates to Research Objective 3, as well as identifying strategies that

large streaming platforms use to effectively balance the needs of security and user experience. Section 4.6 synthesises the findings from all four dimensions and comes back to the research gap and theoretical and practical implications.

## 4.2 Architecture Design Choices

This section reports results based on Dimension 1 of the analytical framework, which seeks to answer the following Research Objective: To examine and compare the architectural components of Widevine, PlayReady, and FairPlay to identify specific design features that affect security strength and user experience. Repeated coding of architectural-decision references on 9 documents within the corpus revealed three different strategic patterns representing three distinct philosophies on the security-usability balance allocation. The analysis occurs in two parts. Section 4.2.1 compares these divergent strategic approaches using integrated cross-case comparison, and Section 4.2.2 considers the consequence, at the industry level, of the incompatibility of architectures, that is the convergence on multi-DRM deployment.

### 4.2.1 Differing Strategic Models of the Security-Usability Trade-off

Thematic analysis of the corpus of documents showed three clear trade-off allocation strategies, which in this study are characterised as a market-segmentation strategy (Widevine), a complexity-transfer strategy (PlayReady), and an environmental-control strategy (FairPlay). Rather than being representative of purely technical optimisations, these patterns seem to represent conscious decisions regarding value allocation based on the priorities of each vendor's commercial interests and philosophy of their respective ecosystem. The following paragraphs examine the impact of these strategies by means of integrated cross-case analysis that draws out the contrasts within the common thematic dimensions.

**Security-tier architecture and device reach.** The most pronounced architectural contrast between the three platforms is that of security level as compared to the device

accessibility. Widevine utilises a multi-tiered architecture and offers three levels of security: Level 1 (L1) is where all content processing is performed in hardware-based Trusted Execution Environments, Level 2 (L2) limits the use of cryptographic operations to the TEE, and Level 3 (L3) uses software-based security altogether (Patat et al., 2022; Roudot & Sabt, 2025). This segmentation results in 3 parallel implementations at different points on the trade-off spectrum. By contrast, FairPlay requires the HLS protocol, and AES-128 CBC encryption with per-frame unique initialisation vectors for all implementations, and effectively refuses to support use-cases which would call for compromised security (Delaune et al., 2024). Every FairPlay implementation is functionally equivalent to Widevine L1, but this is accomplished using the exclusivity of the platform rather than the ubiquity of the hardware. PlayReady is an intermediate solution, it offers granular policy controls allowing content providers to set their own security requirements, such as key rotation, output protection requirements and domain-based licensing (Pellegrini, 2024). The platform serves as a flexible architecture instead of a hard DRM implementation and it requires content providers to set up content encryption, user authentication, and key management themselves.

**Trade-off cost allocation.** A key finding of this comparative analysis is that the three platforms distribute the costs of the security-usability trade-off among different stakeholders. Widevine scatters the burden of costs on users: users with L1-certified devices get 4K Ultra-HD and HDR content while L3-only devices only get standard definition content, even though users may be paying the same subscription fees (Patat et al., 2022). Deployment data show that L1 hardware protection only reaches about 40 per cent of Android devices, meaning that the majority of users suffer from a degraded experience as a trade off for the wide market reach (Roudot & Sabt, 2025). PlayReady shifts the responsibility to the content providers, who need to have the adequate knowledge to configure the policy frameworks securely, the flexibility of the platform creates the space for unintended vulnerabilities through configuration complexity (Pellegrini, 2024). FairPlay focuses costs on users who need

cross-platform access because content purchased or licenced through FairPlay protected services cannot be used outside of Apple's ecosystem (Volckmann, 2024). The restrictions have been argued to go far beyond what content protection alone requires to meet Apple's commercial agenda as much as legitimate security aims.

**Security implications of architecture decisions.** The security implications of these divergent strategies are quite different. Across 15 coded segments relating to vulnerability evidence, Widevine presented the widest attack surface that is documented. The L3 root of trust was recovered (CVE-2021-0639) by means of unprotected OEMCrypto interface functions monitoring, making it possible to obtain the 128-bit AES Device Key (Patat et al., 2022). More recently, the desktop Widevine CDM was found to be vulnerable to practical replay attacks which allow for never expiring licences which can be replayed across devices (Roudot & Sabt, 2025). Schmidt (2024) adds to this context of these vulnerabilities, pointing out that there are hardware support mechanisms such as Trusted Execution Environments which can lower the amount of system lock-down necessary for DRM protection, but that authentication of Content Decryption Modules against licence servers remains an unanswered challenge on open platforms. PlayReady's known weaknesses are less but include client-identity compromise due to implementation decisions rather than protocol weaknesses (Roudot & Sabt, 2025). FairPlay has the most opaque profile with essentially no public vulnerabilities being published in the academic or security research literature, although this may be due to Apple's closed ecosystem and legal posture rather than good security.

**Cross-case synthesis.** The comparison evidence seems to point to the three platforms representing fundamentally different answers to the question of who should bear the costs of balancing security with usability. This pattern casts doubt on the assumption, which is found in some of the DRM literature, that trade-offs can be optimised through improved technical design alone. Within the limits of the available evidence, the data suggest that such trade-offs represent strategic decisions regarding the

allocation of value based on commercial priorities, ecosystem philosophy and target markets. The important dimensions of this comparison are summarised in Table 2.

**Table 2**
*Comparative Summary of Trade-off Allocation Across DRM Platforms*

| Dimension | Widevine | PlayReady | FairPlay |
|---|---|---|---|
| Strategy | Market segmentation through tiered security levels | Complexity transfer through configurable policy controls | Environmental control through ecosystem exclusivity |
| Trade-off cost bearer | Users (unequal experiences by device capability) | Content providers (configuration expertise required) | Users requiring cross-platform access (ecosystem lock-in) |
| Key security evidence | L3 RoT recovery (CVE-2021-0639); Narrowbeer replay attack on desktop CDM | Client identity compromise from implementation choices | No CVE records; limited publicly documented weaknesses |
| Primary usability limitation | Reduced quality on lower-tier devices despite equal subscription cost | Risk of misconfiguration without adequate vendor guidance | No cross-platform access; complete ecosystem dependency |

*Note.* Put together by the author of this paper based on thematic analysis from Patat et al (2022), Roudot and Sabt (2025), Pellegrini (2024), Volckmann (2024), and Schmidt (2024).

