2018

Digital content security: video streaming digital rights management system

Benjamin O. Odonya
Faculty of Information Technology (FIT)
Strathmore University

Recommended Citation

Odonya, B. O. (2018). *Digital content security: video streaming digital rights management system* (Thesis). Strathmore University. Retrieved from https://su-plus.strathmore.edu/handle/11071/5992

DIGITAL CONTENT SECURITY: VIDEO STREAMING DIGITAL RIGHTS MANAGEMENT SYSTEM

Benjamin Odonya Owenda

Submitted in partial fulfilment of the requirements for the Degree of Master of Science in Information Systems Security (MSc. ISS) at Strathmore University

Faculty of Information Technology
Strathmore University
Nairobi, Kenya

April, 2018

Declaration

I declare that this work has never been previously submitted and approved for the award of a degree by Strathmore University or any other university. To the best of my knowledge and belief, this dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

Student Name Benjamin Odonya Owenda

Signature ……………………………

Date ……………………………

Approval

This dissertation of Benjamin Odonya Owenda was reviewed and approved by the following:

Supervisor Name Dr. Joseph Sevilla

Signature …………………………………

Date …………………………………

Abstract

The usability and applicability of digital videos, especially through the Internet, offers great opportunities for Kenyan content creators to further their careers as the platform enables them to share ideas which contributes to knowledge in the field which in turn generates wealth in the industry as new and efficient ways of creating the content are discovered making the production and distribution process cost effective. The Internet is however proving to be a double-edged sword as there have been multiple reports and incidences of copyright infringement within the country. This can be largely attributed to the fact that the platforms available to the average user provide a convenient environment for them to make several copies of the protected media file and distribute them as they wish: which facilitates misuse, piracy and plagiarism.

The purpose of this project was to mitigate the unlawful replication and dissemination on an enormous scale of digital videos that are owned by practitioners in the education industry and presented to end users over the Internet. This followed a move by the players in the industry to convert their content into a digital format to meet the demand for online classes.

Popular avenues that have been used to acquire copies of the digital streams include by use of standalone file grabbing software such as Internet Download Manager or browser plugins such as DownThemAll. These software implementations are extremely simple to use and allow users to create local copies of the streams through a single click of a button. They therefore present a threat to an entire ecosystem as content creators are heavily dependent on revenues generated from their material.

This study seeks to develop a solution in the form of a Digital Rights Management (DRM) system that can be used to secure video streams and, in the process, preserve their economic value. A DRM system secures and implements the rights associated with the use of digital content by use of a set of access control technologies, which ensures that the videos are consumed as intended, and no illegal duplicates are created. Rapid Application Software Development Methodology were leveraged to accomplish the objectives

Keywords

Digital Video Streaming, Copyright Infringement, Digital Rights Management, Access Control Technologies

Table of Contents

Declaration 1

Abstract ii

Table of Figures vi

List of Tables ix

List of Abbreviations ix

Chapter 1 Introduction to the Study 1

1.1 Introduction 1

1.2 Problem Statement 3

1.3 General Objective 4

1.4 Specific Objectives 4

1.5 Research Questions 4

1.6 Scope and Limitations 4

1.7 Justification 5

Chapter 2 Literature Review 5

2.1 Digital Video 5

2.1.1 Online Video Piracy 5

2.1.2 Digital Videos for Education 7

2.1.3 Digital Videos in the Kenyan Education Industry 8

2.1.4 State of Piracy and Copyright Infringement in Kenya 10

2.2 Video Security 10

2.2.1 Video Standards 11

2.2.2 Video Encryption Techniques 12

2.2.3 HTTP Live Streaming 15

2.2.4 Digital Rights Management 17

2.3 Discussion 19

Chapter 3 Research Methodology 20

3.1 Introduction 20

3.2 Software Methodology 21

3.3 Requirements Planning 22

3.3.1 Location of Study 23

3.3.2 Target Population.. 23

3.3.3 Research Instruments 24

3.4 User Design.. 24

3.4.1 System Design.. 25

3.4.2 System Architecture 26

3.5 Rapid Construction 26

3.5.1 System Testing 26

3.6 Cutover... 28

3.6.1 System Validation... 28

Chapter 4 System Design and Architecture 28

4.1 Overview... 28

4.2 System Architecture 28

4.2.1 Registration Modules ....
35 29

4.2.2 Video Upload and Encryption Module 29

4.2.3 Subscription Module 30

4.2.4 Video Streaming Module 31

4.3 System Design Tools... 33

4.3.1 Use Case Diagram 33

4.3.2 Use Case Diagram Descriptions... 33

4.3.3 Sequence Diagram 39

4.3.4 Class Diagram 39

4.3.5 Database Schema 40

Chapter 5 System Implementation and Testing ....
49 5.1 Introduction.. 48

5.2 Implementation Environment 49

5.2.1 Registration 49

5.2.2 Video Upload and Encryption 50

5.2.3 Course Subscription.. 53

5.2.4 Encrypted Video Streaming.. 54

5.3 System Testing 55
5.3.1 Unit Testing 55
5.3.2 Compatibility Testing 57
5.3.4 Functionality Testing 59
5.3.3 User Testing 59
5.4 System Validation 67
Chapter 6 Discussion of Results 68
6.1 Overview 68
6.2 Objective One 68
6.3 Objective Two 69
6.4 Objective Three 70
6.5 Objective Four 71
Chapter 7 Conclusions, Recommendations and Future Work 71
7.1 Conclusions 71
7.2 Recommendations 71
7.3 Future Work 72
References 73
Appendices 78
Appendix A: Content Creators Questionnaire 78
Appendix B: Test User Questionnaire 81
Appendix C Content Creator Responses 85
Appendix D: System Code 89
Appendix E: Turn it in Report 91

Table of Figures

Figure 2.1 HTTP Live Streaming 16
Figure 2.2 Media Source Extensions 17
Figure 3.1 Rapid Application Development (RAD). 23

Figure 4.1 Three-Tier Architecture 35
Figure 4.2 Use Case Diagram 36
Figure 4.3 Sequence Diagram 42
Figure 4.4 Class Diagram 43
Figure 4.5 Entity Relationship Diagram 44
Figure 4.6 Catalogue Page 49
Figure 4.7 Video Streaming Page 50
Figure 5.1 Provider Application Form 52
Figure 5.2 Lesson Creation Form 53
Figure 5.3 OpenSSL Key Generation 54
Figure 5.4 OpenSSL IV Generation.. 54
Figure 5.5 PesaPal API 56
Figure 5.6 Video.js Video Player 57
Figure 5.7 User Registration Form 58
Figure 5.8 FFmpeg library Processor Usage on Test PC One 60
Figure 5.9 FFmpeg library Processor Usage on Test PC Two 60
Figure 5.10 Development Environment Hardware Specifications 61
Figure 5.11 Test Users Skills in IT 62
Figure 5.12 Browser Used to Evaluate System 63
Figure 5.13 Browser Access Capability.. 64
Figure 5.14 Number of Mobile Users 64
Figure 5.15 Test Users Internet Access Speed Ratings 65
Figure 5.16 System Resource Response Rate 66
Figure 5.17 System's Compatibility with Network 66
Figure 5.18 System User Interface Rating 67
Figure 5.19 System Navigability Rating 67
Figure 5.20 System's Stream Functionality 68
Figure 5.21 Presence of File Grabbers 68
Figure 5.22 File Grabber Effectiveness 69
Figure 5.23 Alternate Download Means 69

VT OMNES
VNVM SINT

List of Tables

Table 4.1 Login Use Case 37

Table 4.2 Add Content Use Case 38

Table 4.3 Video Conversion Use Case 39

Table 4.4 Course Subscription Use Case 40

Table 4.5 Video Streaming Use Case 41

Table 4.6 Users Table 45

Table 4.7 Providers Table 45

Table 4.8 Course Table 46

Table 4.9 Categories Table 46

Table 4.10 Lecturers Table 46

Table 4.11 Enrolment Table 47

Table 4.12 Syllabus Table 47

Table 4.13 Week Table 47

Table 4.14 Lessons Table 48

Table 4.15 Videos Table 48

List of Abbreviations

AES - Advanced Encryption Standard

ATM - Asynchronous Transfer Mode

BASCAP - Business Action to Stop Counterfeiting and Piracy

CA - Communications Authority of Kenya

CBC - Cipher Block Chaining

CENC - Common Encryption

DECE LLC - Digital Entertainment Content Ecosystem LLC

DRM - Digital Rights Management

DV - Digital Video

FPS - FairPlay Streaming

HLS - HTTP Live Streaming

HTTP - Hypertext Transfer Protocol

ICC - International Chamber of Commerce

ICT - Information and Communication Technology

IP - Intellectual Property

IPTV - Internet Protocol Television

ISPs - Internet Service Providers

IV - Initialisation Vector

KICD - Kenya Institute of Curriculum Development

KPA - Kenya Publishers Association

MIME - Multi-Purpose Internet Mail Extensions

MPEG - Moving Picture Experts Group
MVC - Model–View–Controller

OMA - Open Mobile Alliance compliant Digital Rights Management

P2P - Peer-to-peer

RAD - Rapid Application Development

VCEG - Video Coding Experts Group

VEA - Video Encryption Algorithm

VoD - Video on Demand

WIPO - World Intellectual Property Organization

W3C -World Wide Web Consortium

Chapter 1 Introduction to the Study

1.1 Introduction

A report by Deloitte (2015) found that media use around the globe is progressively occurring in digital formats. Besides increasing Internet access speeds, the rise in the number of gadgets that have the ability of supporting digital media has given consumers a choice of accessing their preferred media content be it information, entertainment or social activity at any time or location. Media use in the United States of America has exhibited stupendous increase and has experienced a remarkable leap from conventional media to new media. The ascent of digital media players, for example Amazon, Hulu and Netflix, are challenging the customarily conserved primacy of the television as the principle entertainment hub. The same report also notes that greater part of this data growth is credited to various digital media particularly the entertainment services like video and audio. The report states that globally, video and audio traffic has ruled the Internet data consumption for a few years now.

The most popular method that consumers use to view the videos is through streaming. Streaming can be defined as transporting content that is continually received by, and presented to, the user, while it is being delivered by the provider. Streaming media is therefore multimedia data transferred in a stream of packets that are interpreted and rendered, in real time, by a software application as the packet arrives (Green, 2012). Continuity of transmission while the content is already being consulted and the absence of permanent transfer of data to the user computing device make up the distinguishing features of streaming (Rayburn, 2007).

Streaming has led to the rise of Video on Demand (VoD) concept which concentrates on content that is in video format. VoD can be defined as non-linear appropriation services of dematerialised audio-visual content. Nonlinear implies that the content is consumable independent of a program, at the time picked by a consumer. The strategies of access differ: for example, to be viewed once or several times, downloadable on a media to own or to rent, or leased for a given duration. Payper-View (purchase of a program made available at a fixed time) is excluded from VoD because while VoD is available to watch at whatever moment that a consumer deems fit, Pay-per-View events unlocks a channel for a specific block of time with programming that starts and ends at scheduled times (Philippe, 2009). A study by the Directorate-General for Internal Policies also notes that VoD may be streamed or downloaded (Maciejewski, Fischer, & Roginska, 2014).

This development has brought about a novel technique of conducting business which is founded on access to services as opposed to product sales. It is like a move to cultural production from industrial production where the centre of attention is concentrated on the advertising of social assets as paid-for private entertainment (Helberger, 2005). This shift is frequently made reference to as digital media revolution comprising of a suite of digital, media-capable gadgets and services that are positioned to deliver the goal of anywhere-anytime access to information (Ce, Yuenan, & Xiamu, n.d.). The drift towards the digitalisation of data stream has prompted the metamorphosis of initial e-commerce (initially acting as electronic windows for physically-performed transactions) into advanced e-commerce (working solely on an electronic premise, for instance downloading of digital goods and services), and eventually into omnipresent commerce (where rights to prevalent, established and portable access to connectivity and services are characterised by and based on electronic recognition and digital identity; thus placing the user, instead of technology, as the focus. This evolution is exemplified by the growing role one's Facebook identity plays in bestowing a digital identity over the Internet.

The above mentioned digital shift has been experienced in Kenya in the form of online classes which are popularly referred to as distance learning locally. Distance learning in Kenya is a field of education that centres on delivering education to students who are not physically present in the institution of learning, university or college. It aims at providing access to students when the lecturers or professors and the learners are separated by distance. This therefore means that the student does not have to attend classes in person, the learner may undergo training by help of technology. The only time that students make it to physical classes is when they are undergoing practical courses. This is very effective for those who have other commitments like work and do not have time to enrol for traditional classes. Examples of distance learning programs include Kenyatta University’s Digital School, University of Nairobi’s Centre for Open and Distance Learning, Moi University Institute for Open and Distance Learning and JKUAT’s Distance Learning and Continuing Education.

Kenyan students are opting for streaming and online access to content mainly because of the ease of access and services available. Lessing (2004) explains that, when connecting to services that grant access to content becomes tremendously simple, then it would be simpler to use these services for content access rather than downloading and storing the same amount of content on numerous gadgets that one might have for playing/consuming the content. Essentially, subscription would be the simpler option compared to being a database manager, which is what everyone in the download-sharing world basically is. The online shift however has not been a walk in the park. The new trend has led to misappropriate use of the video content, with piracy leading the line. Piracy can be defined as the unsanctioned or forbidden use of audio-visual works covered by copyright law, in a way that infringes one of the copyright owner's exclusive rights, such as the right to reproduce the copyrighted work, or to make derivative works (collinsdictionary, 2018).

The main countermeasure has been to enact laws that have been geared at curbing the trend. Internationally, the laws that have been enacted for punishing piracy in developed countries are severe and correctional in nature. In Kenya, however, piracy does not get the attention it deserves due to more pressing issues that the country faces. It however does not mean that there exists no interest in the field: various industries have been taking active interest in stopping or at least slowing down the trend. These firms pinpoint sources of piracy and afterward organise raids with the assistance of the police. Convictions are nonetheless few and penalties not sufficiently harsh to act as a deterrent.

There is therefore the need for a technological solution in the form of a Digital Rights Management (DRM) system. DRM is a far-reaching term that refers to any scheme that controls access to copyrighted material using technological means (Layton, n.d.). Essentially, DRM removes usage control from the individual in possession of digital content and places it in the hands of a computer program.

1.2 Problem Statement

The emergence of digital videos and analogue/digital conversion technologies, especially those that are usable on personal computers, has vastly increased the ease at which copyrighted videos can be pirated. Malicious users target video streaming sites and platforms as avenues of accessing copies of these media files. This act is enabled by a slew of popular file grabbing tools that allow users to download videos as they are being streamed to their devices.

There is therefore a danger of content creators losing millions of shillings in revenue because of piracy on their digital video streams. They are faced with the challenge of delivering content to users while safeguarding their intellectual property against misuse.

1.3 General Objective

To develop a DRM system that protects and enforces the rights associated with the use and consumption of digital video streams. This includes access control that ensures that access to protected content is only possible under pre-specified conditions and the prevention of creation of unauthorised copies.

1.4 Specific Objectives

i. To find out about the application of digital videos in the Kenyan education industry and understand the online video streaming piracy issue,

ii. To find out video encryption techniques and existing Digital Rights Management (DRM) solutions,

iii. To design, develop and test a system that enforces rights for digital video stream owners,

iv. To validate the effectiveness of the developed solution.

1.5 Research Questions

i. How are digital videos used in Kenyan education industry?

ii. What are the current techniques and solutions used to address video stream piracy?

iii. What features will be integrated into the developed system? iv. Does the developed system address the local challenge of video stream protection?

1.6 Scope and Limitations

The scope of the developed system covers protecting videos that are streamed by users with intermediate computer skill level. The system is also targeting the Kenyan market.

Even though there exist many ways of delivering digital videos to the end user, this research will only focus on streaming as it is currently the most widely used method of consumption.

1.7 Justification

Digital video files do not suffer from analogue properties as they can be duplicated severally with no degradation in quality for subsequent copies. Consumers can conveniently use personal computers to convert media originally in a physical/analogue form or a broadcast form into a universal, digital form. This, combined with the advent of the Internet and popular file sharing tools, has made unauthorised distribution of copies of copyrighted digital videos much easier.

It is necessary to prevent the widespread infringement that the digital environment enables, and thus to protect the revenues of content creators. The revenue generated provides the incentive that keeps these individuals creating more content.

Chapter 2 Literature Review

This chapter explores the literature review with the purpose of identifying the need for a digital video stream DRM system in Kenya. This is followed by a research on securing digital video information through encryption and an overview look at existing solutions that are currently in use.

2.1 Digital Video

Rahul Sikarwar (2016) defines digital media as digitised content that can be transmitted over the Internet or computer networks. This can include text, audio, video, and graphics. He also states that most digital media are based on translating analogue data into digital data. The focus of this research is on digital videos which falls under digital media. Digital Video (DV) is video that is captured and stored in a digital format as ones and zeros, instead of a series of still pictures captured in film. Digital signals are used as opposed to analogue. Information is processed and stored as a sequence of digital data for easy manipulation by computers, however the video is still presented to the viewer through a screen in analogue form (Digital Video, n.d.). Digital videos have an advantage over analogue in that they facilitate ease of sharing and storage, they do not suffer from degradation of data quality when copied, it is generally easy and inexpensive to copy them, and they have the capacity for multicasting.

2.1.1 Online Video Piracy

Intellectual property refers to manifestations of the mind which includes inventions, scholarly and imaginative works and symbols, names and images used in commerce. Intellectual property is partitioned into two categories. The first category which is industrial property comprises of patents for inventions, trademarks, industrial designs and geographical indications while the other is copyright which covers literary works (such as novels, poems and plays), films, music, artistic works (for example, drawings, paintings, photographs and sculptures) and architectural design (World Intellectual Proprety Organization [WIPO], 2004). Copyright forms the main point of focus for this research. Intellectual Property Rights on the other hand are exclusive legal rights over creations of the mind. They give the proprietor rights from which to exploit their intellectual creation. They are deemed pivotal to nurturing innovation by bestowing a financial incentive to spark creativity, whereby businesses can garner the benefits from their inventions and will be more eager to invest in research and development (Broomfield, 2009).

The invention of the Internet has vastly disrupted the above concepts. Its advent has revolutionised our society from one that was powered by industrial might to one that is predominantly driven by information access. Kenya's intellectual property laws for instance have not kept up with this transition. Intellectual property was originally created to promote the growth of technologies and culture in a way that provides the maximum benefit to all individuals. This was setup in a manner that provided individuals exclusive rights to their intellectual property for a limited amount of time, ideally enough to make their investment worthwhile (Digital Rights and Intellectual Property, n.d.).