For researchers and practitioners interested in understanding what implementation strategies are optimal to the security-usability balance, the results of this research indicate that there is no one strategy that is best for everyone. The best way to do this seems to depend on the particular situation, including the diversity of the target device population, the technical capability of the content providers, and the extent to which the cross-platform access is commercially important.

### 4.2.2 Multi-DRM as Forced Industry Convergence

A critical observation that emerges from reviewing the patterns of deployment over the corpus is that incompatibilities in architecture have pushed the streaming industry towards a standardised solution, that is, the deployment of all three DRM systems in

parallel. Analysis of the deployment documentation of major streaming platforms shows tremendous consistency. Netflix, Disney+, Amazon Prime video and pretty much every other major content provider use FairPlay for Apple devices, Widevine for Android and Chrome and PlayReady for Windows systems (ScoreDetect, 2024). Kumar et al (2024) notes that cloud-based video streaming services use DRM as an integral part of the content delivery pipeline, where the cloud platform architecture requires the packagers for both live and video-on-demand content to use DRM encryption to generate platform-specific manifests for distribution through content delivery networks. This convergence, with all the huge complexity involved, indicates that single-platform trade-offs become unacceptable for services with a need for wide market penetration.

Multi-DRM deployment adds a significant amount of operational overhead, such as a separate encryption workflow for every platform, multiple implementations of a licence server, detection logic for devices, and expertise in three different architectures (ScoreDetect, 2024). However, third-party multi-DRM service providers such as Axinom, Intertrust ExpressPlay and Verimatrix have appeared to abstract this complexity in unified interfaces. The commercial viability of these intermediaries can offer us a clue: platform fragmentation has generated a secondary market for the management of complexity.

The data suggest that DRM fragmentation remains a long-term characteristic of the ecosystem and not a problem that is in the transition phase. Existing interoperability standards such as CPIX for key exchange have yet to be implemented by any of the three major DRM systems, which would seem to indicate that technical solutions for reducing fragmentation are available but are not implemented (Rafi et al., 2023). This raises questions as to whether platform vendors have the right incentive to pursue interoperability. For the research question, this finding has implications that the security-usability trade-off is further compounded by deployment complexity, because content providers must deal with parallel systems with different security properties, configurations and vulnerability profiles.

Overall, the under Dimension 1 analysis indicates that the three DRM platforms correspond to basically different philosophies in the architecture in which none of them can be said to have an universally optimal security/usability balance. The resulting ecosystem fragmentation is pushing the content providers towards multi-DRM deployment, which adds complexity to the operation. This finding directly relates to Research Objective 1, and helps to put the security and usability dimensions explored in the following sections in their proper architectural context.

## 4.3 Security Robustness Mechanisms

This section reports findings according to Dimension 2 of the analytical framework dealing with the security aspect of Research Objective 2. Rather than taking the words of vendors about security at face value, documented vulnerabilities are critically analyzed in order to determine actual protection effectiveness versus theoretical capabilities. Across 15 coded segments relating to vulnerability evidence, the analysis identifies patterns that shed light on fundamental differences of the architecture of different platforms in shaping the real-world outcomes of security.

### 4.3.1 Vulnerability Patterns and Architectural Weaknesses

**Comparative vulnerability evidence.** The most striking thing throughout the three cases is the terribly uneven distribution of the vulnerabilities that have been publicly documented. The MITRE CVE database contains 53 records for Widevine and PlayReady between 2014, while the FairPlay code has not received any CVE records (Rafi et al. 2023). However, this difference does not directly reflect relative security strength. DRM security research was essentially barred in many jurisdictions until the Federal Bureau of Investigation (FBI) exemptions, known as the DMCA, were broadened in 2018, which allows only limited independent scrutiny for all platforms (Roudot and Sabt. 2025). Drawing direct security comparisons on the basis of publicly documented vulnerabilities is therefore methodologically limited and the findings presented here should be interpreted with this constraint in mind.

Widevine has the widest documented vulnerability profile amongst the three platforms. The vulnerability named Narrowbeer continued to exist throughout Widevine version history from 2018 to mid-2024 and was present in billions of devices worldwide (Roudot & Sabt, 2025). Critically, this impacted all security levels including L1, this demonstrated that hardware based cryptographic protection in no way provides any defence against protocol-level logical flaws. Formal security analysis performed using the TAMARIN prover, however, revealed a further vulnerability allowing attackers to load arbitrary consumption policies for any licence that could be renewed at least once, by taking advantage of incomplete memory-commit behaviour in the two phase licence loading process (Delaune et al., 2024). Schmidt (2024) concurs with this general result, stating that even in places where Content Decryption Modules run within Trusted Execution Environments it has been an unresolved issue to authenticate these modules against licence servers because private keys embedded in CDM binaries can be recovered using reverse engineering.

PlayReady comes with a strikingly different profile characterised by low public documentation. A compromise of client identity is the most serious documented publicly released vulnerability, but no complete technical details are available (Roudot & Sabt, 2025). This opacity makes it hard to compare, because the analysis cannot conclude whether or not PlayReady really offers stronger protection, or is simply not as heavily targeted by public security research. FairPlay has the most closed security profile of all three platforms and there are literally no documented vulnerabilities in academic and security research literature. This non-existence seems to be a reflection of Apple's closed ecosystem approach, legal stances towards security research, and architectural integration that makes analysis from outside forces hard (Volckmann, 2024). From a comparative point of view, the security effectiveness of FairPlay still cannot be largely verified through independent research.

**Organisational factors shaping security outcomes.** Equally illuminating is the way in which organisational responses to vulnerability disclosure affect longer-term protection. After responsible disclosure of the Narrowbeer vulnerability, Google refused to include researchers in the patch development process, gave no remediation timeline, and released fixes without notifying researchers who had reported the vulnerability (Roudot & Sabt, 2025). The first patch addressed the issue of licence replay but did not address the problem of temporal validation weakness completely. This response pattern implies that the effects of organisational factors, such as communication practises and procedures for handling vulnerabilities, on security outcomes are as great as the effects of technical architecture choices, confirming the socio-technical systems approach taken in this research (Ding, 2023).