A report published by Sohn (2006) explains that the exponential proliferation of the Internet and digital media has created both stupendous opportunities and unfamiliar threats for content creators. The report attributes this to the advances in digital technology which the author notes offer pristine approaches to marketing, distributing, interacting with, and giving legal value to creative works, yielding rise to broadening new markets that did not exist in the prior years. The author also states that these technologies also vow to democratise the production of creative content by putting the creation and wide dissemination of creative works within the reach of private individuals. The report however warns that the technologies have fostered considerable obstacles for copyright custodians striving to discharge jurisdiction over the distribution of their works and harbour against piracy.

In recent years, malicious users have used Peer-to-peer (P2P) file sharing to distribute material. P2P file sharing can be described as the practice of sharing and transferring digital files from one computer to another. In a P2P network, each peer is an end-user's computer connected to the other peer via the Internet; without going through an intermediary server. Users take part by downloading and installing a P2P software program (Peer-to-Peer File Sharing, 2014). This form of illegal file sharing has however faced several litigations with several countries' courts ordering their Internet Service Providers (ISPs) to start blocking a range of torrent sites. A torrent is a file type used by BitTorrent file-sharing protocol. It sanctions and pinpoints to a remote server that holds the location of distinct remote hosts with an instance or part of the file to be shared or downloaded (techopedia, 2018). This has prompted pirates to shift from peer-to-peer downloads to illegal streaming-video sites for film and television content. These were the revelations according to a study on global piracy conducted by Muso (2017), a United Kingdom antipiracy firm. The firm reports that in 2015, out of a total 78.5 billion visits around the globe to film and TV piracy sites, 73.7% were to streaming sites. It further reports that torrent-based sites like the Pirate Bay constituted just 17.2% of overall user visits, with direct-download sites accounting for the remainder. Additionally, Muso's study found that traffic to torrent sites for movie and TV shows declined by 19% in the final six months of 2015 compared with the first half of the year 2016.

These findings indicate that there is a global uptick in piracy on streaming sites, which is how majority of Kenyan content creators deliver their content. A different study conducted by the nonprofit Digital Citizens Alliance found that video streaming accounted for 21% of revenue generated by piracy-site operators in 2014, up from 12% in the previous year (Trouble in Our Digital Midst, 2017).

2.1.2 Digital Videos for Education

Educators have embraced digital videos as they have realised their benefits over traditional classroom lectures. According to The University of Queensland (2018), the utilisation of innovative video in education gives some pedagogical advantages, for example, encouraging reasoning and critical thinking, helping with mastery learning, motivating and drawing in students, and authentic learning opportunity. By utilisation of sight and sound, digital videos are the ideal medium for students who are auditory or visual learners. With the additional use of subtitles every student then has the option of watching, listening to, or reading each presentation. Video empowers and engages students creating interest and maintaining that enthusiasm for longer timeframes, and it provides an inventive and compelling means for teachers to address and convey the required curriculum content (zaneeducation, 2018).

Digital Videos can be effectively applied in education through the use of Video on Demand (VoD) Services. VoD services are preferably positioned to extend the reach of value education and even assist in the subsidisation of the cost of education. According to Stephen Watson (2016) ondemand is not just for entertainment, as education can be regarded as a standout opportunity of streamed content as cutting-edge video on demand platforms allow for customisation and revenue generation through memberships, sponsorship and advertising models, which could be used to fund education and reduce the cost of tuition. The platforms allow students to choose and watch video content of their choice by means of either their televisions or computers. VoD also enables teachers to customise and live stream their own content which also gives students in remote regions access to the most effective lectures (Rehorn, 2016).

2.1.3 Digital Videos in the Kenyan Education Industry

Kenya has been using digital videos since the turn of the new millennium in many key sectors of its economy including television, advertising and entertainment industries. A key area that had not been explored however was in education. Most of the curriculum in Kenya has been in analogue format for years with textbooks being the main mode of delivery. The digital shift gained traction with the digital learning program which was one of the key flagship programs underlined in the Jubilee Manifesto. The key objective of the programme was to align incorporation of Information and Communication Technology (ICT) into teaching and learning for standard one pupils in primary schools. The undertaking constituted of the enhancement of ICT infrastructure, development of digital content, capacity building of the teachers and acquisition of ICT devices (Digital Learning Programme, 2018). The key highlights from the undertaking was that the Government designated 17.58 billion Kenyan shillings (167 million US dollars) for deployment of ICT learning devices to schools in the 2015 budget, which was used to develop digital content, building the capacity of teachers and set up computer laboratories in state funded schools across the nation (Odero, 2016).

After the official commencement of the project, focus shifted to the digitisation of content. The Kenya Institute for Curriculum Development (KICD) took centre stage at this point. The body's aim was to provide digital content both for learners and teachers with its most recent achievement being the launch of digital content for Standard One. The content was made available through an interactive platform where anyone can access it using any Internet enabled device. Though the field of digital learning is still growing in Kenya, the country has seen a lot of interest in the sphere with local content creators seeing the potential in growth. This has inspired them to enter the domain and start producing digital content. These entities include both public and private universities with the most notable institution to take full advantage of the technology being Kenyatta University. The university's platform called Digital School of Virtual and Open Learning (formerly Institute of Open, Distance and e-Learning) seeks to provide learning opportunities to students who are unable to take up full-time on-campus programs. The School offers an extensive variety of programs at Diploma, Undergraduate and Postgraduate levels using blended teaching and learning that merges digital instructions with live tutorials in major towns including Nairobi, Mombasa and Nakuru (Kenyatta University Digital School, 2018). The platform currently hosts 2,462 digital videos and has 9,853 students enrolled (Digital School, 2018).

Once all the content has been digitised, a key area of focus that the content creators may turn to is video distribution. Several developments in the country in recent years all point to VoD services as the best suited avenue. One key development has been the penetration of the Internet. According to the first quarter sector statistics of the Communications Authority of Kenya (CA) for the year 2017-2018 (July-September 2017), the demand for Internet saw a jump of 12.5 percent to post 51.1 million users compared to 45.4 million users that was reported in the previous quarter. The report also noted that there had been an increased uptake of broadband Internet, which rose by 14.3 percent to stand at 17.6 million users compared to the previously reported 15.4 million users. The CA also pointed out that mobile data remained the key component to Internet subscriptions with 41 million users.

This remarkable growth in Internet access and connection within the country provides an opportune platform for the assumption of VoD services, both from an end-user and service provider point of view. This is because Internet is persistently becoming less expensive due to the ever-growing rivalry in the telecommunication industry. Limitless Internet packages by most telecommunication firms can provide an opportunity that VoD services can leverage as it can encourage bulk use of

data therefore encouraging the appropriation of VoD services. Although the Internet is regarded as the cornerstone of the sector, inventive payment options and content also
assume a fundamental part in the growth of the VoD sector (Tredger, 2016).

2.1.4 State of Piracy and Copyright Infringement in Kenya

A study that was conducted by the International Chamber of Commerce (ICC) Business Action to Stop Counterfeiting and Piracy (BASCAP) (2013) initiative reported that Kenya's current intellectual property (IP) rights regime performs poorly in international gauges, ranking 95th of 130 countries in the IPR Index and 106th of 140 economies in the Global Competitiveness Index 2010. The report was accompanied by recommendations for Kenya to bring its IP regime and IP enforcement efforts up to international standards. The study is supported by a report by the US Chamber of Commerce which outlines the international intellectual property (IP) index. The index shows that actual enforcement of laws in Kenya is weak, with regulatory bodies lacking the right expertise and resources. It ranked the country at a low position of 31 out of the 45 world economies that were indexed. The report states that the rank was hugely attributed to the weak and judicial system dogged by case backlog, gaps especially in the digital space and ambiguous legislation (US Chamber of Commerce, 2017).

Copyright infringement has already been an issue for textbook publishers within the country which was highlighted in Longhorn Publisher's 2016 annual financial report (Longhorn Publishers, 2016). This trend prompted the Kenya Publishers Association (KPA) in partnership with the Ministry of Education and Kenya Institute of Curriculum Development (KICD) to develop a tool which checks unique hidden numbers at the front, inside or back of books to verify whether individuals are buying authentic books. The system was developed in an effort to lower losses attributed to piracy which stands at 7 billion Kenyan Shillings annually (Matinde, 2017).

2.2 Video Security

While the focus of the content owners is to guarantee that maximum users consume the content legitimately; the same content should be safeguarded against unlicensed copying, illegal redistribution, misappropriation and piracy (Bhat, 2016). Security has proved to be vital for individuals in the field so much so, that the Digital Entertainment Content Ecosystem LLC (DECE LLC), a cross-industry consortium dedicated to driving a new, open market for digital content distribution unveiled UltraViolet, a digital rights system (Vrechek, 2010). Content security is clearly important to content creators; therefore, an assessment of the techniques used to encrypt videos and the solutions that are currently being used is required to build a security system. According to Sing and Hooda (2012) The objectives of secure video transmission are: confidentiality, conditional access, authentication, copy control and content tracking. Different video applications require different level of security. They further differentiate the security needs into sensitive video applications and entertainment applications. Applications under the former category generally demand stringent security preconditions like the ones employed by text encryption. The encryption algorithms for personalised video services must hold out against not only classical cryptanalytic attacks but also the perceptual attack to ensure that no visible information related to the sensitive communication is revealed (Uhl & Pommer, 2005). On the other hand, perceptible information in the multimedia can be used in Perceptual attacks that endeavour to recreate the video from the scrambled parts. Perceptual attacks can be carried out in two ways; the first method treats scrambled data in the multimedia stream as corrupted sequences that are caused by packet loss or bit errors. Assailants can then recreate the initial multimedia through methods that disguise the errors by relying on the medium's statistical information. The other method tries to make the video perceptible by substituting scrambled segments with random data. These techniques can only be used on selective encryption techniques that encrypt a fixed amount of data (Wu & Kuo, October 2005).

The techniques that are used for secure video transmission encompass cryptography, digital signature and video watermarking. It is widely accepted that no single technology can allot a comprehensive solution for guarding video transmission and that cryptography, digital signatures and watermarking each has a role in security applications (Eugene, Gregory, Paul, & Edward, 2001). Liu and Koenig (2010) maintain that encryption for video applications can only be deemed secure if either the cost involved in breaking the algorithm is higher than the license fee for the content; or the time required to break the encryption is longer than the time that the content is considered valuable.

2.2.1 Video Standards

A basic understanding of the various available video standards is necessary before looking at encryption. A standard video file in a digital format is composed of two parts, a "codec" and a container. A codec is used to compress and decompress a video file while a container is a collection of files that stores information about the digital file. A combination of both audio and video data in a single file allow for simultaneous audio-with-video playback (motionelements, 2013).

a. MPEG-1

Video file compression using the MPEG-1 codec may incorporate both sound and video, however the sound track may utilise a different sort of compression. MPEG-1 standard was intended for coding of moving pictures and related sound for digital storage media at up to around 1.5 Mbit/s, for example, compact disks. Unfortunately, the standard was not intended to be robust against bit errors rendering it unsuitable for broadcast transmission (Haskell, Puri, & Netravali, 1996).

b. MPEG-2

MPEG-2 is a standard for the compression of video and sound. MPEG-2 is optimised for the compression of TV and HDTV with a high quality. MPEG-2 is used for TV-distribution (DVB) over the air, cable and satellite, and on DVD. The typical bit rates for the compression of TV is 4 to 9 Mbit/s. For high definition TV, the bit rate is in the order of 80 Mbit/s (telecomabc, n.d.). The standard can support Asynchronous Transfer Mode (ATM) networks.

c. H.264/MPEG-4

This is a video coding standard of the ITU-T video coding experts group (VCEG) and the ISO/IEC moving picture experts group (MPEG). H.264/MPEG4-AVC has of late emerged as the most comprehensively acknowledged video coding standard since the deployment of MPEG2 at the inception of digital television, and it may soon eclipse MPEG-2 in daily use. It encompasses all typical video applications ranging from mobile services and videoconferencing to IPTV, HDTV, and HD video storage (Marpe, Wiegand, & Sullivan, 2006).

2.2.2 Video Encryption Techniques

Encryption is the technique of altering a message into cipher code using an encryption algorithm, to hamper unsanctioned access to the message (Kaliski, 1993). Encryption can be used to provide end-to-end security and with the aid of watermarking, copyright protection can be enforced

(Angelides & Agius, 2010). Video encryption algorithms can be grouped into four categories; Perceptual Encryption, Permutation based Encryption, Selective Encryption and Fully Layered Encryption.

Perceptual Encryption

Under these algorithms, the initial acoustic and/or visual quality of the target data is just slightly lowered by the encryption process. This means that the scrambled multimedia elements may still be partly discernible after the scrambling process, which makes it suitable for applications such as pay TV where potential customers may be able to sample the lower quality adaptations of the original media before making the decision to purchase them (Shunjun , Guanrong , Albert , Bharat , & Kwok-Tung , 2007).

Permutation Based Encryption

Algorithms under this bracket predominantly employ disparate permutation algorithms to carry out encryption on the video contents. Algorithms include;

a. Pure Permutation

   Bytes within a frame of a MPEG stream are scrambled under this algorithm. However, use of this algorithm should be cautiously contemplated because, as demonstrated by Slagell J. Adam (2018), their sheer use is defenceless against known-plaintext attack.

b. Zig-Zag Permutation

   Zig-Zag permutation scrambles an individual 8x8 block to 1x64 vector by using a random permutation list (secret key) as opposed to mapping the 8X8 block to 1X64 vector in ZigZag order (Tang, 1996). This algorithm is unable to prevent known-plaintext attack which can be carried out by presuming that specific video frames are known beforehand: by merely contrasting known plaintext attack with matching encrypted frame the secret key can be effortlessly discovered.

c. Huffman Codeword Permutation

   This is a light algorithm which incorporates both MPEG encryption and compression in a single procedure (Shi & Bhargava, 1998). By joining compression and encryption, this algorithm is able to save computation time and simultaneously avoid diminishing video compression rate.

d. Correlation Preserving Permutation

These algorithms allow applications/users to carry out encryption on source data before reaching the compression stage, as opposed to majority of encryption algorithms that cannot achieve this because of the randomisation effect on the source data that they have. This algorithm therefore allows one to scramble video data before the encoding process. Both sorted and "almost sorted" frames are strongly spatial correlate under this scheme. (Socek, et al., 2006).

Selective Encryption

Selective Encryption algorithms carry out encryption tasks by encrypting only selective bytes in video frames. The advantage of this is that computational complexity is decreased as not every byte in video data is encrypted. An example of an algorithm under this class is Video Encryption Algorithm (VEA) (Shi & Bhargava, 1998). Indications of all Discrete Cosine Transform (DCT) coefficients in a MPEG stream are haphazardly altered by VEA, which utilises a secret key. Only a slight segment of the original multimedia is worked on, making VEA fast. Compared to DES algorithm, VEA proves to be more efficient which can also be attributed to the previously mentioned small number of MPEG compressed video bits that are discerningly encrypted/worked on. These selected bits are XORed one time with the corresponding bit of the secret key. Unfortunately, if an attacker discovers the original video image (plaintext and ciphertext), then he/she shall be able to carry out a plaintext attack as VEA is susceptible to it.

Fully Layered Encryption

Standard encryption schemes like Data Encryption Standard (DES) or Advanced Encryption Standard (AES) are employed by this class to encrypt every byte in the MPEG stream. The algorithms do not use any special structures and regard MPEG bitstreams as text data (Shiguo, 2008). The advantage of Fully Layered Encryption is that it offers security to entire MPEG streams as every byte is encrypted, and additionally, there currently exists no algorithm that is capable of breaking either triple DES or AES. This technique however requires considerable computation making it slow and hence unsuitable for use in real time video applications.

2.2.3 HTTP Live Streaming

HTTP Live streaming (HLS) allows individuals to stream audio and video using the http protocol. It does this by first conveying the files through a media encoder, which converts the files into a preferable format for delivery, before sending it to a segmenting process that chops the files into several segments and saves them as sets of TS files (transport stream files). A corresponding manifest file is also generated, which dictates the order of the TS files. The manifest file is what is stored on the server to distributable to users for streaming (Kania & Gusukuma, 2018).

Figure 2.1 illustrates how HLS works. The client software accesses the manifest file through an URL. It then uses this file to process the TS files into a single continuous stream for the end-user to consume.

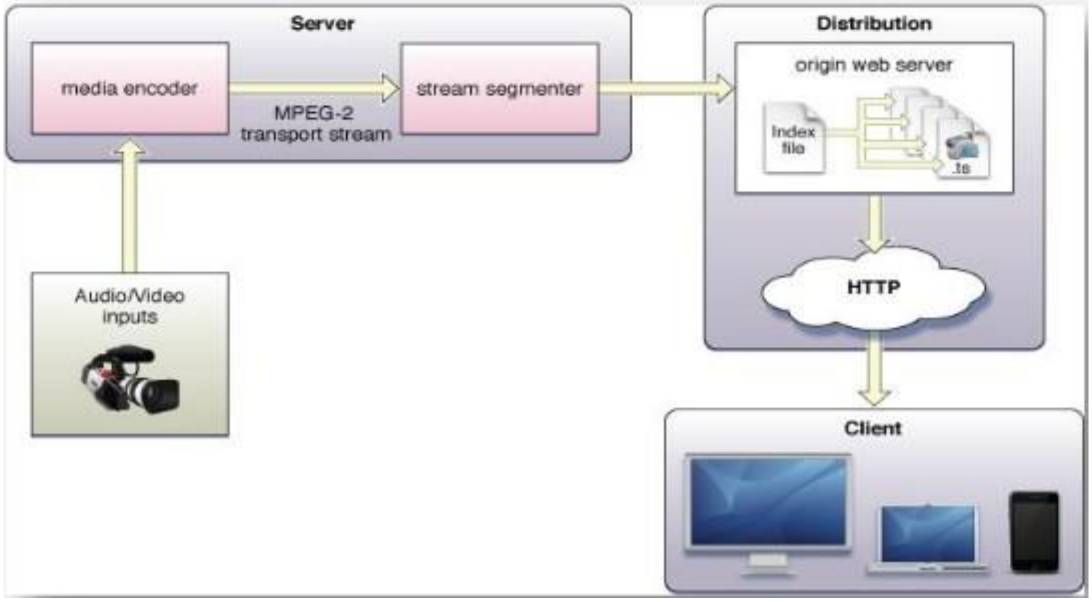


Figure 2.1 HTTP Live Streaming

Source (Kania & Gusukuma, 2018).

Media Source Extensions

Developed by the World Wide Web Consortium (W3C), the specification allows JavaScript to dynamically construct media streams for audio and video. It does this through a MediaSource object that acts as the source of the media data. These objects have several SourceBuffer objects that applications can append data segments to. Data from this buffer is managed as track buffers for audio, video and text that is decoded and played (W3C, 2016). Figure 2.2 illustrates the interaction between the Media Source and HTML media elements through JavaScript.