The vulnerability analysis hence describes a paradox. The most researched platform (Widevine) looks least secure in terms of documented weaknesses but this transparency may in the end actually make it more secure by enabling identification and remediation of any flaws. The least researched platforms might have undiscovered weaknesses. This finding implies that organisational rather than technical factor, vulnerability disclosure culture is an important factor in the security-usability balance.

### 4.3.2 Cryptographic Implementation and Divergent Effectiveness

All three platforms use AES-128 or AES-256 encryption, but the level of their practical security is very different. This uniformity in cryptographic standards along with divergence in protection effectiveness is a significant finding. In all 8 coded segments connected to the issue of cryptographic implementation, it's the architecture of key management and the context of implementation that determine the security in real-world use to a much larger extent than the choice of algorithm.

Widevine L3 goes further by being implemented in software, which was found to be vulnerable to key extraction despite being based on the same AES encryption as

hardware-backed L1 implementations; successful circumvention via differential fault analysis required relatively small effort with publicly available tools (Coates & Abroshan, 2024). Patat et al. (2022) went on to show that the L3 keybox could be retrieved without defeating the underlying obfuscation, by simply monitoring memory areas while executing the protocol. Schmidt (2024) puts this into the context of the wider hardware support context, noting that Intel SGX enclaves encrypt memory transparently, while ARM TrustZone uses physical memory separation, and also that both methods are subject to their own side channel vulnerabilities. Kumar et al. (2024) state that cloud-based video streaming architectures increasingly rely on hardware-backed Trusted Execution Environments for secure key storage, but even these are not free of attack vectors through side-channel attack analysis of power consumption, electromagnetic emissions, or timing variations. This makes the question of security how robust is the encryption rather than how robust is the whole key management system to extraction attack.

PlayReady's policy-based approach enables content providers to set certain cryptographic requirements using policy configurations (Pellegrini, 2024). This flexibility in theory enables for the optimal customisation and tailoring of protection requirements based on a specific value of content and threat assessment. However, the analysis of the patterns of deployment shows low levels of practical exploitation of these capabilities. Most streaming services appear to have broadly equivalent policies, for PlayReady and Widevine, than the granular controls available in PlayReady. This finding suggests that the theoretical value of policy flexibility may be greater than the practical utility of policy flexibility where practises of industry converge around common tiers of security.

FairPlay's mandatory hardware-based cryptography eliminates the software/hardware decision completely, and enables homogenous cryptographic protection across implementations. This uniformity is useful to a content provider who wants to have consistent security characteristics but doesn't give the flexibility to make strategic security exchanges with the user available on other platforms.

In conclusion, the cryptographic analysis under Dimension 2 (Security Robustness Mechanisms) reveals that security-usability trade-off is not so determined by the choice of the cryptographic algorithm, but is dependent on the implementation architecture around it. Hardware isolation, design quality of protocols and organisational processes for vulnerability response are together determinative of protection effectiveness in the real world. This finding has direct implications for Research Objective 2 which aimed to find out the impact of security requirements on the user experience across different deployment scenarios as it suggests that security robustness cannot be considered independently of the broader socio-technical context of its operation.

## 4.4 User Experience Impact Factors

This section reports findings under Dimension 3 of the analytical framework, the user experience component of Research Objective 2. Across 9 coded segments relating to user experience consequences, the analysis explores how architectural decisions and security mechanisms are turned into concrete user experiences that reveal that technical security requirements produce user-facing consequences far beyond the quality of the playback itself.

### 4.4.1 Quality Disparity, Authentication Friction, and Cross-Platform Comparison

The most important user experience impact identified in the comparative analysis is related to the relationship between device security capabilities and content quality access. Users with Widevine L1 certified devices have access to 4K Ultra-HD and HDR content, while L3 only users have access to standard definition (Patat et al., 2022). Premium providers limit video quality for all users of Widevine on the desktop to sub HD (Roudot & Sabt, 2025). By contrast, the mandatory hardware security offered by FairPlay removes quality disparity altogether; all modern Apple devices are guaranteed the same maximum quality depending on the display capabilities,

rather than security certification. However, the same consistency of the quality from FairPlay is offset by the lack of access on other platforms, introducing a different kind of user experience restriction. PlayReady is a middle ground, and its domain-based licencing model is theoretically suited for shared access over multiple devices, but the analysis shows that domain features are not adopted in consumer streaming scenarios to a great degree, presumably because of their implementation complexity.

The comparative finding is that none of the three approaches to authentication and quality management is universally found to be superior; each optimises for different usage patterns whilst creating friction for others. Single-ecosystem users benefit from the consistency brought by FairPlay while users needing cross-platform access suffer from the exclusivity it brings. Widevine's per-device model accommodates individual users with consistent device sets but causes hassles for families sharing devices. This in turn reinforces the general finding under Dimension 1 that the trade-off is context-dependent rather than technically resolvable.

### 4.4.2 Content Portability and Ecosystem Lock-in

Perhaps the most significant consequence to user experience identified in the analysis has to do with portability of content. Widevine allows for a significant amount of portability in the Android and Chrome worlds but does not offer a way to Apple platforms (Patat et al., 2022). FairPlay produces the opposite scenario: it offers perfect portability within Apple's ecosystem (thanks to iCloud integration), but 100% inaccessibility outside Apple platforms (Volckmann, 2024). Content purchased via Apple services is limited to Apple devices and has no legitimate process for playback on other devices. Schmidt (2024) contextualises this finding into a wider critique; arguing that DRM protection compromises the longevity of content availability, as content locked to proprietary licence servers is no longer available when companies drop services, or platforms, and change regional licensing agreements. The technical barriers to FairPlay interoperability seem like architectural choices rather than the inevitable security requirements.

The findings of this study suggest that the platform fragmentation forces users to make ecosystem allegiance decisions with long-term consequences that fundamentally change the nature of digital content ownership. Effectively, content purchases are investments in specific ecosystems rather than something that is actually owned media. This is a departure from physical media ownership in which purchased DVDs or Blu-ray discs continued to be accessible no matter which playback device manufacturer is used. The analysis under Dimension 3 shows that the user experience costs of DRM go far beyond limitations in the quality of playback to include basic questions of whether and how digital content is owned, and for which platform the owner is loyal - this analysis directly relates back to Research Objective 2.