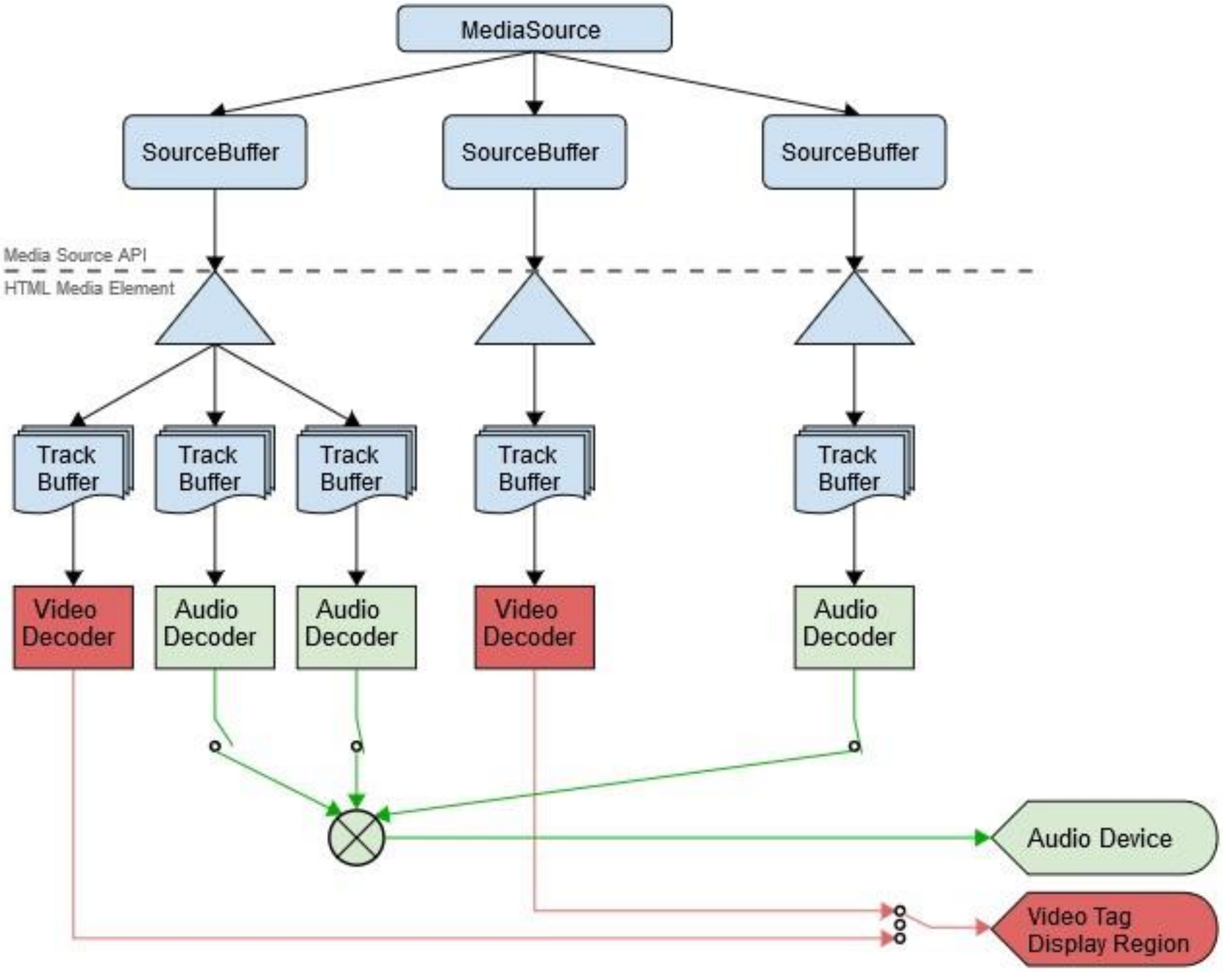


Figure 2.2 Media Source Extensions

Source (W3C, 2016).

Encrypted Media Extensions

Encrypted Media Extensions offers an API that allows web applications to interact with content protection systems to permit playback of encrypted audio and video. It allows for the same application and encoded files to be used in whichever browser, regardless of the underlying protection system using Common Encryption (Dutton, 2018). Common Encryption solutions enable content providers to encrypt and package their content once per codec, and use it with a variety of Key Systems, CDMs and clients. For example, a video packaged using Widevine can be played back in a browser using Playready obtaining a key from a Playready license server.

These implementations are mentioned briefly below.

2.2.4 Digital Rights Management

DRM is defined as an extensive variety of technologies that confer control and protection to content providers over their own digital media. The economics of putting content online without a guaranteed return is moving content providers to re-examine their business models. From their point of view, there are three key components to its life cycle: the creation of content, the distribution and upkeep of content, and the use of content (Xiao, 2018).

PlayReady

PlayReady is a DRM technology by Microsoft used to protect premium content from being viewed without a valid license. It is used in conjunction with Microsoft's Smooth Streaming protocol (ooyala, 2018). The platform has a wide ecosystem that covers a broad array of devices and Operating Systems that emphasize on user experience (microsoft, 2018). The platform is comprised of servers that carry out packaging, licensing and distribution of content; and metering and domain control servers.

Widevine

Widevine is Google's DRM scheme for securely licensing distributing and protecting playback on video on any consumer device. Content creators, MSOs, and other enterprise media companies use Widevine to guarantee the monetisation of content across each gadget. Google purchased Widevine in 2010 to extend their support for media and entertainment enterprises, accelerate the YouTube video streams, and to assist with Android and adaptive streaming (encoding, 2018). It implements a selection of industry standards to protect content as it's transferred over the Internet and played back on devices; these include a combination of Common Encryption (CENC), licensing key exchange, and adaptive streaming quality to manage and send videos to users. The idea is to simplify the amount of work on the service provider's end, by supporting multiple levels of streaming quality based on the security capabilities of the receiving device. The system is available as two versions; Modular and Classic. Widevine Modular is the successor to Widevine Classic.

FairPlay

Apple's DRM platform, FairPlay, is a DRM scheme initially created by Veridisc, and more broadly adopted by Apple, Inc. It is designed to encrypt content packaged using HTTP Live Streaming and is envisaged for use with all iOS devices as well as Apple TV. On the desktop, Apple's DRM converter FairPlay is also built into QuickTime. Apple initially used FairPlay to protect content distributed through the iTunes Music Store. While Apple no longer encrypts iTunes Music downloads, FairPlay DRM is still used in the new Apple Music service for content stored locally (encoding, 2018).

FairPlay Streaming (FPS) is Apple's DRM system used exclusively to secure video content for delivery across Apple products and services (drmtoday, 2018). It secures the distribution of streaming media to devices through the HTTP Live Streaming protocol. FPS therefore allows content providers, encoding vendors and delivery networks to encrypt content, securely exchange keys, and protect playback on iOS, tvOS and Safari on macOS (apple, 2018).

Other DRM Solutions include;

a. DivX DRM: According to DivX (2018), the platform was developed with MPAA and Hollywood studios' contribution to safeguard copyrights online and in devices while delivering a seamless user experience. The solution permits secure digital distribution of DivX video through a content licensing platform for playback on a computer and other DivX Certified consumer electronics products. It protects the copyrights holders against unsanctioned replication and illegal appropriation without limiting where, how or when consumers may enjoy their video.
b. Marlin: Marlin DRM is an open-standard content protection system for consumer devices and services. It offers sophisticated copyrights management for playing entertainment and media content (including, audio, video, eBooks, and games) distributed over mobile, broadband, broadcast, and all other popular channels. The main advantage that Marlin has is that it is not a proprietary DRM, making it capable of delivering content over any network or physical media (intertrust, 2018).
c. Open Mobile Alliance compliant Digital Rights Management (OMA): OMA is a Digital Rights Management standard published by the Open Mobile Alliance for the secure delivery of digital content across the Android open source platform. OMA DRM Engine checks for licenses, evaluates the rights language of the license and decrypts the content for the application, working in conjunction with Android software (helpnetsecurity, 2009).

2.3 Discussion

From the available literature, piracy is an issue that is yet to be fully solved globally. In Kenya, local content creators have been losing millions of shillings in revenue owing to the plague as evidenced by the report by longhorn publishers. The report also indicates that the problem is experienced to a large extent in traditional media such as textbooks.

The literature review has also shown that the country has already started its shift to a digital era with the education industry being the latest entrant. This move is expected to cause ripple waves within the sector as content creators, which includes both universities and private individuals, rush to convert their content into a digital format; to be compliant with the new curriculum. A method that has emerged for content delivery is through the use of digital videos. By use of the medium both the individuals and institutions who hold digital rights to them are guaranteed feasible revenue streams. However, to maximise on profits the content must be purchased by as many individuals as possible with little room for malicious enterprising individuals to make copies and redistribute them for their own personal gain.

There is therefore a need to get ahead of the issues that has plagued the education industry in the past. The gap can be filled by a digital solution that can help prevent, or at the very least reduce, the widespread trend of piracy within the country. The solution launched for textbooks is a revolutionary idea that is destined to alter the status quo in the industry, however its launch came at a time when book publishers had already lost millions of shillings in revenue streams. A local digital rights management system can therefore offer assurance and guarantee to content creators that their content shall be secure once they are done with digitising them and are ready to publish.

The literature has additionally recognised a wide assortment of video encryption algorithms; nonetheless, a number are not secure against cryptanalysis attacks. It likewise shows that although fully layered encryption algorithms are slow in nature and do not offer real time support, they give the highest level of security. The benefit of Permutation based algorithms is that for the most part they are quicker, however, the matter of security is not adequately addressed when the level offered is considered. The benefit of Selective encryption algorithms is that they limit the overhead associated with encryption by selecting just a subliminal amount of data to encrypt, however, similar to Permutation based algorithms, their level of security and speed can be called to question as they are heavily dependent on the specific parameters that they encrypt, and the number of these parameters. It can be argued that Perceptual encryption algorithms are not suitable for applications that require high security mostly because of their applications on services such as pay per view TV where it would be suitable for potential users to be allowed to view low quality versions of a videos before they make the decision of acquiring them. In summary, it may be a difficult task to select and use any of the encryption algorithm as none satisfies all performance specifications. It therefore advisable to pick one based on the intended purpose or use of an application.

The literature review has also briefly identified several proprietary solutions that can be used to secure digital videos. However, the objective of this project is to develop a security solution which is both accessible to Kenyan content creators who do not want to be subjected to lengthy licensing processes and that is also affordable and easily accessible.

Chapter 3 Research Methodology

3.1 Introduction

This chapter provides a formal documentation for the phases that the system was subjected to during its development life cycle. It defines the precise objectives for each phase and the results required from a phase before the next one can begin. It is worth noting that the chosen methodology and subsequent steps were arrived at after carefully reviewing the literature and observing how other eLearning and DRM systems work.

The first two objectives of the research which were, first: to find out about the application of digital videos in the Kenyan education industry and to understand the online video streaming piracy issue, and secondly to find out video encryption techniques and existing Digital Rights Management solutions were addressed under the Requirements Planning phase of the selected RAD methodology. The third objective which was to design, develop and test a system that enforces rights for digital video stream owners was addressed under the phases of User Design and Construction. The final objective, which was to validate the effectiveness of the developed solution was addressed under the Cutover phase of RAD.

3.2 Software Methodology

Rapid Application Development (RAD)

RAD was used to achieve the objectives previously indicated. RAD refers to a development life cycle intended to yield significantly faster development and higher quality outcomes than traditional life cycles. It is designed to take maximum advantage of powerful development tools that have evolved in recent business environments. The characteristics of RAD can be harnessed to deliver robust, flexible and quality systems in the shortest time scale possible (CASEMaker Inc, 2000). The basis of RAD is use of evolutionary prototyping techniques operating in an environment of tight delivery time scales. It focuses upon identifying the important users and involving them via workshops at early stages of development and on obtaining commitment from the business users. It also requires a CASE/integrated development environment or 4GL tools and RDBMS products. The concept of RAD has been in existence for some time, traditionally viewed as a ‘quick fix’ approach and not considered a technique to deliver quality systems (agilebusiness, 2014). However, it has evolved over the years with its application within a framework to achieve project/quality control measure associated with other development methodologies.

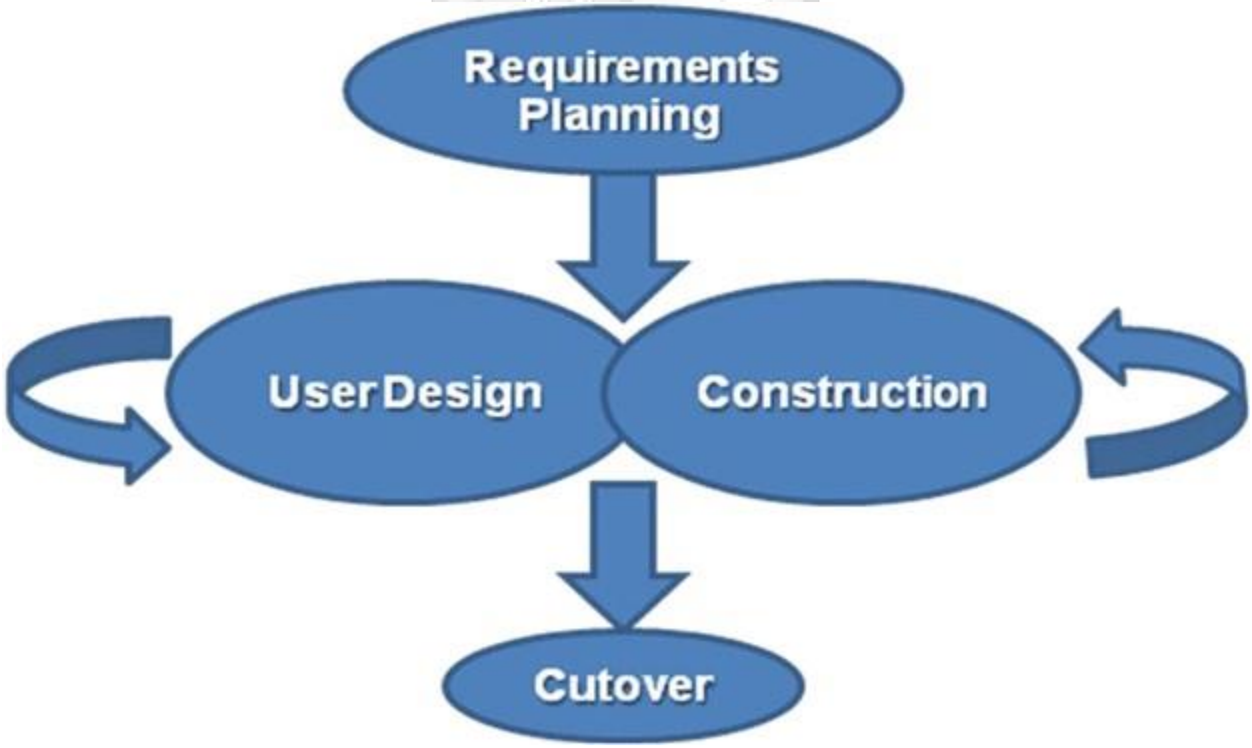


Figure 3.1 Rapid Application Development (RAD) process structure

Source (svantesystems, 2018)

The steps can be divided into four distinct phases;

i. Requirements Planning: This phase usually involves designers, developers and users whose main task is to determine a rough estimate of project scope and application requirements. The benefit of carrying out this phase is that it allows for subsequent phases to begin which comprise of prototyping.

ii. User Design: Opinions from users is collected to ensure that information is geared towards determining the system architecture. The phase is important as it allows initial modelling and prototypes to be created. This step is usually repeated as often as necessary as the project evolves.

iii. Rapid Construction: This phase follows the previously mentioned stages and involves the actual construction of the application through programming, testing, and integration activities. This phase, along with User Design, is repeated as often as necessary to match the new component requirements. Alterations are therefore made to meet the needs of the project.

iv. Cutover: This phase, which is also referred as the Transition stage involves the switch of components from a development environment to a live production environment. This stage is carried out by the development team who may be able to also carry out comprehensive testing or team training.

The RAD approach was deemed suitable as it involves several techniques which enable the requirements, and subsequently the system to be developed via a series of iterative activities generally involving the use of prototypes. Once developed, the prototypes allowed the system to be examined and modifications and refinements were made quickly and easily. The prototypes then became the final delivered system.

3.3 Requirements Planning

The requirements planning stage consisted of collecting insights from key stakeholders. The focus was on both developing a high-level list of initial requirements as well as setting the project scope. The phase aimed at constraining the solution space to solutions that encouraged small-problem solutions that synergistically worked together to satisfy the large-problem solution which was the system. The phase involved an analysis of the current tools used in DRM and looking at the industry needs. This was important as the results guided the project scope and requirements as constraints surrounding the project's environment were considered. The iterative prototypes produced thereafter were used to guide the development process as feedback was received after every iteration and every change incorporated. This ensured that the delivered system was in line with expectations.

3.3.1 Location of Study

The study was carried out at @iLabAfrica, a Centre of Excellence in ICT innovation and Development based at Strathmore University. The department offers numerous courses and certifications which are best suited to be digitised and optimised for the system.

3.3.2 Target Population

The target population mainly comprised of individuals with intermediate to advanced Information Technology skills. While the scope of the project was earlier indicated as users who had up to intermediate Information Technology skills, users with more advanced skills were deemed more suitable in order to guide the development process and aid in the identification of system requirements.

A Non-Probability Sampling technique was used in selecting the target population. Nonprobability sampling is a sampling technique where the samples are gathered in a process that does not give all the individuals in the population equal chances of being selected (explorable, 2018). This approached was used because the research required a skill set that could not be easily identified by random sampling.

Judgmental Sampling approach to Non-Probability Sampling was used. Judgmental sampling is a non-probability sampling technique where the researcher selects units to be sampled based on their knowledge and professional judgment (edrm, 2018). The population was divided into two. The first group comprised of four members of Digital Learning team of @iLabAfrica and six other individuals in their network. The department deals with content creation and digitisation of education material and has done extensive research in the field and is conversant with matters affecting it and other players in the industry. The team is comprised of graphic designers, video editors and researchers and has connections with other individuals in the same field, six of them being selected for this study. The sample size for this group was therefore ten. It is also worth noting that this research relied heavily on the presented literature and the purpose of this group was to ascertain the degree that finding agreed with the actual subject matter. The second population was made up of fifteen Information Technology professionals with at least a bachelor's degree in the field. This comprised of programmers, system and network administrators and individuals in technical support. This second group's main purpose was to test the system for various aspects discussed in section 3.5.2.

3.3.3 Research Instruments

Questionnaire

A questionnaire is a research instrument consisting of a series of questions for gathering information from respondents (simplypsychology, 2018). Two sets of questionnaires were used for the two sets of target population identified in section 3.3.2. The questionnaires were used with pre-determined questions and an opportunity for correspondents to clarify on responses. The first questionnaire, which can be found on Appendix A of this document, was aimed at confirming the level at which the findings from the Literature Review corroborated with the target group, while the second questionnaire, which can be found on Appendix B, investigated whether the system met its requirements.