## 4.5 Implementation Strategies That Optimise Trade-offs

This section provides the results under Dimension 4 of the analytical framework, in response to Research Objective 3: to identify approaches adopted by major streaming platforms that support a desired balance between security requirements and user experience. The analysis is a synthesis of patterns seen across the above three dimensions, and identifies emergent industry practices that can be seen as collective learning about optimal deployment strategies.

### 4.5.1 Multi-DRM and Adaptive Security Strategies

The overwhelming dominance of multi-DRM deployment is the industry's tacit judgment on single platform approaches. By implementing FairPlay, Widevine and PlayReady in parallel, content providers get the best of each system and reduce the weaknesses (ScoreDetect, 2024). Multi-DRM is an effective way to turn the security-usability trade-off from a situation of either-or into a situation of choosing appropriately and contextually. This architecture is described by Kumar et al. in this analysis of cloud-based video platforms, in which live and video-on-demand content flows through separate pipelines for transcoding, packaging, and DRM-encryption before being delivered to the content delivery networks and streaming clients. The

cloud platform architecture they describe is an example of how multi-DRM works in practice - with different packagers using platform-specific encryption to encrypt segments of content before it's distributed.

A second important finding is that leading platforms increasingly implement adaptive security strategies with different requirements of protection depending on content characteristics, temporal aspects, and risk assessment. Deployment documentation identifies new theatrical films as being granted mandatory L1 hardware protection, limited offline access and enhanced forensic watermarking, whilst catalogue content takes L3 for broadly maximum accessibility (Patat et al, 2022). Temporal protection windows grant maximum levels of security during the early stages of release when the risk of piracy is at its highest, which increasingly eases as the content ages and business value declines (Pellegrini, 2024). This temporal approach recognizes that the protection requirements change over time as commercial value changes, thus proving that the security-usability trade-off is not static but varies for different content lifecycles.

Forensic watermarking integration is a radical change in protection philosophy from prevention to detection and deterrence. Leading services such as Netflix, Disney+, and Amazon Prime Video is implementing proprietary watermarking systems that embed invisible identifiers that can be used to trace the piracy back to its origin (Hassan et al., 2020). The strategic significance here is that watermarking provides content providers a way to relieve themselves of some of the cryptographic requirements to protect, but still ensure that the fighting of piracy is accomplished by the accountability mechanism. The popularity of forensic watermarking suggests industry acceptance that cryptographic protection is insufficient to prohibit sophisticated piracy and is pragmatic acceptance of the limitations of DRM combined with complementary methods.

### 4.5.2 User-Centric Optimisation Approaches

Beyond technical protection strategies, the analysis identified patterns of user-centric optimisation in the deployment documentation. Approaches to communicating device capability and quality limitations are instructive examples of reducing friction by transparency where device certification status is prominently displayed and limitations of quality are explained in accessible language (Patat et al., 2022). This openness makes invisible constraints become manageable user choices, and is a representation of optimisation by information rather than technical modification.

Graceful degradation, reveals the principle that graduated responses that are commensurate with available security capabilities are more user-friendly whilst preserving acceptable protection levels. Widevine's tiered model, if done well, is a perfect example of this: when L1 certification is found to be unavailable, services are degraded to L3 with lower quality, rather than denying access altogether (Patat et al., 2022). Authentication optimisation thus seems to work best through integration with the platform rather than through proprietary methods; Fairplay's integration with iCloud, and Widevine's Google account authentication, both exploit existing platform credentials and alleviate the burden of password fatigue while retaining robust identity verification. This shows that security and usability can be strengthened at the same time through intelligent implementation which uses existing user relationships.

Overall, the analysis under Dimension 4 shows that the best implementation strategies do not attempt to make the security-usability trade-off through a single architecture choice. Instead they combine different platforms, tailor protection needs to content context and combine technologies with complementary functions, such as watermarking, and invest in transparent user communication. These strategies represent emerging industry practises that address limitations that are overcome by no single platform, directly addressing Research Objective 3.

## 4.6 Discussion and Synthesis

This section brings together findings from the four analytical dimensions to answer the research questions and objectives. Rather than restate the previous findings, the discussion emphasises on return to research gap and emphasise the contribution of this study as well as give higher level conceptual insight of theoretical and practical implication.

### 4.6.1 Answering the Research Question and Theoretical Implications

The research question was how architecture design decisions in major DRM systems make the tradeoff between security robustness and user experience, and what strategies are best when they are implemented. The comparative analysis reveals that this balance is achieved through fundamentally different strategies reflecting divergent philosophical positions as to who is to bear costs of trade offs, and what requirements are to be given priority.

The central contribution of this study is the empirical demonstration that the security-usability trade-off in DRM systems is not a technical problem admitting one optimal solution, but a strategic design-space in which different configurations privilege different stakeholders. Widevine is balanced by segmenting the market, PlayReady by flexibility of policies, and FairPlay by controlling the environment. This finding complements the cross-platform comparison given by Rafi et al. (2023), who presented a feature-level security comparison of the three systems without considering the impact of these architectural choices on the end user, and without analyzing how these choices are indicative of larger strategies for value allocation. Where Rafi et al. have catalogued the presence or absence of particular security features, the present study adds analytical depth to the issue by situating these security features in their strategic and socio-technical context.

The implementation strategies that are most effective in optimising trade-offs integrate multiple platforms through multi-DRM deployment, provide adaptive

security, with varying levels of protection depending on content value and temporal factors, and provide forensic watermarking, and emphasise transparent communication with reduced user friction. These strategies are emergent industry practices to overcome limitations that no one platform overcomes on their own.

The findings offer empirical evidence for conceptualising DRM as socio-technical systems in which technical mechanisms, organisational processes and user behaviours interact to produce emergent outcomes, extending Ding's (2023) theoretical framework through systematic empirical analysis. The Narrowbeer vulnerability illustrates these kinds of socio-technical dynamics: although the vulnerability was a result of a technical implementation flaw, the vulnerability's persistence and impact spoke to organisational factors such as Google's process for responding to vulnerabilities and how it communicates with those who find them (Roudot & Sabt, 2025). Similarly, the formal analysis by Delaune et al. (2024) showed that protocol-level design assumptions resulted in exploitable design gaps when organisational modularity was used to split the process across two API calls.