Document Review

The study reviewed documents from the Literature Review with two objectives; one was to identify the gaps in the education industry in Kenya and possible solutions, while the other was to reveal the technical requirements and specifications of a DRM system.

3.4 User Design

The data collected in requirement planning phase, as well as the identified gaps in the industry and input from users, offered valuable insights that helped to identify the most important driving factors to be considered. By identifying these factors, the causal relationships of the target industry were identified, which was modelled in the simulation model at the System Design stage in the modelling process. Once the various bits and pieces of information were gathered, it was structured in a way that allowed their relations to be formed. This was necessary to identify which of the many factors identified was crucial to solve the problem defined; as explained below.

i. Functional Requirements: The weakness and gaps that arise from the current status quo of piracy and lack of a proper DRM systems in the local e-learning market, which were identified in the conclusion under the Literature Review formed the proposed functionality of the system.

ii. Technical Requirements: The technical requirements were developed in accordance to the above identified functional requirements, they describe how the functional requirements were implemented.

3.4.1 System Design

The System Design stage applied an object-oriented design methodology approach. An objectoriented methodology is defined as the system of principles and procedures applied to objectoriented software development (Object-Oriented Languages and Systems, n.d.). The System Design therefore made use of the Unified Modelling Language (UML), which is a standardised modelling language that is made up of diagrams that aid system and software developers to specify, visualise construct and document the artefacts of software systems (visual-paradigm, 2018). This stage was expected to yield an effective and efficient implementation, with its deliverables being;

i. Use Case diagram: A use case diagram is used to summarize the details of a system's users (also known as actors) and their interactions with the system (lucidchart, UML Use Case Diagram, 2018). It was used to clearly define the scope of the system and the goals that the system helps the actors achieve.

ii. Class diagram: A class diagram in the UML is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects (visual-paradigm, 2018). Was used to show how the classes relate to the actual code. It was also used to show integrated subsystems that make up the system.

iii. Sequence diagrams: Sequence diagrams describe interactions among classes in terms of an exchange of messages over time (smartdraw, 2018). It was also used to visualise runtime scenarios between a user and the system.

iv. Database Schema: A database schema is the skeleton structure that represents the logical view of the entire database (tutorialspoint, 2018). It was used to show how the data is organized and how the relations among them are associated.

v. Wireframe diagrams: A wireframe diagram is a visual tool used to show where different elements on an interactive media page should be displayed (sqa, 2018). The diagrams were used to ensure the system is built according to goals as they show how features are implemented and how they work, hence focusing on usability.

3.4.2 System Architecture

The system makes use of a 2 tier Client/Server architecture. The system along with its database is hosted on a web server running in a cloud environment. End-users (clients) gain access to the server through a web browser; requiring an active Internet connection to act as a communication medium between them and the server.

3.5 Rapid Construction

System Implementation uses the structure created during architectural design and the results of system analysis to construct system elements that meet the stakeholder requirements and system requirements developed in the early life cycle phases (Sebok, 2017). The development of the system was in two parts; construction of a web application that is connected to a relational database and secondly, implementation of security standards required to satisfy the main goal of the project. The implementation covered the following phases:

i. Backend development: Technical specifications and the developed Use Cases and Class Diagrams from design phase were used to guide the backend development of the system to ensure intended functionalities were met.

ii. Frontend development: The frontend which is a web-based interface, was developed and guided by target end-users to ensure that other users would be able to information that is relevant and easy to see.

iii. Languages: Backend development was implemented with PHP. PHP is a recursive acronym for Hypertext Preprocessor, a scripting language used to create dynamic and interactive HTML Web pages. A server processes PHP commands when a website visitor opens a page, then sends results to the visitor’s browser (techopedia, PHP, n.d.)

iv. Framework: Laravel, which is a free, open-source PHP web framework, was used to develop the system. Laravel is based on the model–view–controller (MVC) architectural pattern (laravel, 2018).

3.5.1 System Testing

The system was tested against its specifications to verify whether it met its functional requirements. The tests included;

i. Unit Testing: It involves breaking the program into pieces and subjecting each piece into a series of tests. The tests were run periodically after every change to the source code to limit future problems. Tests included checking whether the helper classes returned the right results, checking the algorithm on different inputs and checking all edge cases.

ii. Compatibility Testing: Was performed when the build got stable enough to ensure that it worked well for all platforms. Test included **browser** compatibility testing which was the most important compatibility test. It checked compatibility of the three major browsers which are Chrome (version 65.0.3325.181 (Official Build) (64-bit)), Firefox (version 59.0.2 (64-bit)) and Microsoft Edge (version 38.14393.2068.0) to check the compatibility of the software applications. The next test involved the **hardware.** The system was configured on a server running Ubuntu 16.04.3 LTS. Checks included software compatibility with the host hardware configuration such as allocated memory and processor time. A **network** test was also carried out to evaluate the performance of the system in a network with varying parameters such as Bandwidth, Operating speed and Capacity. The final check was to ensure **mobile device** compatibility on different operating systems such as android and iOS.

iii. Functionality Testing: It is a type of testing which verifies that each function of the software application operates in conformance with the requirement specification (functional Testing Tutorial, 2018). The tests covered mainline functions which tested the main functions of the system and a basic usability test to check whether a user can freely navigate through the system without any difficulties.

iv. User Testing: User testing refers to a technique used in the design process to evaluate a product, feature or prototype with real users (everyinteraction, 2018). The tests were carried out by a carefully selected test group of fifteen users. This group comprised of Information Technology professionals with at least a bachelor’s degree in the field. These users were provided with a questionnaire, which can be found on Appendix B of this document, to fill in **after** evaluating a live demo of the system. The tests included an accessibility test which checked the level of accessibility of the system to the user, browser compatibility and mobile compatibility.

3.6 Cutover

This phase involves moving the system from a development environment, carried out on a computer running windows 10 OS, to a live production environment, which is a Linux server running Ubuntu 16.04.3 LTS. A direct approach was taken as there were no other systems to replace/phase out.

3.6.1 System Validation

Once the system was deployed on a live environment, system validation was done to ascertain that the developed system serves its intended purpose. The process determined if the requirements specified in the User Design phase were correct and verify that the developed system met these requirements. The system was validated by the security department of @iLabAfrica. Validation included carrying out an assessment of the ease or difficulty that an experienced hacker would have when trying to pirate/copy/download a video stream on the system. The system would be validated if the amount of effort required by the experienced hacker would surpass the amount of effort that an intermediate user would logically use under normal circumstances.

Chapter 4 System Design and Architecture

4.1 Overview

This chapter shall cover the architecture and design of the Video Streaming DRM System which satisfy all the requirements that were discovered and gathered during the Requirement Planning and User Design phases. The developed system allows for a special group of users called providers to create courses and add content to these courses which include video files. During the video upload process the files are encrypted and stored in a secure location on the server. System administrators can thereafter approve the lessons for viewing by a separate group of users known as learners. This group can access the content via a web browser. The prototype was developed using RAD methodology.

4.2 System Design

The system design was based on the findings that were identified during the Literature Review stage and feedback obtained from content creators, which can be found on Appendix C of this document. There were some similarities in the findings from these sources such as the need for video encryption and watermarks which are key to this research and were considered. The content creators were however keen on a system that not only provides for security through encryption, but also offers a monetization platform, ability to track content and share it on social media sites. While some of the offered feedback fell out of the bounds of this research, key insights such as a monetization platform was considered and integrated with the already established requirements, which led to the identification of four key modules that include Registration, Video Upload and Encryption, Subscription and Video Streaming modules. These modules are discussed in detail below.

4.2.1 Registration Modules

Users who intend on accessing restricted pages of the system shall be required to first create user accounts. This process shall be facilitated by a user registration HTML form that shall email, username and password fields. Once submitted, the system shall validate the input fields and post the data into a MySQL relational database. This process shall be followed by an email being sent to the indicated email address with a link to validate it and activate the registered account.

The system is intended to allow any content creator to be able to host their content on it. Registered users shall be provided with a conveniently placed “Become a provider” tab which shall direct them to a HTML form that shall allow them to set up a company profile. Once all the required fields are filled the users submit the form which are posted to a providers table. If the application is approved by system administrators, the users gain access to course creation pages, which they can use to create courses and upload their content.

4.2.2 Video Upload and Encryption Module

The security aspect of the system shall be in two parts; the first one being video upload and encryption. This section shall briefly discuss findings from the Literature Review and how they guided the system design.

The genesis of the entire process shall begin with the video standard. As already pointed out, MPEG-4 has emerged as the most comprehensively acknowledged video coding standard and is optimised for a wide variety of applications including Internet Protocol Television (IPTV) which Video on Demand falls under. The system shall therefore include a validation class that checks the Multi-Purpose Internet Mail Extensions (MIME) type of the uploaded video to ensure that only MPEG-4 files are uploaded. This shall also ensure the system is future proof by not accepting an outdated standard like MPEG-1 and the soon to be phased out MPEG-2. The video upload process shall be handled by a lesson creation form, which providers can use to specify various aspects of a lesson including name and additional description/content. This form shall also include an input field that accepts video files.

The literature also evaluated several video encryption techniques including Perceptual Encryption, Permutation based Encryption, Selective Encryption and finally, Fully Layered Encryption. For this project, Fully Layered Encryption which includes Advanced Encryption Standard (AES) shall be used. The selection was based on two factors; first, as evidenced by the literature, Fully Layered Encryption, though slow in nature, provides the highest level of security of all the evaluated techniques. Secondly, and perhaps most importantly, HTTP Live Streaming (HLS) which was also discussed in the literature only supports AES-128. AES is a symmetric key algorithm, which means that the same key that is used to encrypt the video file, is also used by the video player to decrypt it. AES-128 uses a key length of 128 bits (16 bytes). HLS also uses AES in Cipher Block Chaining (CBC) mode; which means that each block is encrypted using the cipher text of the preceding block. An Initialisation Vector (IV) shall therefore be generated to encrypt the first block. The IV is basically a 16-byte randomly generated value that shall be used to start the entire encryption process; therefore, its secrecy is not paramount. Both the key file and IV shall be pregenerated using OpenSSL. OpenSSL is a robust, commercial-grade, and full-featured toolkit for the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols. It is also a generalpurpose cryptography library (openssl, 2018).

To achieve encryption, FFmpeg library shall be used. FFmpeg is a free open source project that produces libraries for handling multimedia data (ffmpeg, 2018). This library shall be installed on the host computer. The use and implementation of FFmpeg shall be discussed under the System Implementation and Testing chapter of this document.

4.2.3 Subscription Module

Part of this project’s justification, apart from preventing widespread infringement of content creator’s intellectual property, was to protect their revenue streams which provides the incentive for them to keep creating more content. This is also in line with some of the feedback offered by content creators (which can be found on Appendix C). The subscription module shall be integrated solely for this purpose. Subscription shall entail either of two options; the first shall involve free courses, where the system shall automatically enrol users when they try to access them, while the second shall involve paid courses. For paid courses, PesaPal payment API shall be integrated to handle money transfers. The API was chosen because of the various local payment options such as Safaricom's M-Pesa and Airtel money which offer convenience to the users who are expected to be predominantly from markets where these platforms are commonly used.

4.2.4 Video Streaming Module

Users on the system shall access encrypted video files through HTTP Live Streaming (HLS) which in recent decades has become the well accepted standard for streaming videos mostly because of its native support on mobile devices. HLS was deemed suitable for use as it supports client-driven adaptive bitrate selection, can be delivered over standard HTTP ports, it uses simple, text-based manifest format and finally because it does not require proprietary streaming servers to work.

However, most major browsers do not natively support HLS (except for safari). Therefore, to provide HTML-based video, the system had to be integrated with a video player with HLS playback capability. This was done using Video.js which is an extendable framework/library around the native video element. It offers a plugin API so that different types of video can be handed to the native video element. However, it only supports DRM video through a plugin. Both Video.js and the plugin will be added to the implementation to allow for playback of the encrypted segments. The same key that was generated under the Video Upload and Encryption Module shall also be used in this module for decryption. An in band key exchange shall be used. In-band key exchange indicates that the two parties share an encryption key in the same communication channel as the encrypted data (gcgapremium, 2018).

The video player shall also include a watermark at the bottom right edge in the form of a logo. This watermark shall be permanently embedded at this location; however the size shall be minimal in order to provide an unobstructed view of the video being watched.

4.3 System Architecture

The developed system is based on the three-tier architecture; these include the user interface (presentation layer), application tier/business rules layer and the data storage layer. The presentation layer is made up of web browsers installed on clients' machines. Users interact with the system through this layer and can also request for resources stored on the server. The application tier is the main layer of the system as it implements access rules for resources and actors. It also controls all the application functionalities and performs detailed processing. The final tier is composed of the MySQL relational database server which is protected from direct access by the client hosts. The server houses all the data and files uploaded and requested by end users. Files are grouped into two, images and videos. The images are publicly accessible without any security measures while video access is strictly forbidden without undergoing specialised procedures; therefore, interactions can only occur through the application tier.

The system is also comprised of four actors, namely; system administrator, content provider, learner and PesaPal. The administrators have both read and write rights and have the authority to approve of content that is uploaded to the server or prevent it from being viewed by deleting it. Providers contribute content to the system by creating various courses; which includes lessons and videos. The final group of actors are the learners. This group subscribe to courses and consume their content. The subscription process includes making monetary deposits to PesaPal before being granted access to courses. Figure 4.1 shows an illustration of the architecture.

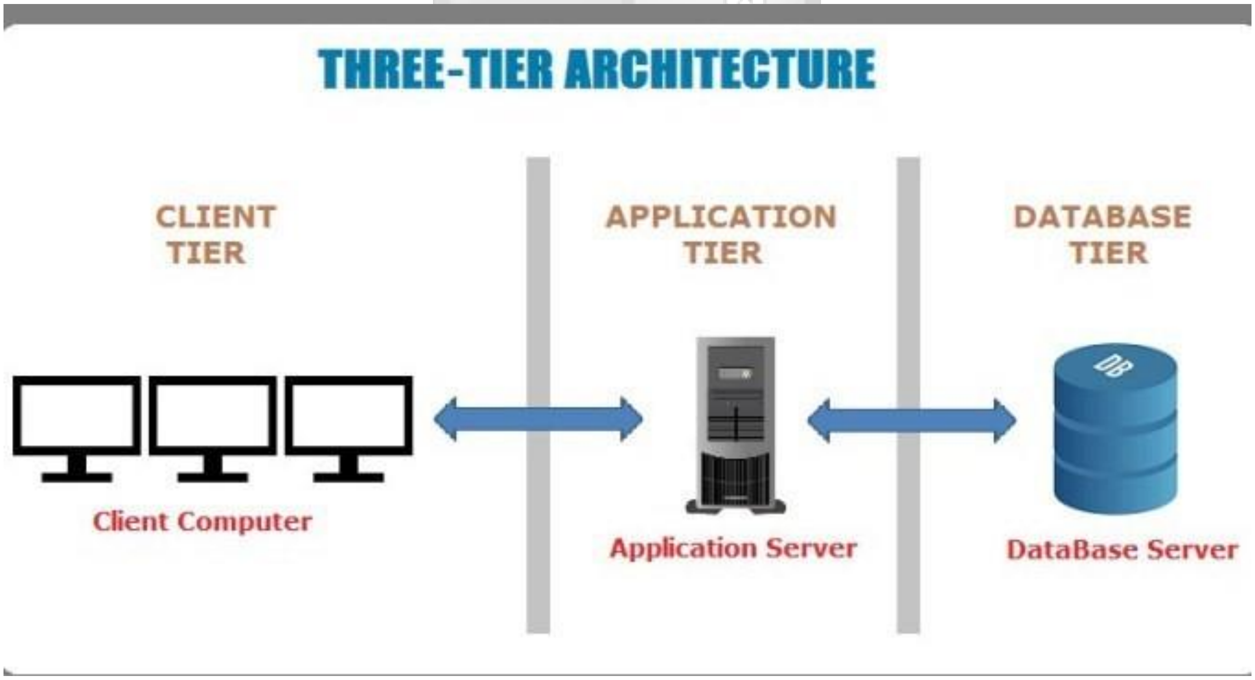


Figure 4.1 Three-Tier Architecture

Source (Gaur, 2018)

4.4 System Design Tools

This section includes a discussion on the system design which is supported by a use case, use case diagram description tables, a sequence diagram, a class diagram and an entity relation diagram.

4.4.1 Use Case Diagram

The use case represented by Figure 4.2 below represents the actors' interaction with the video DRM system and the relationship between them and use cases that they are involved in.

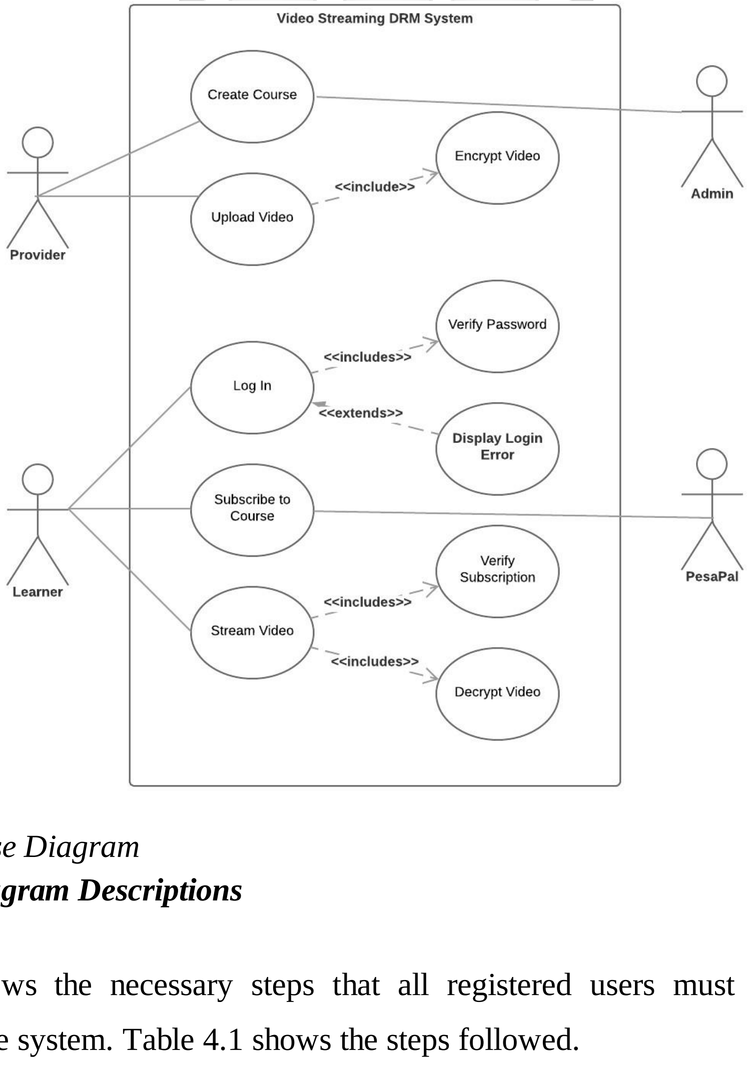


Figure 4.2 Use Case Diagram

4.4.2 Use Case Diagram Descriptions

Login Use Case

This use case shows the necessary steps that all registered users must follow to be fully authenticated by the system. Table 4.1 shows the steps followed.