The findings also argue against simplistic characterisations of the security-usability trade-off in terms of binary opposition. The analysis highlights a complex multi-dimensional design space in which security robustness is made up of such factors as cryptographic strength, quality of protocol design, hardware versus software implementation and organisational response processes, while user experience is made up of factors such as device compatibility, content quality, authentication friction and cross-platform accessibility. Furthermore, examples such as biometric authentication and platform-integrated sign on prove that security and usability are two aspects that can get stronger together through good design, and the trade-off represents design limitations and choices rather than fundamental opposition between irreconcilable requirements.

### 4.6.2 Practical Implications and Research Limitations

For content providers considering DRM platforms, the analysis suggests selecting based on particular deployment situations, content properties and business models as opposed to finding universally optimal solutions. Services that focus on wide device reach may prefer Widevine even though of L3 vulnerabilities; enterprises that need complex policy control may prefer PlayReady even though implementation complexity; and Apple-exclusive services can offer optimal protection via FairPlay. For consumer streaming service that need to have a broad market reach, multi-DRM is, in spite of complexity and cost, the most efficient deployments strategy.

Content providers should consider adopting adaptive security approaches instead of uniform security protection policies. Content-value-based tiering allows for concentrating the expensive protection mechanisms where they provide the greatest value. Forensic watermarking can be used to complement cryptographic protection and provide detection capabilities that allow for accepting more accessible DRM configurations. Services should invest in transparent communication with respect to device capabilities and limitations in quality, as there is a body of evidence that communication framing may have a significant impact on the user perception of service quality, independent of technical characteristics.

For developers of DRM platforms, the results point in a number of directions. Widevine would benefit from improved L3 protection systems or faster L1 adoption via device manufacturer partnerships. The Narrowbeer attack shows the limitations of software-only CDM implementations and raises the question that hardware-backed CDMs, like ARM TrustZone backed ones on new desktop hardware, are the most realistic mitigation effort in the long run (Roudot & Sabt, 2025). Schmidt (2024) corroborates this assessment arguing for the usage of Trusted Execution Environments to reduce the required system lock-down for DRM protection whilst acknowledging that output protection via HDCP is broken due to the master key's leakage. PlayReady's policy flexibility means that there are better documentation and

developer tools needed to mitigate the risks of misconfiguration.

Several limitations or constraints make the generalisability of the findings. The analysis is based on publicly available documentation, which might not reflect an up to date implementation specifics for fast evolving commercial systems. Security vulnerabilities probably exist in addition to those publicly documented, especially for PlayReady and FairPlay as the research scrutiny is quite low for those. The results are a snapshot in time; further work on the platform can be done to deal with problems shown. The research concentrates on 3 dominant Western platforms with the exclusion of alternative DRM systems and emerging approaches. Enterprise deployments and regulated industries may have unique trade-offs not addressed in full in the consumer streaming platform analysis.

## 4.7 Chapter Summary

This chapter has provided the main conclusions of the systematic comparative analysis of Widevine, PlayReady, and FairPlay for the four analytical dimensions. 12 documents resulting in 46 coded segments organised into platform-specific comparison matrices, and all three research objectives were covered, while the main research question was answered.

Under Dimension 1, it was found that the three platforms embody fundamentally different strategic approaches to the security-usability balance as characterised by market segmentation (Widevine), complexity transfer (PlayReady), and environmental control (FairPlay). Under Dimension 2, the analysis of vulnerability has shown that organisational factors, specifically transparency in security research, might be more important for long-term protection than any specific technical mechanism. Under Dimension 3, the analysis of user experience showed that the costs of DRM go beyond limitations on quality to include fundamental questions of digital ownership and platform allegiance. Under Dimension 4, the most effective implementation strategies were found to be a combination of multiple platforms,

adaptation to the content context of protection, integration of complementary technologies, and investment in transparent user communication.

No platform has the optimum balance in all circumstances. The results support the use of socio-technical systems theory in DRM, and offer empirical comparative evidence for identified gaps in DRM literature, which can offer insight into the theory and practical guidance for platform choices and content protection strategies. These findings form the basis for Chapter 5's conclusions which draw together insights into recommendations for action and directions for future research.

# Chapter 5: Conclusion

## 5.1 Overview

This concluding chapter summarises the main conclusions of this work, which focused on understanding the trade-off between security robustness and user experience in the architectural design decisions taken in Google Widevine, Microsoft PlayReady and Apple FairPlay applications and implementations, and what is the optimal implementation strategy. Drawing on the qualitative comparative case study approach presented in Chapter 3, the research relied on a purposively sampled corpus of vendor specifications, peer-reviewed security publications, independent technical assessments and industry white papers and produced coded segments across four analytical dimensions. The main conclusions are presented in this chapter, research implications are discussed, limitations are acknowledged, recommendations for practise are made and directions for future research are suggested.

## 5.2 Conclusions

First, the security-usability trade-off in DRM is first and foremost a strategic design choice and not a technical problem that admits one optimal solution. Widevine, PlayReady, and FairPlay represent distinct philosophies as to who should shoulder the burden of protecting content (in case of a leakage scenario): Widevine's tiered architecture spreads the costs between users in the form of device-dependent quality restrictions; PlayReady's configurable policy framework shifts the costs to content providers who must have the expertise to configure it in a secure manner; and FairPlay's closed-ecosystem approach concentrates the costs on users who require cross-platform access. This finding, which is at the heart of Research Objective 1, challenges the assumption that tension between security and usability can be solved by better engineering alone.

Second, the context of implementation turns out to be far more important than the strength of cryptography in deciding the relative effectiveness of security in the real

world. All three platforms use AES-128 or AES-256 encryption, but the protection results in practise are significantly different. Key management architecture, quality of protocol design, hardware isolation and organisational vulnerability response processes are collectively responsible for actual robustness to a much greater extent than the choice of algorithm (Coates & Abroshan, 2024; Roudot & Sabt, 2025).

Third, vulnerability disclosure culture, which is an organisational rather than technical factor, may be more important for long term security than any individual protection mechanism. Widevine's openness to outside scrutiny is an advantage in the identification and correction of flaws, while FairPlay's obscurity may only mask weaknesses not yet tested by others.