Table 4.1 Login Use Case

Use Case Name:	login
Description:	This use case allows for users to log into the system to access the relevant functions based on the user’s role. The various user roles are administrator, learner and provider. To log into the system, all users must enter their email addresses and password. Upon successful login, the system will display the relevant user’s home page
Primary Actor:	User
Secondary Actor:	None
Preconditions:	1. User must have a valid account
Postconditions:	1. The system displays the relevant homepage
Main Flow:	1. The user enters the email address and password 2. The user submits the email address and password 3. The system validates the email address and password 4. The system verifies the email address and password 5. The system authenticates the user and redirects to the homepage 6. The use case ends
Alternative Flows:	3a Missing email address/password 1. The system prompts for email address/password 2. Use case resumes at main flow step 1 4a Invalid email address/password 1. The system displays “invalid email address/password” message 2. The system prompts for email address/password 3. Use case resumes at main flow step 1

Create Content

Table 4.2 shows part of the steps taken by the video upload and encryption module that is initialised by a provider.

Table 4.2 Add Content Use Case

Use Case Name:	addContent
Description:	This use case allows for users to add their content to the system. The users must have the 'provider' role to access this functionality. Users first create courses before proceeding to upload videos.to storage. The system first stores the uploaded files in a secure location before triggering the video conversion. The encrypted files are stored in a separate location. System administrators must approve of the content
Primary Actor:	Provider
Secondary Actor:	Administrator
Include use case:	1. Trigger video conversion
Preconditions:	1. User must have a 'provider' role 2. Video file must be in mp4 format
Postconditions:	1. The system displays a success message
Main Flow:	1. The user enters relevant course information 2. The user selects a video file in mp4 format 3. The user submits the course information and video file 4. The system validates the course information and video file 5. The system uploads the file to a publicly inaccessible folder 6. The system triggers the video conversion use case 7. The system updates the RDBMS with the new information 8. The system verifies the email address and password 9. The system notifies the administrator of pending approval 10. The system displays a success message 11. The use case ends
Alternative Flows:	3a Missing course information 1. The system prompts for necessary information

	2. Use case resumes at main flow step 1 3b Invalid video file format 1. The system displays “invalid video file” message 2. The system prompts for video file 3. Use case resumes at main flow step 2

Video Conversion

Table 4.3 shows the other half of steps taken by the video upload and encryption module.

Table 4.3 Video Conversion Use Case

Use Case Name:	convertForStreaming
Description:	This use case allows for conversion of uploaded video files into a streamable format.
Primary Actor:	Provider
Secondary Actor:	None
Preconditions:	1. FFmpeg must be installed on the host machine 2. AES 128 key file must be created 3. A file with the necessary encryption details must be created
Postconditions:	1. The system updates the database
Main Flow:	1. The system verifies the installation status of FFmpeg 2. The system retrieves the uploaded video file 3. The system converts the file for HTTP Live streaming by segmenting it and encrypting each segment with the provided key 4. The system generates the main manifest file with playlist information 5. The system stores the generated files in a secure folder 6. The system updates the database 7. The use case ends

Alternative Flows:	1a Missing FFmpeg 1. The system prompts for ffmpeg installation 2. Use case resumes at main flow step 1 3a Missing Key File
	4. The system displays “invalid video file” message 5. The system fails and exits

Course Subscription

Table 4.4 shows the steps taken to the subscription module which is initialised by a user. *Table 4.4 Course Subscription Use Case*

Use Case Name:	subscribeToCourse
Description:	This use case allows for a user to subscribe to paid courses
Primary Actor:	Learner
Secondary Actor:	Pesapal
Preconditions:	1. The user must be authenticated 2. The user must not be subscribed
Postconditions:	1. The system updates course subscription details
Main Flow:	1. The user tries to access a course 2. The system checks subscription status 3. The system redirects to PesaPal with auth details and course cost 4. The user completes payment 5. Pesapal confirms payment and redirects to the system 6. The system updates course subscription details 7. The use case ends
Alternative Flows:	4a Insufficient funds 1. The system displays “request could not be completed” message 2. The system redirects the user back

Video Streaming

Table 4.5 shows the steps taken to allow user to stream a video.

Table 4.5 Video Streaming Use Case

Use Case Name:	streamVideo
Description:	This use case allows for a user to stream encrypted video files
Primary Actor:	Learner
Secondary Actor:	None
Preconditions:	1. The user must be subscribed to the course 2. The user must be logged in
Postconditions:	1. The video player decrypts each segment and streams the content to the user
Main Flow:	1. The user tries to access a video 2. The system checks subscription status 3. The system retrieves location of the manifest file from the RDBMS 4. The system redirects to the webpage with a video player 5. The video player loads the manifest file with the location of AES key 6. The video player retrieves the encryption key 7. The video player decrypts each segment and streams the content to the user 8. The use case ends
Alternative Flows:	2a User not subscribed 1. System redirects user to subscription page 5a Key file not found 1. The system displays error message on player

4.4.3 Sequence Diagram

Figure 4.3 shows the sequence diagram, it depicts the interaction between a learner and the system when trying to stream a protected video file.

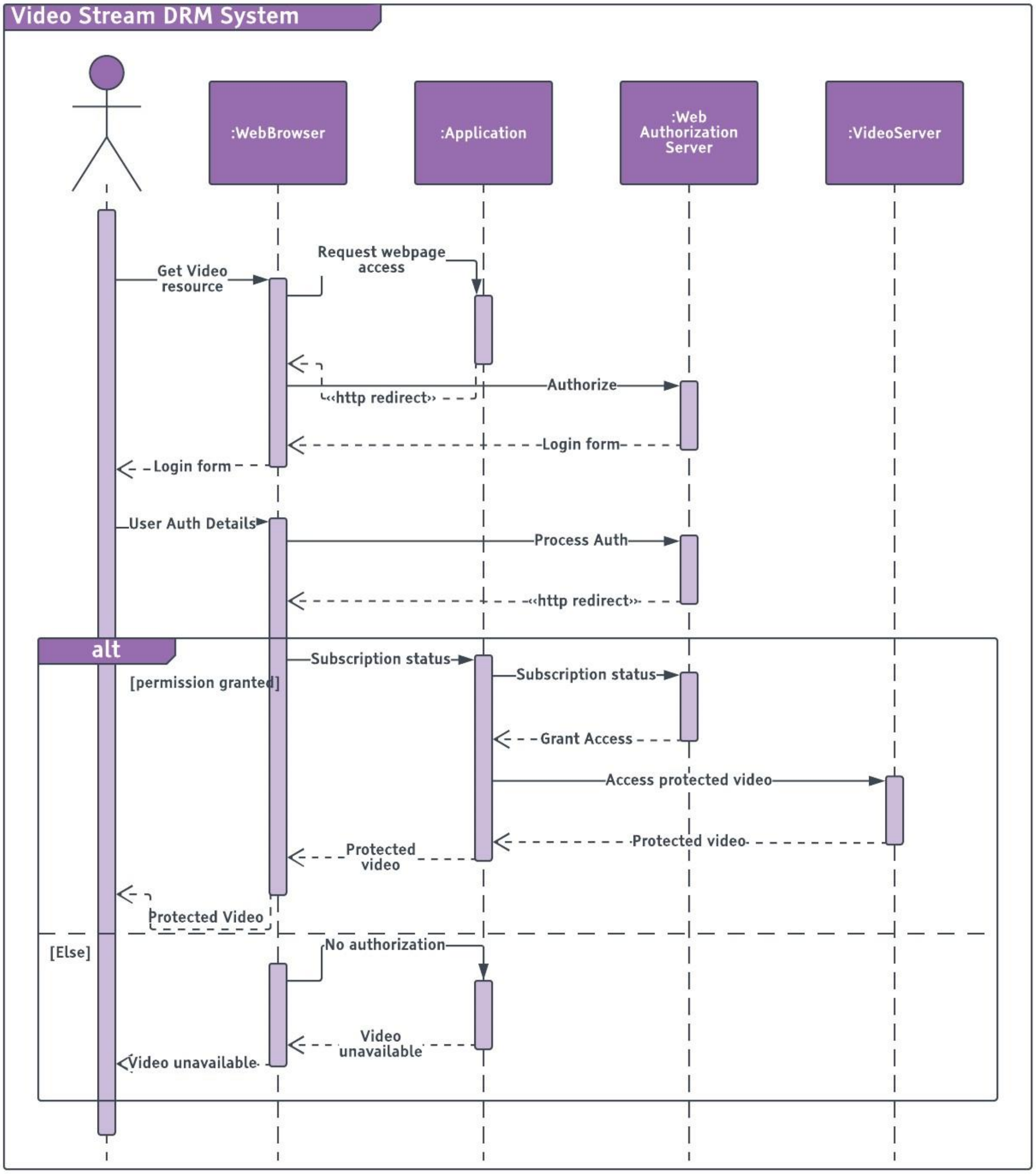


Figure 4.3 Sequence Diagram

4.4.4 Class Diagram

Figure 4.4 shows a static view of the system's classes and the main attributes and methods that they possess. It also shows the relationship and interaction among other objects.

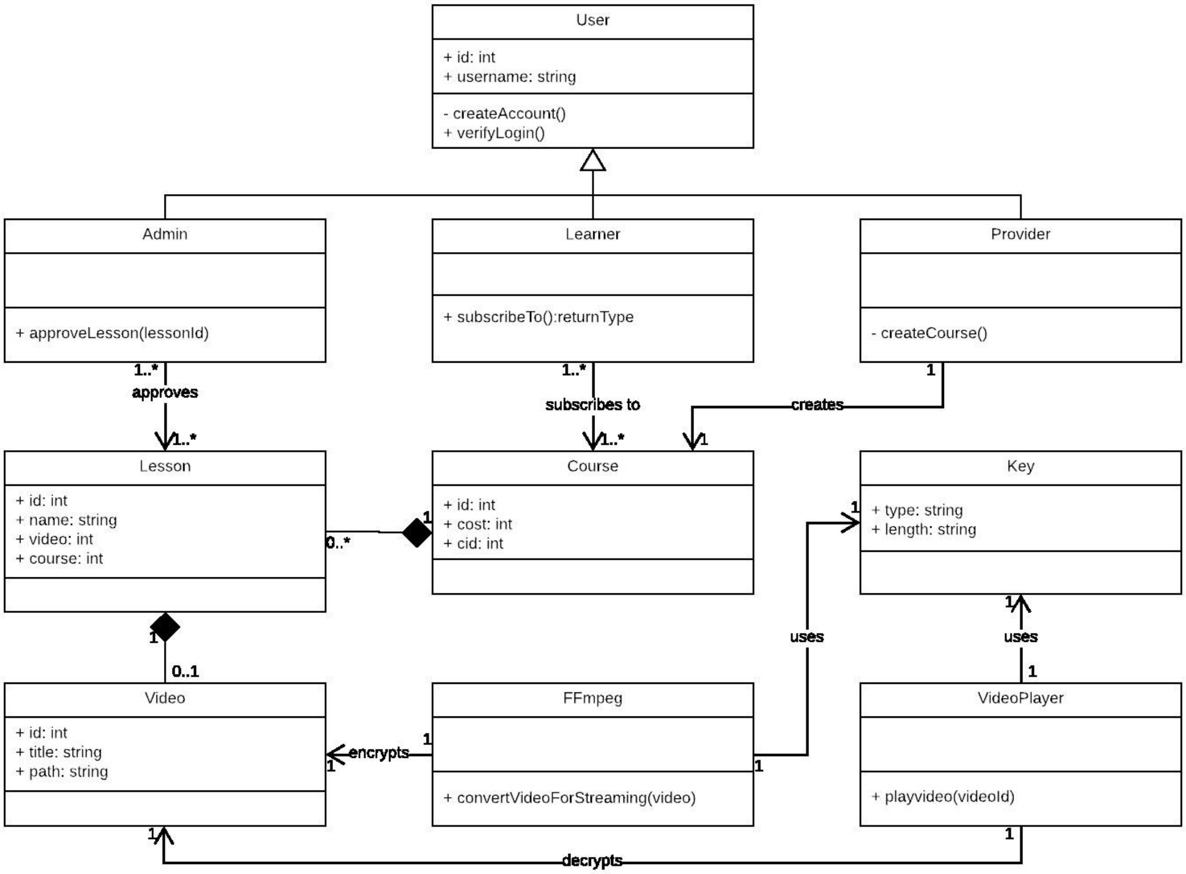


Figure 4.4 Class Diagram

4.4.5 Database Schema

The video streaming DRM system organizes its data in various tables as demonstrated by Figure 5.4. This organization allows all groups of users to conveniently navigate through the system with minimal interference. For instance, lessons table by Providers are organized under Syllabus and Week tables which are used to organize the data.

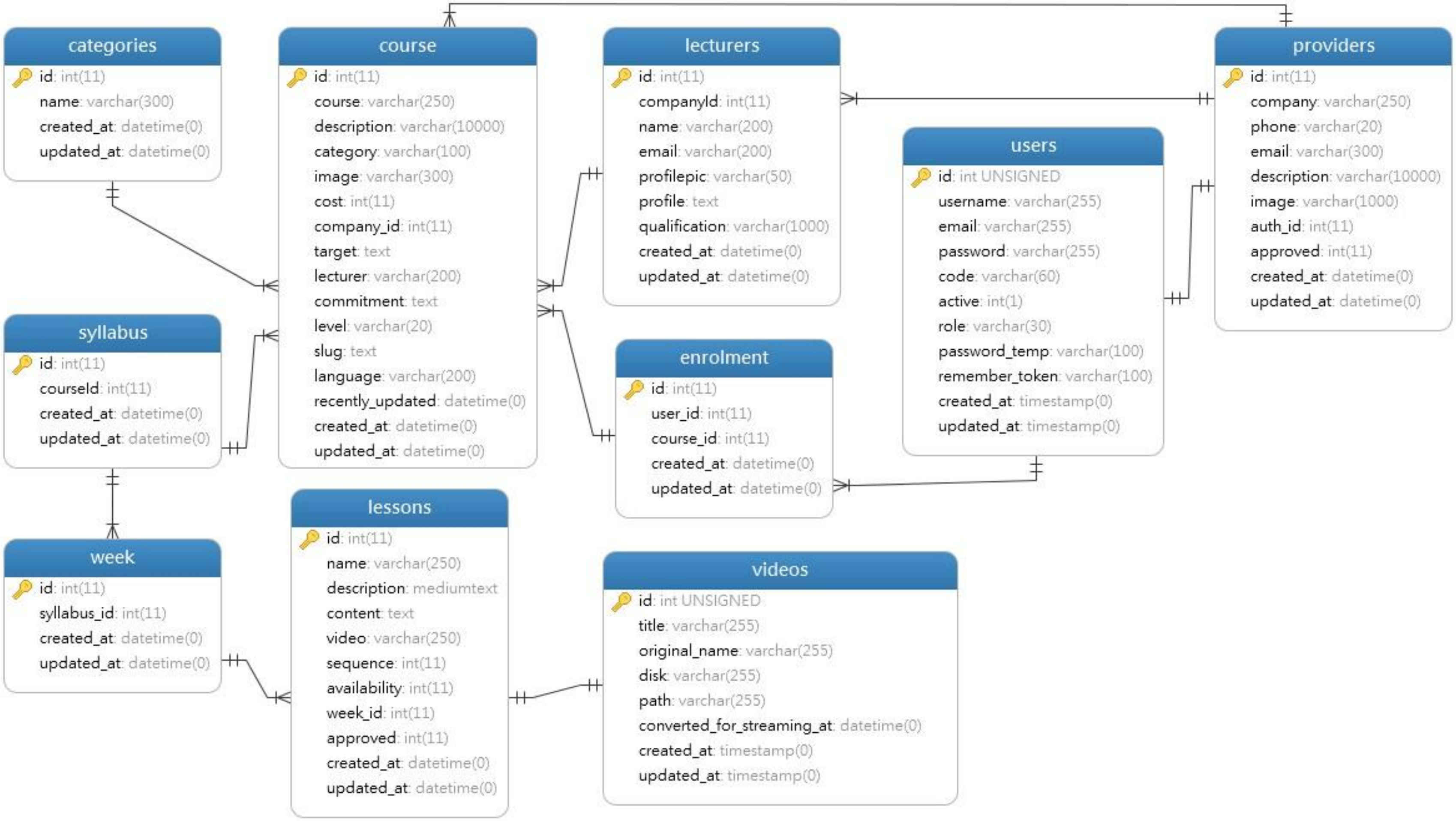


Figure 4.5 Entity Relationship Diagram

The tables below describe the main attributes of the tables contained in the diagram. Some tables have foreign keys that shall also be pointed out.

Users Table

Table 4.6 shows the users table. Users must create accounts in order to access restricted pages on the system.

Table 4.6 Users Table

Field	Data Type	Details	Notes
Id	int	PK, AI	Serves as the Primary Key for the Users table. Auto Increments for each new record
email	varchar	Unique	The email field is used as an identifier during logging in. A valid email address is also required during registration
password	varchar		
Role	varchar		The system has three categories of users, learners (default), administrators and providers.

Providers Table

Table 4.7 shows the providers table. Registered users who wish to provide content to the system become providers once approved

Table 4.7 Providers Table

Field	Data Type	Details	Notes
Id	int	PK, AI	Serves as the Primary Key for the Providers table. Auto Increments for each new record.
auth_id	int	FK	Foreign Key, references the Primary Key of Users table.
approved	int		Has a default value of 0. Increments to 1 if approved by system administrators.

Course Table

Table 4.8 shows the course table. Courses are created by providers. Each course has to fall under a category and is assigned to a specified lecturer.

Table 4.8 Course Table

Field	Data Type	Details	Notes
Id	int	PK, AI	Serves as the Primary Key for the Course table. Auto Increments for each new record.
category	int	FK	Foreign Key, references the Primary Key of Categories table.
company_id	int	FK	Foreign Key, references the Primary Key of Providers table.
lecturer	int	FK	Foreign Key, references the Primary Key of Lecturers table.

Categories Table

The categories table is used to classify courses under various disciplines to aid in system navigability. Table 4.9 illustrates this database table.