Fourth, the costs to users of DRM go far beyond simply restrictions on the quality of playback to include issues of digital ownership and platform loyalty. Architectural fragmentation forces users to make ecosystem commitment decisions with long-term consequences to effectively convert content purchases into investments in a particular vendor's ecosystem (Volckmann, 2024).

Fifth, and addressing Research Objective 3, multi-DRM deployment and, with it, adaptive security is the most effective optimisation strategy currently available. The best implementations combine multi-DRM implementation with tiering content based on value, temporal protection windows, forensic watermarking, and transparent communication about the quality limitations of a device.

## 5.3 Research Implications

### 5.3.1 Theoretical Implications

This study has three main theoretical contributions. First, it expands a socio-technical systems theory (Ding, 2023) with empirical comparative evidence that the security outcomes of DRM are not based on technical architecture but rather on the interaction between design decisions, organisational behaviour and ecosystem philosophy. The Narrowbeer vulnerability case is a confirmation that socio-technical theory provides a

more comprehensive explanatory lens on content protection than do purely technical frameworks. Second, the research challenges the current binary conceptualisation of the security-usability trade-off by showing that it is a multi-dimensional design space in which security and usability under certain conditions can be strengthened at the same time through well-thought, designed decisions such as biometric authentication and platform-integrated sign-on. Third, the findings add to access control theory (Ma, 2017) by demonstrating that the three platforms reflect fundamentally different value-allocation strategies - market segmentation (Widevine), complexity transfer (PlayReady), and environmental control (FairPlay). This typology provides a new theoretical vocabulary for classifying DRM architectures according to the location of trade-off costs among stakeholders.

### 5.3.2 Practical Implications and Recommendations

The findings have direct implications for the modern practise of business for three stakeholder groups. For content providers, the study shows that the choice to use a particular DRM platform should be addressed as a strategic business decision with ramifications for customer retention, operational cost and competitive positioning rather than merely as a technical implementation detail to be relegated to the engineering teams. Three specific recommendations suggest themselves. First, many view multi-DRM deployment as an afterthought rather than a built-in architectural standard, given that the fragmentation of platforms is structural (Kumar et al., 2024) and interoperability standards like CPIX are unadopted (Rafi et al., 2023). For smaller providers who do not have dedicated DRM engineering teams, third-party multi-DRM service providers such as Axinom and Intertrust ExpressPlay provide a viable way to cope with this complexity. Second, providers can move towards adaptive, content-value security tiering, focusing L1 hardware protection and forensic watermarking (Hassan et al., 2020) on high-value new releases while allowing for greater L3 access to catalogue titles, complemented by time windows when restrictions are eased as commercial value falls (Pellegrini, 2024). Third, investment in transparent communications about device-dependent quality limitations represents

a low-cost way of enhancing user satisfaction, since the evidence suggests that perceived legitimacy of restrictions matters apart from the technical severity of the limitations.

For the developers of DRM platforms, the analysis holds two priorities. Given the demonstrated exploitability of L3 that allows hacking of the majority of Androids that do not have L1 certification, Widevine should either more aggressively strengthen its software-only CDM taking the protections, or promote more aggressive adoption of hardware backed CDM via partnerships with manufacturers. All three vendors need to progress towards more openness in vulnerability disclosure because the current model of not including researchers in the remediation processes ultimately undermines security at ecosystem-wide scale. PlayReady in particular needs improved supporting infrastructure, such as reference implementations and policy validation tools, to ensure that its configurable flexibility does not create a source of risk for misconfiguration. For industry standards bodies, it could be material to encourage (or mandate) common formats for key exchange (e.g. CPIX) to materially reduce the costs of fragmentation, reduce entry barriers for smaller organisations, and reduce the attack surface that parallel DRM deployments create (Rafi et al., 2023).

## 5.4 Limitations

In addition to the limitations discussed above at the data level (Section 4.6.2), such as the proprietary character of all three systems, the unevenly distributed vulnerability evidence base, and the temporal sensitivity of findings, there are also inherent limitations associated with the methodology itself that bear on the interpretation of the above conclusions. As a qualitative research based on document analysis of secondary sources, the research has not been able to access primary data such as source code, controlled security testing, or direct evaluation of user experience. The purposive sampling method, while suitable for specialised technical areas (Ahmed, 2024), may not have represented all relevant perspectives or, in particular, those of industry practitioners who have experience in implementation and whose experiences are not

documented. The single researcher approach to the coding and analysis may have constrained the interpretive scope of the thematic analysis because several independent coders were not employed to understand the data. The rather small corpus of 12 documents, while adequate for theoretical saturation for this specialised domain, limits the evidence that can be drawn across the platforms. As a qualitative case study, the results are analytical generalisation to theoretical propositions instead of statistical generalisation to wider populations (Yin, 2018).

## 5.5 Future Research

Several directions for future work are suggested from the contributions and limitations of this study. There is a great need for independent security research for FairPlay and PlayReady at a depth similar to the existing Widevine analyses, so that the security industry can decide whether Fairplay's clean CVE record is evidence of architectural superiority and not just lack of access. Empirical research based on an examination of how content providers actually setup DRM systems in practice would help to clarify whether or not theoretical flexibility is translated into real security benefits. The development of the post-quantum cryptographic threat is a major area, as none of the existing systems use post-quantum algorithms (Rafi et al., 2023). Hardware-security developments, such as ARM TrustZone implementation on desktop platforms, deserve attention since Intel SGX is being deprecated (Roudot & Sabt, 2025). Finally, quantitative research investigating whether adaptive security strategies are related to lower levels of piracy would yield evidence-based guidance of direct practical value (Oestreicher-Singer & Sundararajan, 2010).

In sum, this study has revealed that DRM security-usability trade-offs are not technical issues waiting for perfect solutions but strategic choices based on commercial interests, ecosystem philosophies and stakeholder priorities. Within a global DRM market expected to expand substantially over the next decade (IMARC Group 2024), these findings provide an analytical framework for understanding platform design decisions as well as a basis for their improvement. For the digital

content industry, the key value of the study in terms of modern business practice is that it shows that platform selection, adaptive security tiering and clear communication of security to users are strategic decisions with direct ramifications in customer retention, operational cost and competitive positioning, decisions that merit executive-level attention and not be left to engineering teams alone.