Table 4.9 Categories Table

Field	Data Type	Details	Notes
Id	Int	PK, AI	Serves as the Primary Key for the Categories table. Auto Increments for each new record.
name	Varchar		The name of a specific discipline

Lecturer Table

Lecturer profiles are created by providers. The details are added to the course overview page to provide more details to users on courses before subscribing. Table 4.10 shows this database table.

Table 4.10 Lecturers Table

Field	Data Type	Details	Notes
Id	int	PK, AI	Serves as the Primary Key for the Lecturers table. Auto Increments for each new record.
companyId	int	FK	Foreign Key, references the Primary Key of Providers table.
Name	varchar		

Enrolment Table

Table 4.11 illustrates the Enrolment table. Before users can gain access to courses, they must subscribe to them. This table holds the subscription status and is checked by the system each time a user tries to access a course.

Table 4.11 Enrolment Table

Field	Data Type	Details	Notes
Id	int	PK, AI	Serves as the Primary Key for the Enrolment table. Auto Increments for each new record.
user_id	int	FK	Foreign Key, references the Primary Key of Users table.
course_id	int	FK	Foreign Key, references the Primary Key of Course table.

Syllabus Table

The Syllabus table helps in organising the content under courses. Weeks and lessons that are created by various providers for a specific course all fall under a specified syllabus. Entries are automatically generated by the system. Table 4.12 illustrates this database table. *Table 4.12 Syllabus Table*

Field	Data Type	Details	Notes
Id	int	PK, AI	Serves as the Primary Key for the Syllabus table. Auto Increments for each new record.
course_id	int	FK	Foreign Key, references the Primary Key of Course table.

Week Table

Providers organise content into weeks. Content is comprised of lessons. Table 4.13 illustrates this database table.

Table 4.13 Week Table

Field	Data Type	Details	Notes
Id	int	PK, AI	Serves as the Primary Key for the Week table. Auto Increments for each new record.
syllabus_id	int	FK	Foreign Key, references the Primary Key of Syllabus table.

Lessons Table

Lessons table hold information pertaining to lessons which fall under specified weeks. The Lessons table also points to a specific video that users shall stream. Table 4.14 shows this database table.

Table 4.14 Lessons Table

Field	Data Type	Details	Notes
Id	int	PK, AI	Serves as the Primary Key for the Lessons table. Auto Increments for each new record.
week_id	int	FK	Foreign Key, references the Primary Key of Week table.
Name	varchar		
Video	int	FK	Foreign Key, references the Primary Key of Videos table.
Content	text		

Videos Table

The videos table holds all data on the uploaded videos including the original name before encryption and the name under which the unencrypted video is stored in the database. Table 4.15 shows this database table.

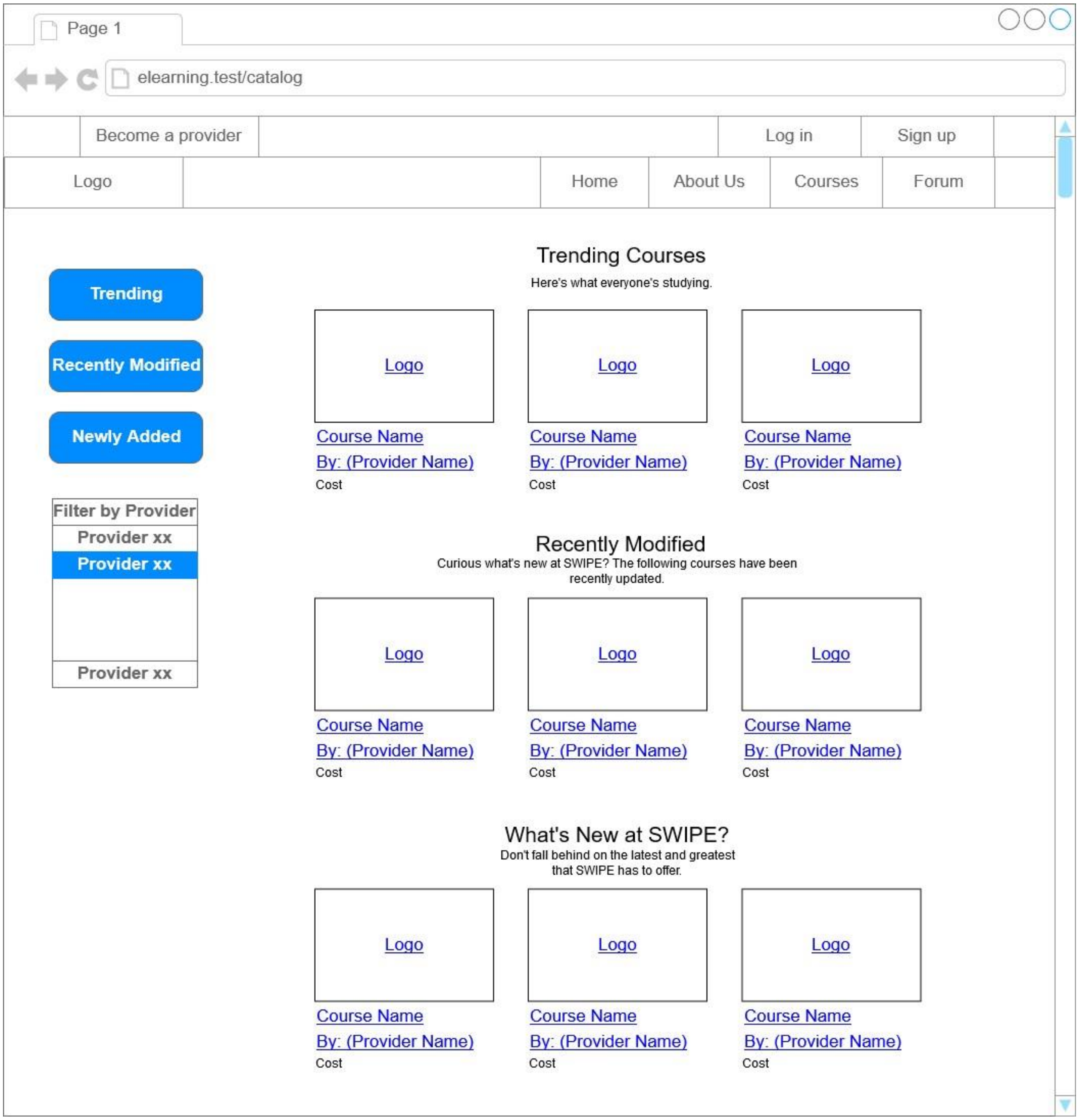
Table 4.15 Videos Table

Field	Data Type	Details	Notes
Id	Int	PK, AI	Serves as the Primary Key for the Videos table. Auto Increments for each new record.
Title	varchar		New randomly generated characters
original_name	varchar		Name used to upload the video
path	varchar		Storage URL

4.4.6 Wireframe Diagrams

Catalogue Page

Figure 4.6 shows the catalogue page where all courses created by providers are listed. Courses can be ordered according to trending (accessed by a lot of users), recently updated by providers and according to newly created courses. Users can also see the subscription cost associated with each course. The “Become a provider” link is clearly visible and persistent on every page. Interested users can start uploading content by applying through this link.



Here's what everyone's studying.

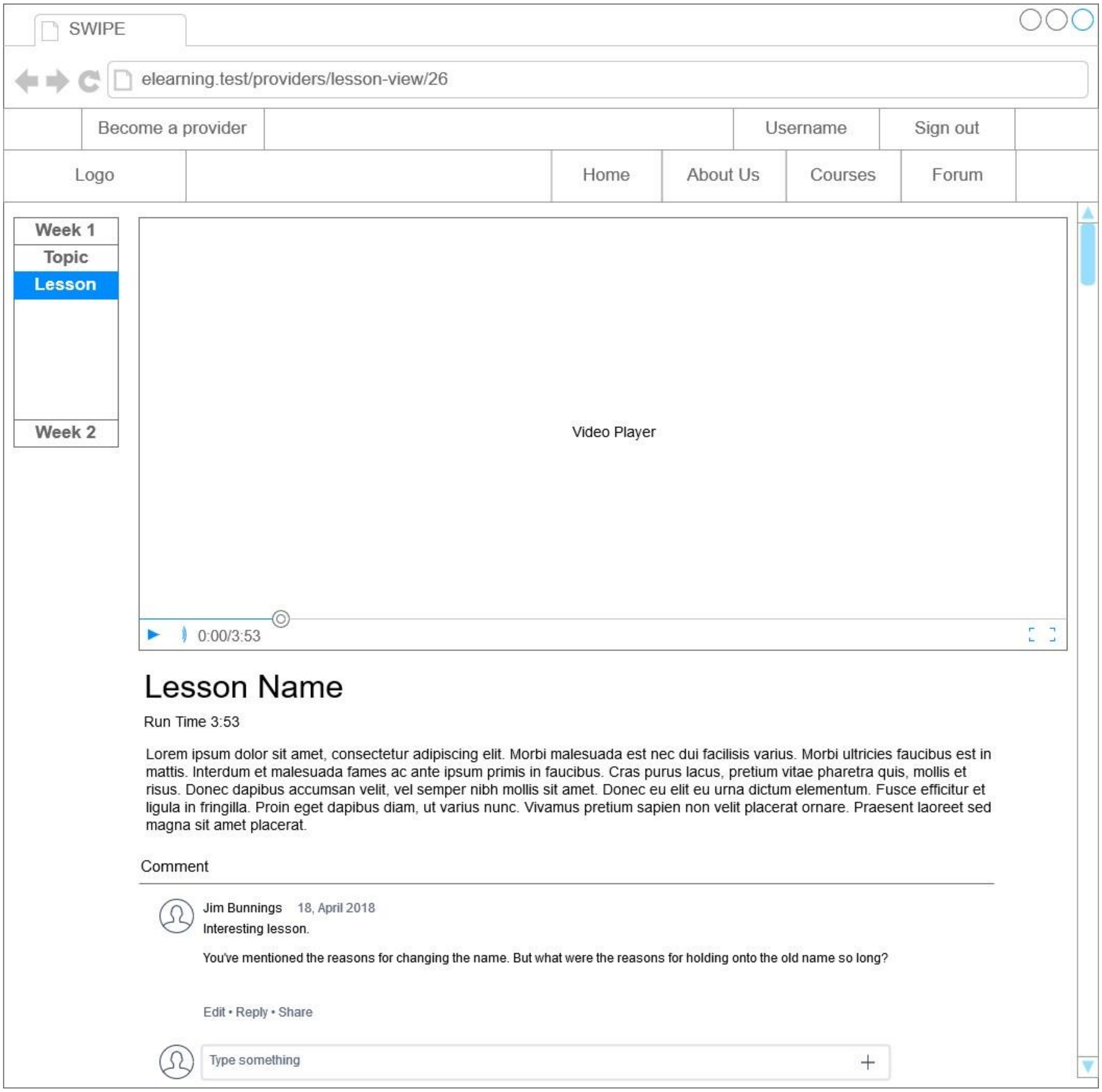
Curious what's new at SWIPE? The following courses have been recently updated.

Don't fall behind on the latest and greatest that SWIPE has to offer.

Figure 4.6 Catalogue Page

Video Player

Figure 4.7 shows a wireframe diagram of the page learners use to gain access to the video resources. The page is divided into four main sections. The first section is the tab that is left to the video player. The tab provides an overview of the week, topic and lesson that a learner is currently undertaking. The second section is the video player. The player decrypts the video segments and allows users to view the content. The third section is the lesson overview where details of the lesson are displayed. The final section is the comment section where users can engage with each other in discussions related to the lesson.



Lesson Name

Run Time 3:53

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi malesuada est nec dui facilisis varius. Morbi ultricies faucibus est in mattis. Interdum et malesuada fames ac ante ipsum primis in faucibus. Cras purus lacus, pretium vitae pharetra quis, mollis et risus. Donec dapibus accumsan velit, vel semper nibh mollis sit amet. Donec eu elit eu urna dictum elementum. Fusce efficitur et ligula in fringilla. Proin eget dapibus diam, ut varius nunc. Vivamus pretium sapien non velit placerat ornare. Praesent laoreet sed magna sit amet placerat.

Jim Bunnings 18, April 2018
Interesting lesson.

You've mentioned the reasons for changing the name. But what were the reasons for holding onto the old name so long?

Figure 4.7 Video Streaming Page

Chapter 5 System Implementation and Testing

5.1 Introduction

This chapter discusses the implementation of the video streaming DRM system and highlights the significant features. These features were obtained as a result of the evolutionary prototype phase. This section shall include screenshots of important user interfaces and tests that were carried out on the system, which shall also be discussed in this section.

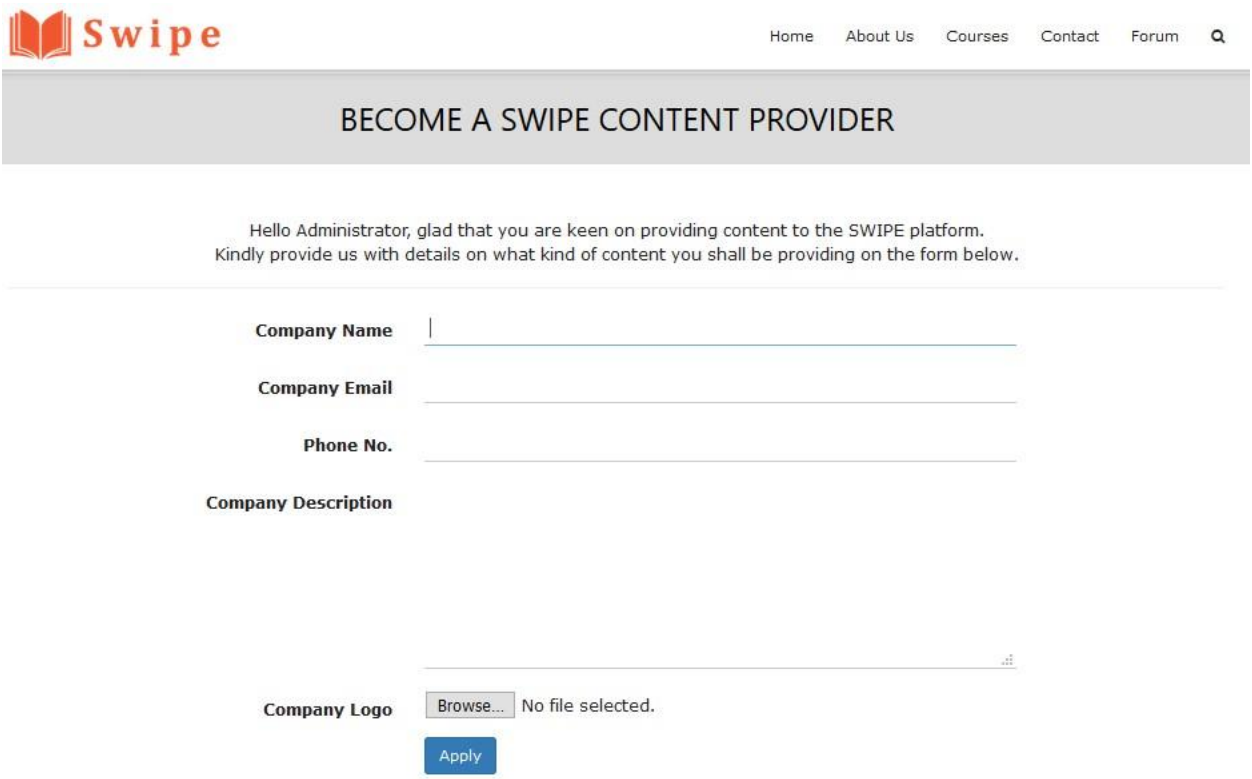
5.2 Implementation Environment

The system's backend was developed and implemented using PHP v7.1.1. Apart from being free with no licensing costs, the language possesses the trait of being able to interact with a wide range of database languages, including MySQL which was also used for this project. Both PHP and MySQL are compatible with Apache server (also used in the project) which has versions that can run on Windows, Linux and Unix servers. The front-end was implemented using HTML5, which is the fifth and current major version of the HTML standard. HTML5 was chosen mainly because of its support for HTTP Live Streaming, which is an instrumental part of the system.

The development of the system was also supported by Laravel v5.4 framework. Laravel is a free, open-source PHP web framework that can be used to develop web applications that follow the Model-View-Controller (MVC) architectural pattern that is Symfony (upshotmediagroup, 2018). Symfony is a set of reusable PHP components (symfony, 2018). The framework used for the frontend was Bootstrap. Bootstrap is a free front-end framework for fast web development; it includes both HTML and CSS based design templates for typography, forms, buttons, tables, navigation, modals, image carousels and many other, as well as optional JavaScript plugins (w3schools, 2018). The system's implementation follows the modules illustrated in the Design phase. These modules shall be illustrated in detail below through the aid of screenshots.

5.2.1 Registration

Users on the system can access restricted pages by creating accounts. They shall be presented with a standard HTML form which they can use to input their details. Once the account is created an email is sent to their email accounts with a link which, when followed, activates their accounts. Registered users can switch their roles and become content providers through the conveniently placed "Become a provider" tab. This option allows them to set up their company profile along with an image. If approved by an administrator, these users' roles will be elevated, and they will gain access to course editing pages, which also allow them to upload pictures and video files.
Figure 5.1 shows the application page.



BECOME A SWIPE CONTENT PROVIDER

Hello Administrator, glad that you are keen on providing content to the SWIPE platform.
Kindly provide us with details on what kind of content you shall be providing on the form below.

Company Name

Company Email

Phone No.