# References


Acharya, S., Mishra, A., & Acharya, O. (2025). Digital Rights Management: Addressing Copyright Protection in the Digital Era. *International Journal for Multidisciplinary Research*, *7*(4). https://doi.org/10.36948/ijfmr.2025.v07i04.51834

Agarwal, D. D., & Cherukuri, A. K. (2025). Confidential Computing for Cloud Security: Exploring Hardware based Encryption Using Trusted Execution Environments. ArXiv.org. https://arxiv.org/abs/2511.04550

Ahmed, S. K. (2024). Research methodology simplified: How to choose the right sampling technique and determine the appropriate sample size for research. Oral Oncology Reports, 12(100662), 1–7. https://doi.org/10.1016/j.oor.2024.100662

Association for Computing Machinery. (2018). *ACM code of ethics and professional conduct.* https://www.acm.org/code-of-ethics

Bitmovin. (n.d.). *Widevine DRM: Google's leading content protection solution*. https://developer.bitmovin.com/playback/docs/widevine-security-levels-in-web-video-playback

BuyDRM. (n.d.). *DRM piracy: What it is and how to prevent it*. https://www.buydrm.com/drm-piracy

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

British Computer Society. (2022). *Code of conduct for BCS members*. https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/

Coates, S. K., & Abroshan, H. (2024). Guideline for the production of digital rights management (DRM). *International Journal of Security, Privacy and Trust Management*, 12(3/4), 31–45. https://doi.org/10.5121/ijsptm.2023.12403

CyberSecurity News. (2024, July 28). DRM vulnerabilities. https://cybersecuritynews.com/microsoft-playready-drm/

Delaune, S., Lallemand, J., Patat, G., Roudot, F., & Sabt, M. (2024). Formal security analysis of Widevine through the W3C EME standard. In Proceedings of the 33rd USENIX Security Symposium (pp. 6399–6415). USENIX Association. https://www.usenix.org/conference/usenixsecurity24/presentation/delaune

Ding, S. (2023). Digital rights management. In V. Mulder, A. Mermoud, V. Lenders, & B. Tellenbach (Eds.), *Trends in data protection and encryption technologies* (pp. 389–402). Springer. https://doi.org/10.1007/978-3-031-33386-6_28

Du, A. Y., Das, S., Gopal, R. D., & Ramesh, R. (2014). Optimal Management of Digital Content on Tiered Infrastructure Platforms. *Information Systems Research*, 25(4), 730–746. https://doi.org/10.1287/isre.2014.0548

Sheokand, R. (2025). Safeguarding Innovation in the Digital Age: The Role of Intellectual Property Rights in the Emerging Digital Economy. International Journal for Research Publication and Seminar, 16(2), 218–230. https://doi.org/10.36676/jrps.v16.i2.273

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods, 5*(1), 80–92. https://doi.org/10.1177/160940690600500107

Filipe, C. (2016). Security on over the top TV services. Ulisboa.pt. https://repositorio.ulisboa.pt/entities/publication/1af7a09b-8ee3-43c3-8ac3-b5641c52e595

Gartner. (2022, October 31). Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly $600 Billion in 2023. Gartner. https://www.gartner.com/en/newsroom/press-releases/2022-10-31-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-600-billion-in-2023

Gillespie, T. (2006). Designed to "effectively frustrate": copyright, technology and the agency of users. New Media & Society, 8(4), 651–669. https://doi.org/10.1177/1461444806065662

Han, L., & Liu, M. (2024). Digital Rights Management (DRM) technologies and legal research: Applications and regulations of encryption, digital watermarking, and copyright protection systems. Applied and Computational Engineering, 82(1), 106–111. https://doi.org/10.54254/2755-2721/82/20240957

Harman, M. (2024, December 4). How to create accessible ebooks—Best practices for digital content. Kitaboo. https://kitaboo.com/accessible-digital-content/

Hassan, H. E.-R., Tahoun, M., & ElTaweel, Gh. S. (2020). A robust computational DRM framework for protecting multimedia contents using AES and ECC. Alexandria Engineering Journal, 59(3), 1275–1286. https://doi.org/10.1016/j.aej.2020.02.020

Hoang, V. P., Pham, T. V., Cao, V. L., & Xu, J. (2023). A first look at digital rights management systems for secure mobile content delivery. *arXiv preprint*. https://doi.org/10.48550/arXiv.2308.00437

H. S., R. (2024). Securing the Digital Landscape: Present Concerns and Hurdles in Digital Rights Management. International Journal of Science and Research (IJSR), 13(1), 1128–1131. https://doi.org/10.21275/sr24118193759

IMARC Group. (2024). Digital rights management (DRM) market: Global industry trends, share, size, growth, opportunity and forecast 2024-2032. https://www.imarcgroup.com/digital-rights-management-market

International Organisation for Standardization. (2024). *ISO/IEC 23078-1:2024 Information technology—Specification of digital rights management (DRM) technology for digital publications—Part 1: Overview of copyright protection technologies in use in the publishing industry*. https://www.iso.org/standard/84956.html

Kasprowski, R. (2010). Perspectives on DRM: Between digital rights management and digital restrictions management. Bulletin of the American Society for Information Science and Technology, 36(3), 49–54. https://doi.org/10.1002/bult.2010.1720360313

Kerscher, G., & Kawamura, H. (2000). *Position paper: DRM for persons who are blind and/or print disabled*. W3C DRM Workshop. https://www.w3.org/2000/12/drm-ws/pp/daisy.html

Kumar, T., Sharma, P., Tanwar, J., Alsghier, H., Bhushan, S., Alhumyani, H., Sharma, V., & Alutaibi, A. I. (2024). Cloud-based video streaming services: Trends, challenges, and opportunities. CAAI Transactions on Intelligence Technology, 9(2). https://doi.org/10.1049/cit2.12299

Lu, Z. (2023). Analysis on AES encryption standard and safety. *Proceedings of SPIE*, 12462, 1246215. https://doi.org/10.1117/12.2662564

Ma, Z. (2017). Digital rights management: Model, technology and application. China Communications, 14(6), 156–167. https://doi.org/10.1109/cc.2017.7961371