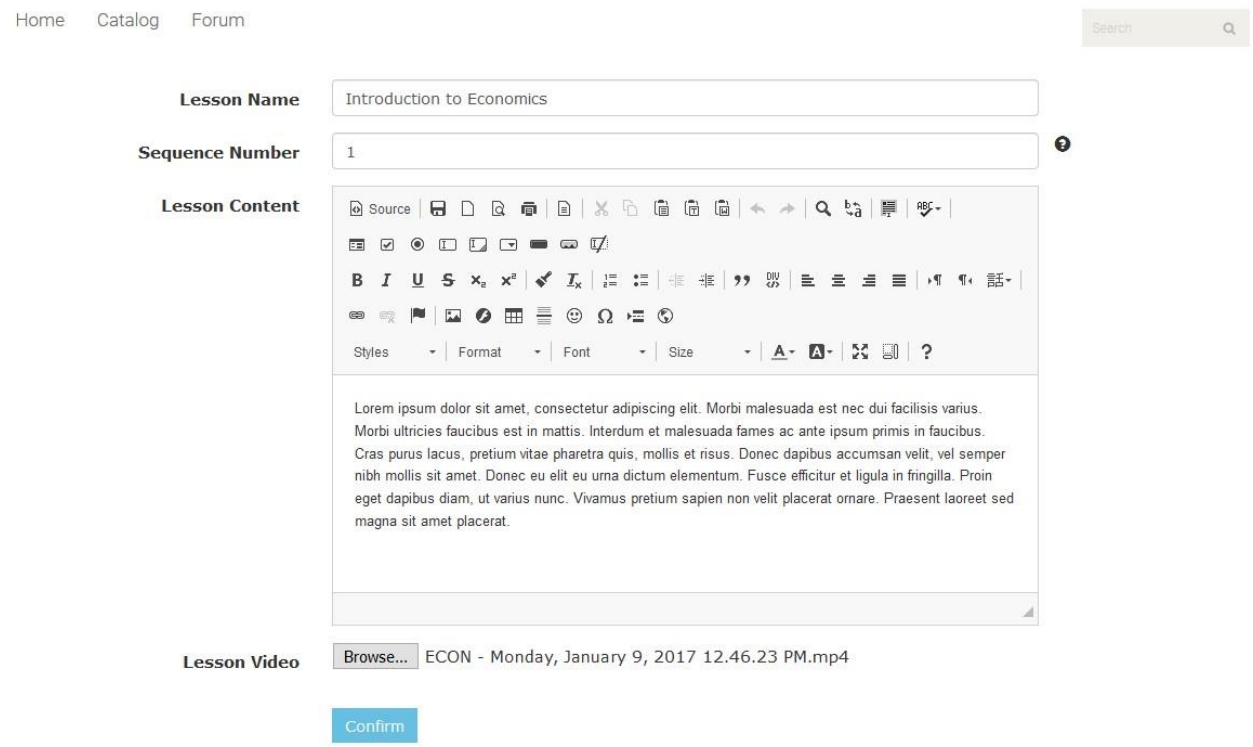
Company Description

Company Logo Browse... No file selected.

Figure 5.1 Provider Application Form

5.2.2 Video Upload and Encryption

Video upload is carried out by a content creator. This user navigates to the lesson editing page which is a HTML form that accepts text inputs as well as video files. The form is illustrated by Figure 5.2.



Lesson Name: Introduction to Economics

Sequence Number: 1

Lesson Content:

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi malesuada est nec dui facilisis varius. Morbi ultricies faucibus est in mattis. Interdum et malesuada fames ac ante ipsum primis in faucibus. Cras purus lacus, pretium vitae pharetra quis, mollis et risus. Donec dapibus accumsan velit, vel semper nibh mollis sit amet. Donec eu elit eu urna dictum elementum. Fusce efficitur et ligula in fringilla. Proin eget dapibus diam, ut varius nunc. Vivamus pretium sapien non velit placerat ornare. Praesent laoreet sed magna sit amet placerat.

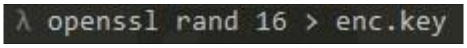
Lesson Video: ECON - Monday, January 9, 2017 12.46.23 PM.mp4

Figure 5.2 Lesson Creation Form

Once the user submits the form, its contents are posted to a "providersEditLessonPost" function under a controller called "ProvidersController." This function takes two arguments, the "StoreVideoRequest" class that handles the file's validation and the form request class to access the user's input. The StoreVideoRequest class checks the form for the field with the name 'video' and verifies that the file is encoded in mime of type video/mp4. Once both the user inputs and the video file have been verified, the controller calls the store method to upload the video file, save it to the database and dispatch the "ConvertVideoForStreaming" job which takes the video instance as an argument.

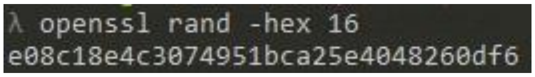
The ConvertVideoForStreaming job handles all the aspects of preparing the video for streaming and encrypting through the FFmpeg library which should be installed on the host machine. The encryption process encodes the uploaded video file to ensure only authorised parties would be able to view it; therefore, requires a secret key and an encryption algorithm; Advanced Encryption Standard (AES) for this case. An Initialisation Vector (IV) is also required to encrypt the first block.

The encryption key was generated using OpenSSL, which generated a key file “enc.key”. The IV was also generated using OpenSSL. Figures 5.3 and 5.4 show these processes.



```
λ openssl rand 16 > enc.key
```

Figure 5.3 OpenSSL Key Generation



```
λ openssl rand -hex 16
e08c18e4c3074951bca25e4048260df6
```

Figure 5.4 OpenSSL IV Generation

The next step was to create a key info file. This file holds information on the key used, the URI to the key and the IV. These details are used by the FFmpeg library during the encryption process. The file is written according to the format below;

Key URI
Path to key file
IV

The first line defines the URI of the key. This information shall be written to the playlist and as shall be later shown, is important to allow the video player to be able to decrypt the files. The second line defines the path to the file which has the encryption key and the third line is the initialisation vector.

The video is first retrieved from storage then filtered with the following options;

i. hls_time (seconds): this option sets the length of the target segments. A value of 60 seconds is chosen for this step.
ii. hls_playlist_type vod: This option emits the #EXT-X-PLAYLIST-TYPE:VOD in the m3u8 header
iii. hls_key_info_file: This option allows for the use of the information in the provided file for segment encryption

Each generated segment is then stored in a separate location from the original unencrypted video file. Once the process is complete, a master playlist file in .m3u8 extension is generated. The file is in the following format;

#EXTM3U

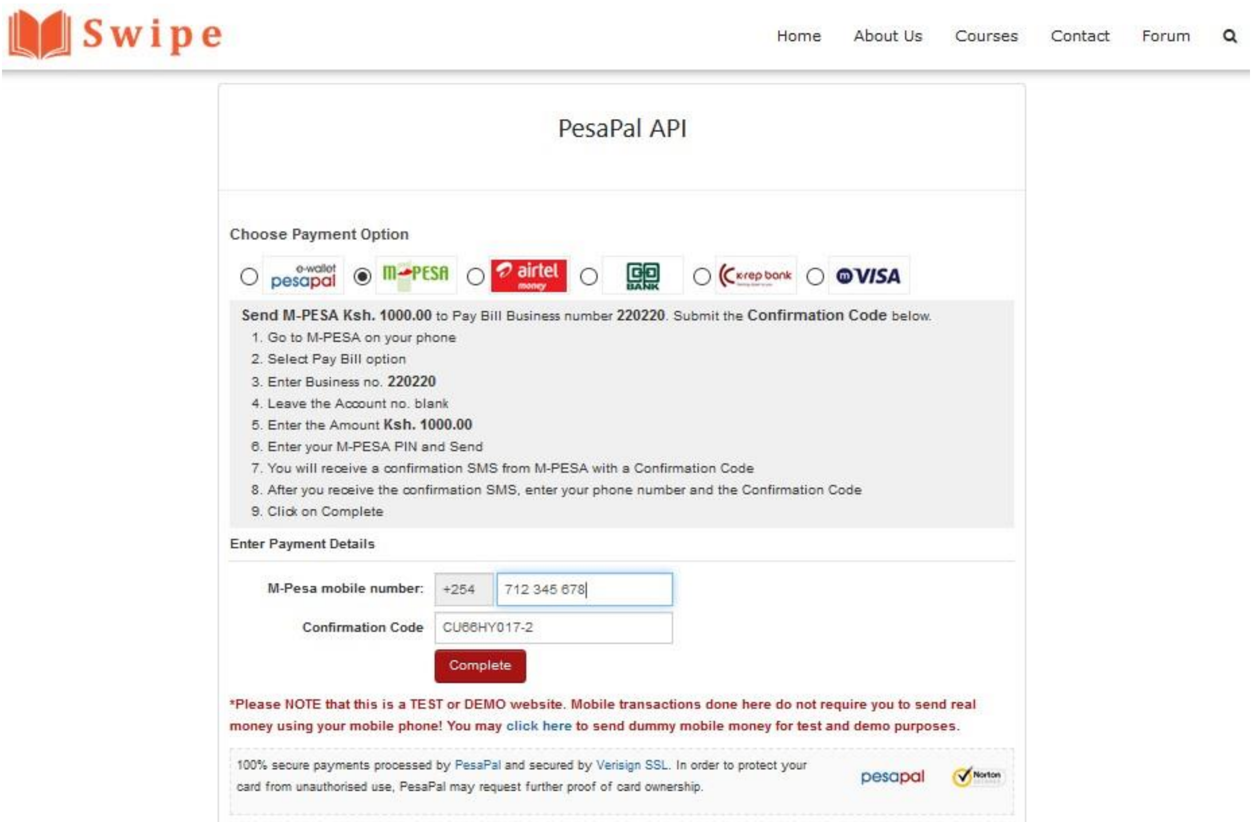
```
#EXT-X-VERSION:3
#EXT-X-TARGETDURATION:29
#EXT-X-MEDIA-SEQUENCE:0
#EXT-X-PLAYLIST-TYPE:VOD
#EXT-X-KEY:METHOD=AES-128,URI="https://urltodomain.com/keyfile",IV=0x
e08c18e4c3074951bca25e4048260df6
#EXTINF:28.333333,
1234.ts
#EXT-X-ENDLIST
```

It is worth noting the URI of the encryption key. The HTML5 video player shall retrieve the key from this specified location to decrypt the media segments. It is advisable to serve the key over **HTTPS.** It is a well-known statement that “Cryptographic security must rely on a secrecy of a key instead of a secret algorithm.” In a live environment, the key should be served over HTTPS to protect it from eavesdroppers.

Once the job is complete, it updates the Videos table in the RDBMS with the name of the generated playlist file. The job exits and returns to the Controller. The controller then updates the Videos table with data for the other columns and returns an “Update Successful” message.

5.2.3 Course Subscription

PesaPal API was integrated to handle user payments. When users try to access courses that have a cost associated to them and that they had not previously subscribed to, they shall be redirected to PesaPal’s payment page which is depicted by Figure 5.5. If the users successfully deposit the prescribed amount, they shall be redirected to the course’s home page and met with a “subscription successful” message.



PesaPal API

Choose Payment Option

○ e-wallet pesapal ● M-PESA ○ airtel money ○ BANK ○ K-rep bank ○ VISA

Send M-PESA Ksh. 1000.00 to Pay Bill Business number 220220. Submit the Confirmation Code below.

1. Go to M-PESA on your phone
2. Select Pay Bill option
3. Enter Business no. 220220
4. Leave the Account no. blank
5. Enter the Amount Ksh. 1000.00
6. Enter your M-PESA PIN and Send
7. You will receive a confirmation SMS from M-PESA with a Confirmation Code
8. After you receive the confirmation SMS, enter your phone number and the Confirmation Code
9. Click on Complete

Enter Payment Details

M-Pesa mobile number:	+254 712 345 678
Confirmation Code	CU66HY017-2

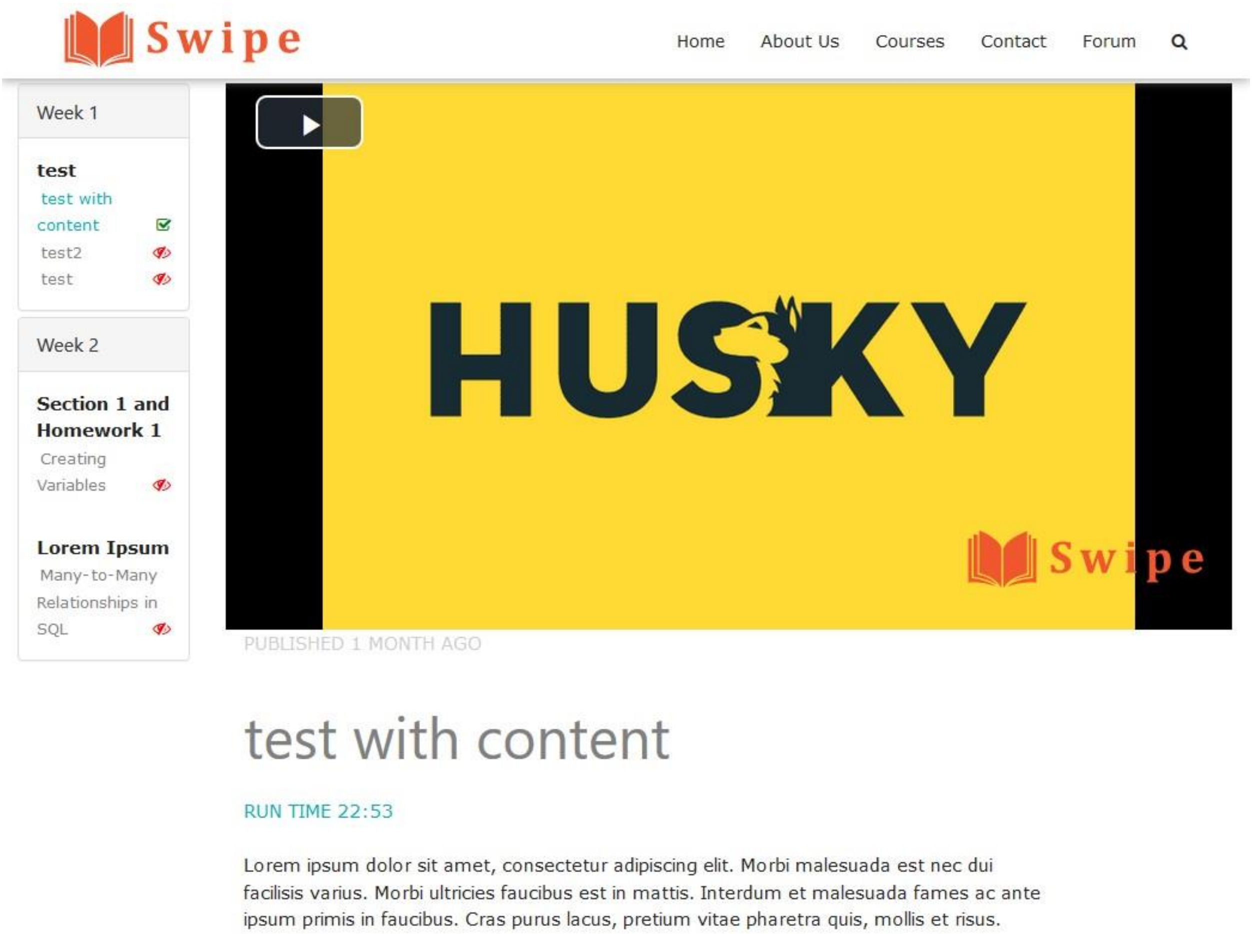
*Please NOTE that this is a TEST or DEMO website. Mobile transactions done here do not require you to send real money using your mobile phone! You may click here to send dummy mobile money for test and demo purposes.

100% secure payments processed by PesaPal and secured by Verisign SSL. In order to protect your card from unauthorised use, PesaPal may request further proof of card ownership.

Figure 5.5 PesaPal API

5.2.4 Encrypted Video Streaming

Figure 5.6 shows the webpage through which learners can access course lessons. The previously mentioned manifest file is used by the video player to get all information relating to the stream. This includes information on the location of the AES key that was used to encrypt the segments. The video player shall therefore make a HTTP(S) request to the specified URL which retrieves the key file. Once retrieved, the segments are decrypted in the order specified by the manifest file. The player must retrieve the key each time it has to decrypt a new segment. The process is fast and there is no perceivable lag to the end-user.



test with content

RUN TIME 22:53

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi malesuada est nec dui facilisis varius. Morbi ultricies faucibus est in mattis. Interdum et malesuada fames ac ante ipsum primis in faucibus. Cras purus lacus, pretium vitae pharetra quis, mollis et risus.

Figure 5.6 Video.js Video Player

The system also displays a water mark at the bottom-right edge of the video player in the form of a logo. The purpose of this watermark is to identify content from the system in the event that it is copied through screen capture tools and leaked through the Internet. This would warrant an investigation into the source of the leak and any legal measures.

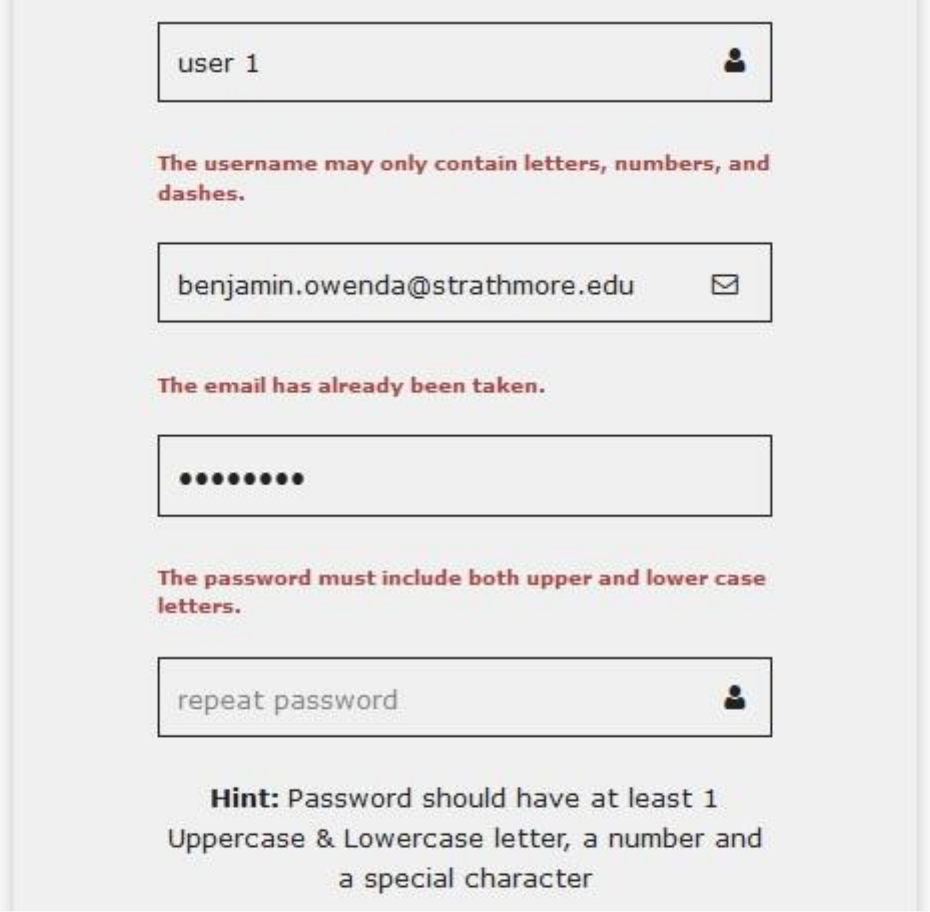
5.3 System Testing

The purpose of the testing was to ascertain that the developed system operates as expected. Unit, Compatibility, Usability and Functional tests were carried out by the developer while a few preselected end users carried out the User tests.

5.3.1 Unit Testing

Unit tests were carried out periodically throughout the development lifecycle of the system to minimize the number of issues in the final system. The individual components that were tested included the following;

i. Input Forms: Tests were carried out to ensure only the relevant data is accepted by the system. These included checking for blank inputs, type of data inserted and length of data. The system was able to validate each user input and reject any type of data that did not conform to the specified rules. Figure 5.7 shows a registration form with perceivable errors.



user 1

The username may only contain letters, numbers, and dashes.

benjamin.owenda@strathmore.edu

The email has already been taken.