Madushanka, T., Kumara, D. S., & Rathnaweera, A. A. (2024). SecureRights: A blockchain-powered trusted DRM framework for robust protection and asserting digital rights. *arXiv preprint*. https://doi.org/10.48550/arXiv.2403.06094

Masoud, M. A., & Ali, H. A. (2015). A practical approach to impede key recovery and piracy in Digital Rights Management System (DRM). *2015 International Conference on Computing, Control, Networking, Electronics and Embedded*

*Systems Engineering (ICCNEEE)*, 318–323. https://doi.org/10.1109/IBCAST.2015.7058528

Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A step-by-step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. International Journal of Qualitative Methods, 22(1), 1–18. https://doi.org/10.1177/16094069231205789

Oestreicher-Singer, G., & Sundararajan, A. (2010). Are Digital Rights Valuable? Theory and Evidence from Ebook Pricing. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.871243

Patat, G., Sabt, M., & Fouque, P.-A. (2022). Exploring Widevine for Fun and Profit. ArXiv.org. https://arxiv.org/abs/2204.09298

Pellegrini, T. (2024). Digital rights management: Technologies, application areas, and governance. In *Springer Reference Wirtschaftswissenschaften*. Springer. https://doi.org/10.1007/978-3-658-34048-3_79-2

Rafi, A., Shepherd, C., & Konstantinos Markantonakis. (2023). A First Look at Digital Rights Management Systems for Secure Mobile Content Delivery. Newcastle University EPrints (Newcastle Univesity), 549–558. https://doi.org/10.1109/trustcom60117.2023.00087

Rehman, S., Bajwa, N. T., Shah, M. A., Aseeri, A. O., & Anjum, A. (2021). Hybrid AES-ECC model for the security of data over cloud storage. *Electronics*, 10(21), Article 2673. https://doi.org/10.3390/electronics10212673

Roudot, F., & Sabt, M. (2025). Narrowbeer: A Practical Replay Attack Against the Widevine DRM Narrowbeer: A Practical Replay Attack Against the Widevine DRM. https://www.usenix.org/system/files/usenixsecurity25-roudot.pdf

Saldana, J. (2021). *The coding manual for qualitative researchers* (4th ed.). SAGE Publications. https://uk.sagepub.com/en-gb/eur/the-coding-manual-for-qualitative-researchers/book273583

Samuelson, P. (2003). The challenge of digital rights management technologies. In J. M. Esanu & P. F. Uhlir (Eds.), The role of scientific and technical data and information in the public domain: Proceedings of a symposium (pp. 193–215). National Academies Press. https://www.ncbi.nlm.nih.gov/books/NBK221850/

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson Education.

https://www.pearson.com/en-gb/subject-catalog/p/research-methods-for-business-students/P200000003484

Simons, B. (2000). From the president: to DVD or not to DVD. Communications of the ACM, 43(5), 31–32. https://doi.org/10.1145/332833.332851

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. John Wiley & Sons. https://www.schneier.com/books/secrets-and-lies/

Schmidt, O. (2024). Hardware Support for DRM: Can Trusted Execution Environments save us from System Lock-down? Retrieved from https://git.orlives.de/schmittlauch/surveypaper-drm-tee/raw/branch/master/main.pdf

Schneider, M., Jayaram, M. R., Shinde, S., Capkun, S., & Perez, R. (2022). SoK: Hardware-supported Trusted Execution Environments. ArXiv.org. https://arxiv.org/abs/2205.12742

ScoreDetect. (2024). *Cross-Platform DRM Guide: Protect Digital Content 2024* https://www.scoredetect.com/blog/posts/cross-platform-drm-guide-protect-digital-content-2024

Sony, M., & Naik, S. (2020). Industry 4.0 Integration with socio-technical Systems theory: a Systematic Review and Proposed Theoretical Model. Technology in Society, 61(1), 1–11. https://doi.org/10.1016/j.techsoc.2020.101248

Subramanya, S. R., & Yi, B. K. (2006). Digital rights management. *IEEE Potentials, 25*(2), 31–34. https://www.researchgate.net/publication/3227866_Digital_rights_management

Tamilselvan, N. (2024). Blockchain-based digital rights management for enhanced content security in digital libraries. *International Journal of Blockchain Technology*, 2(1), 1–8. https://iaeme.com/Home/article_id/IJBT_02_01_001

Tiwari, A., Shukla, P. K., Sharma, S., & Mishra, N. (2025). Algorithms for DRM (Digital Right Management) of OTT (Over the Top) Platforms: A Survey. 1–6. https://doi.org/10.1109/worldsuas66815.2025.11199256

Tripathi, K. P., Giri, S., & Tripathi, N. (2024). Post- positivism Research Paradigm and Philosophical Assumption of Sport Tourism. AWADHARANA, 8, 113–127. https://doi.org/10.3126/awadharana.v8i01.70098

Volckmann, W. M., II. (2024). A model of digital rights management with user disutility. *Journal of Industrial and Management Optimisation*, 20(3), 1269–1308. https://doi.org/10.3934/jimo.2023069

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii–xxiii. https://www.jstor.org/stable/4132319

Wu, D., Nan, G., & Li, M. (2019). Optimal Piracy Control: Should a Firm Implement Digital Rights Management? Information Systems Frontiers, 22(4), 947–960. https://doi.org/10.1007/s10796-019-09907-z

Yilmaz, K. (2013). Comparison of Quantitative and Qualitative Research traditions: Epistemological, theoretical, and Methodological Differences. European Journal of Education, 48(2), 311–325. https://doi.org/10.1111/ejed.12014

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications. https://us.sagepub.com/en-us/nam/case-study-research-and-applications/book250150

Yun, J., Liu, X., Lu, Y., Guan, J., & Liu, X. (2024). DRPChain: A new blockchain-based trusted DRM scheme for image content protection. *PLOS ONE*, 19(9), Article e0309743. https://doi.org/10.1371/journal.pone.0309743

Zhang, L., & Zhang, H. (2023). Protection in DRM and pricing strategies for digital products considering quality degradation. *Economic Analysis Letters*, 2(1), 13. https://doi.org/10.58567/eal02010003

Zwattendorfer, B., & Tauber, A. (2023). Blockchain-based digital rights management systems: Design principles for the music industry. *Electronic Markets*, 33, Article 16. https://doi.org/10.1007/s12525-023-00628-5