••••••••

The password must include both upper and lower case letters.

repeat password

Hint: Password should have at least 1 Uppercase & Lowercase letter, a number and a special character

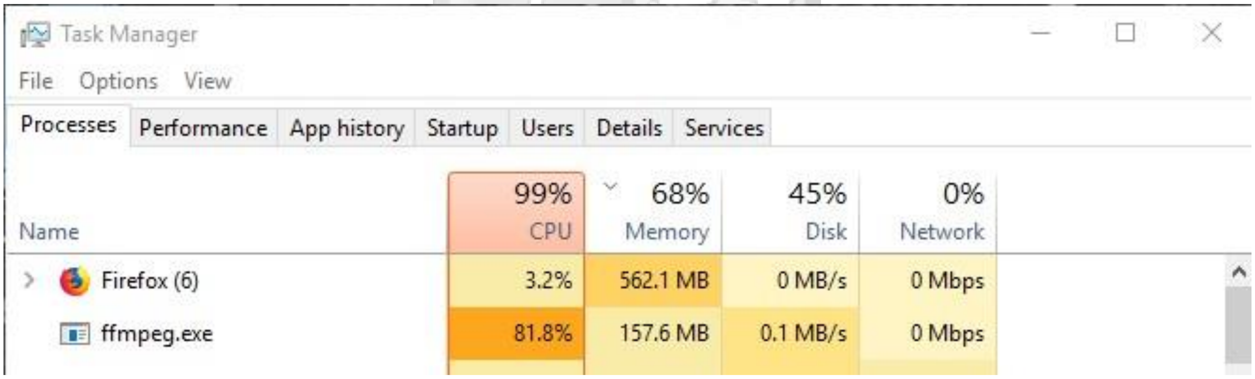
Figure 5.7 User Registration Form

ii. Algorithm: The algorithm was tested on cases where users tried to bypass validation rules. This includes cases where a user tries to access a course by typing in the URL hoping to bypass subscription requirements. The algorithm proved to be efficient at limiting such cases. The algorithm was also tested against various user roles to ascertain that only users with the specified rights could access certain pages; for example, only system administrators to access approval pages and course providers to only edit their own content. iii. Edge cases: Tests were also carried out on the PesaPal API to ascertain that users would not be able to access courses if they pay less than the prescribed amount. The API failed this test, however representatives of the company offered assurance that that behaviour is only experienced in the sandbox environment.

5.3.2 Compatibility Testing

Compatibility tests were carried out in two phases. The first instance was in the development environment while the second was on a production environment once the system was deemed stable enough to be deployed.

The system was developed on a computer running 64-bit version of Windows 10 Pro. The computer's hardware specifications were a dual core Intel Celeron(R) CPU B800 processor with a speed specification of 1.50 GHz and 4.00 GB of RAM. FFmpeg library's compatibility with this hardware was evaluated. During normal system operation, the processor usage was rated at 22% with 65% memory usage. However, using a test video with a duration of two minutes and fifty seconds with a resolution of 1280x720, it was noticed that encrypting this video using the FFmpeg media library used a considerable amount of CPU time consuming an average of 80% of it while RAM usage was not significantly affected. Figure 5.8 shows the task manager logs on the first computer.

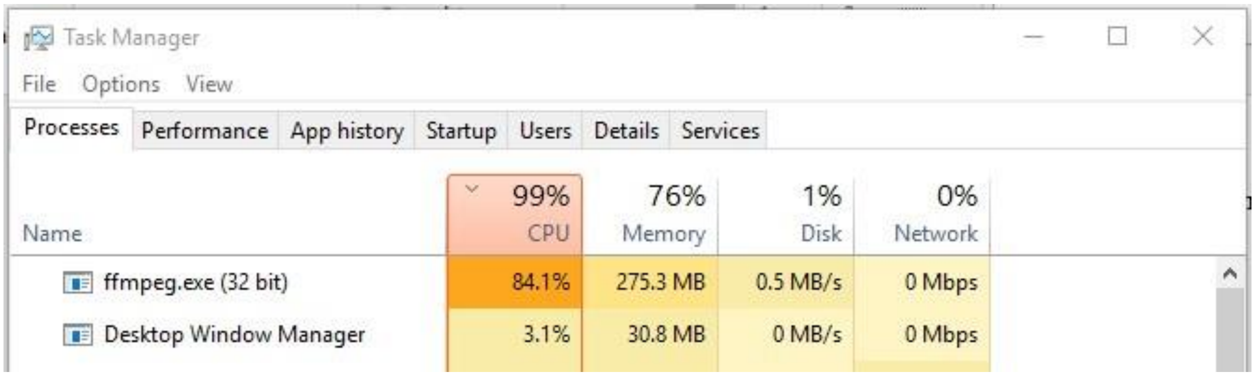

Task Manager
File Options View
Processes Performance App history Startup Users Details Services

Name	99% CPU	68% Memory	45% Disk	0% Network
Firefox (6)	3.2%	562.1 MB	0 MB/s	0 Mbps
ffmpeg.exe	81.8%	157.6 MB	0.1 MB/s	0 Mbps

Figure 5.8 FFmpeg library Processor Usage on Test PC One

The same test was carried out on a separate computer that was also running the 64-bit version of Windows 10 Pro, but with better specification which included a dual-core Intel Core i3-3240 processor rated at 3.40 GHz with 4 GB of RAM. During normal operation, the CPU averaged 5% usage and 70% memory usage. The results were however still similar to the previously tested computer with FFmpeg library's usage averaging 84.1% with no adverse effects on the RAM.

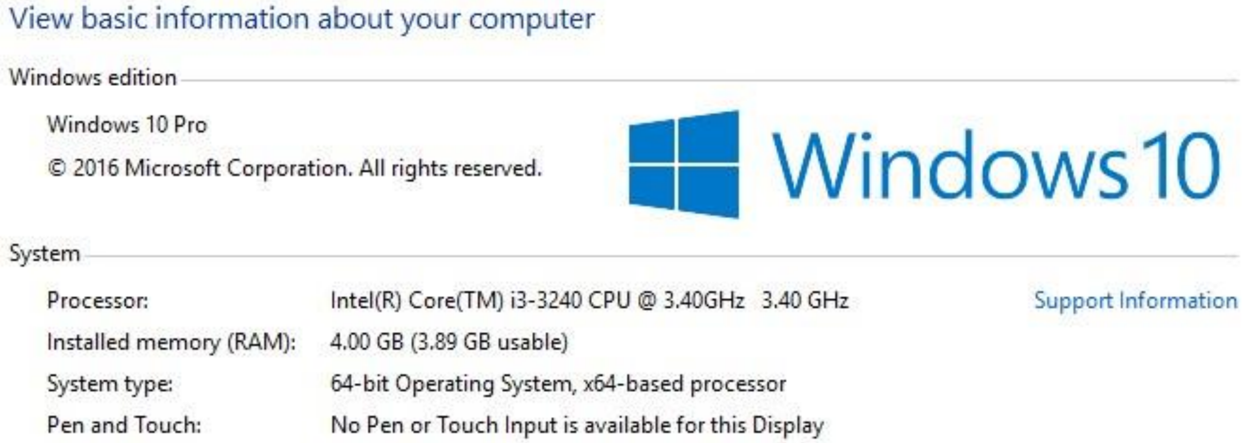
Figure 5.9 shows the task manager log on the second computer.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services

Name	99% CPU	76% Memory	1% Disk	0% Network
ffmpeg.exe (32 bit)	84.1%	275.3 MB	0.5 MB/s	0 Mbps
Desktop Window Manager	3.1%	30.8 MB	0 MB/s	0 Mbps

Figure 5.9 FFmpeg library Processor Usage on Test PC Two

Figure 5.10 shows hardware specifications of the second test computer.


View basic information about your computer

Windows edition

Windows 10 Pro

© 2016 Microsoft Corporation. All rights reserved.

System

Processor:	Intel(R) Core(TM) i3-3240 CPU @ 3.40GHz 3.40 GHz
Installed memory (RAM):	4.00 GB (3.89 GB usable)
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

Figure 5.10 Development Environment Hardware Specifications

The system was then hosted on a server running Ubuntu 16.04.3 LTS. FFmpeg library, being crossplatform, was also installed on the server with minimal difficulty. The developer then tested the system's compatibility with three major browsers namely; Google Chrome v65.0.3325.181, Firefox v59.0.2 and Microsoft Edge v38.14.393.2068.0 which were running on a 64-bit Windows 10 desktop computer. All these browsers were able to access the system. The system's compatibility was also tested on a HTC M8 mobile device running Android 6.0.1 and an iPhone 6s device running iOS 11. It is acknowledged that there exists a wider variety of mobile devices and platforms than the ones used, however the operating system architecture on majority of the devices currently in use are significantly similar and the two devices used offered a great representation of them. On both devices, the system was accessed via the native built in browsers

(HTC browser and Safari) and Google Chrome’s mobile version and they were both able to access the system and stream a sample video.

On a network with a latency of 162ms, download speed of 25.23Mbps and upload speed of 0.52Mbps, the system took an average of three seconds on every page load and an average of four seconds before starting to stream a sample video.

5.3.4 Functionality Testing

A sample video was uploaded to the system and various method were used to try and download it. One such method was use of Internet Download Manager(IDM) which is a popular file grabbing software that is used to acquire a wide range of media files from web sources including documents, audio files and videos. The file grabber displayed a popup over the frame of the video player which allowed for video download. IDM however exited with error code ‘*0x80040154’* which occurs when the grabbing software is unable to transfer the download from the browser to its scheduler. Using this test, the system passed preliminary test, however the functionality test was further explored by users to provide a wider field of view.

5.3.3 User Testing

As mentioned in section 3.3.3 of this document, User Testing had a targeted approach in selection of users. It was deemed fit for users with a background in Information Technology to explore the effectiveness of the system as this group would have a higher success of pointing out bugs and any limitations of the system compared to users without any experience in the field. The test group consisted of programmers, system analysts and various individuals in the field of Information Technology support, totalling fifteen test users. The users evaluated the system based on its usability and general intended functionality.

Information Technology Skills

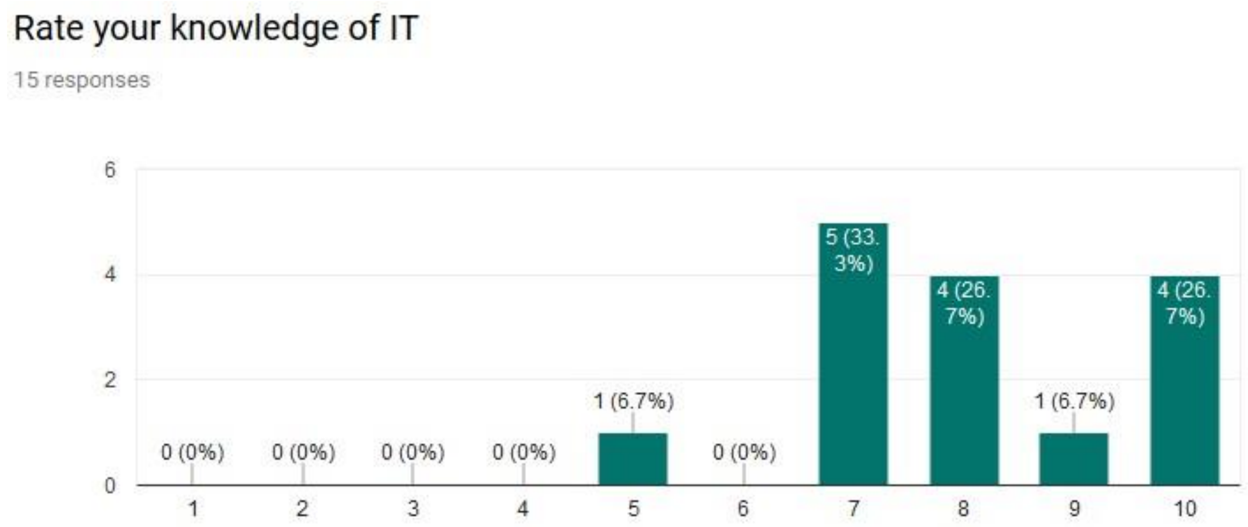


Figure 5.11 Test Users Skills in IT

Test users were first asked to rate their own knowledge of IT on a scale of one to ten. The importance of this question was to first evaluate the competencies of the users and secondly check whether the system would be able to withstand attempts to bypass the security measures by users of various skill levels. Figure 5.11 shows the result of this question. According to the figure, fourteen of the fifteen respondents evaluated themselves as having adept Information Technology skills, which was sufficient enough in evaluating the developed system.

User Compatibility Test

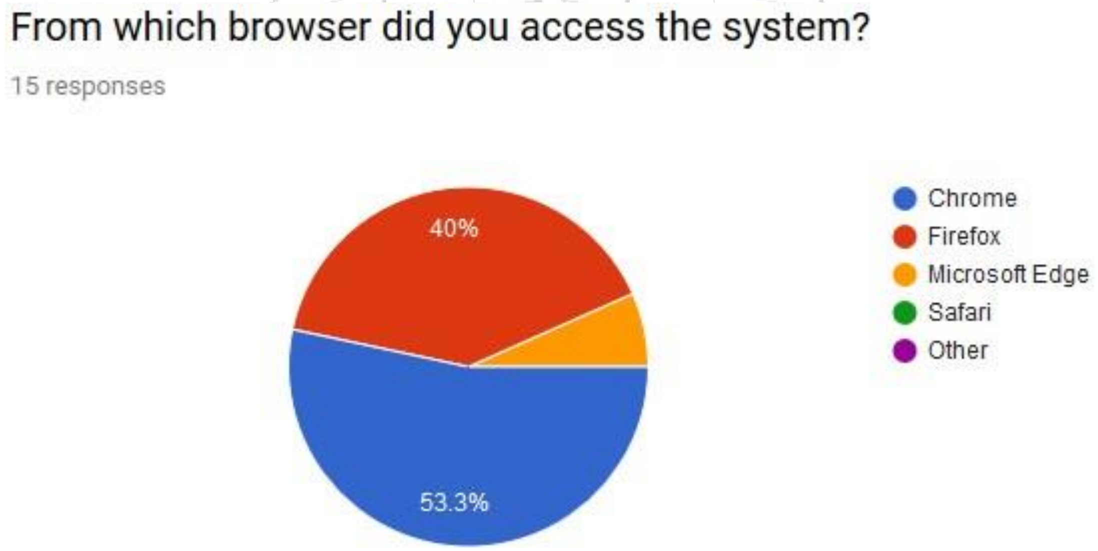


Figure 5.12 Browser Used to Evaluate System

Users were first asked to indicate the browser being used to evaluate the system. This question was aimed at identifying if any browser had any compatibility issues with the system. Google Chrome was the most popular browser with 53.3% of the fifteen users accessing the system through it. Firefox was the second most popular browser with 40% of the users using it. Microsoft Edge had 6.7% users while Safari had no user. No other browser was in use.

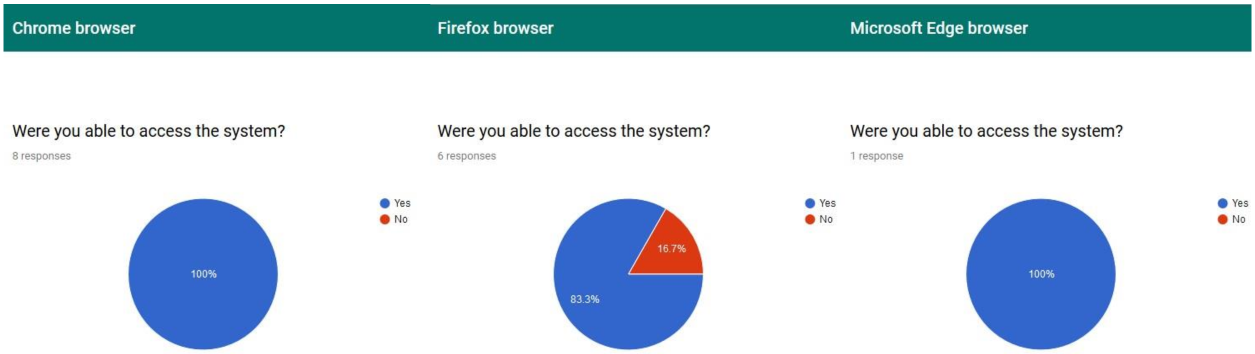


Figure 5.13 Browser Access Capability

100% of users on both Google Chrome and Microsoft Edge browsers (eight and one respectively) were able to access the system. Only 16.7% of six users on Firefox were unable to access the system, however the user(s) did not indicate the exact challenge they had. Figure 5.13 shows the Yes/No responses for browser access.

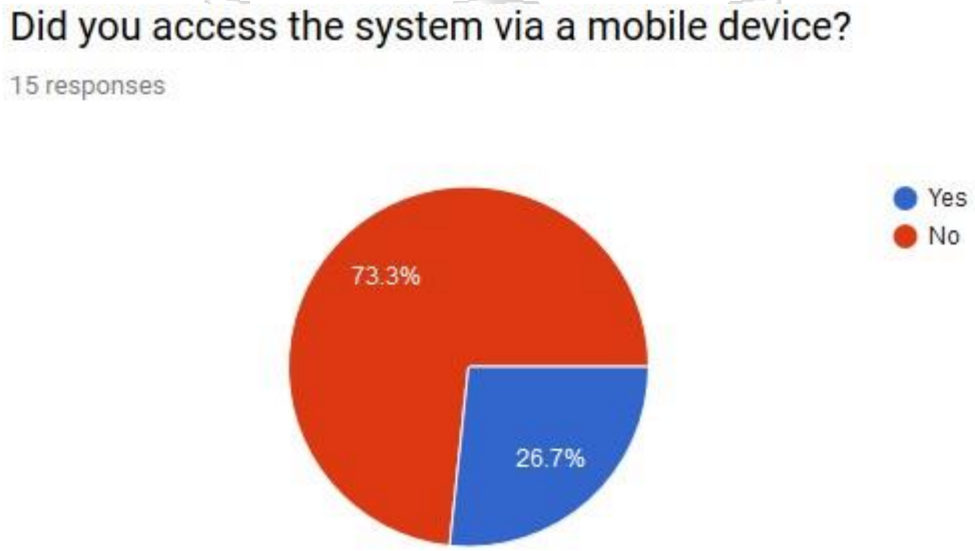


Figure 5.14 Number of Mobile Users

Of the fifteen test users, 26.7% were using mobile devices which is approximately seven users of which 71.4% of them were able to access the system. Figure 5.14 shows number of users evaluating the system using mobile devices.

Users were then asked to rate their Internet access speeds which was a preliminary question to evaluate the rate at which the system responded to requests. A slow Internet speed on the user's side would indicate that if the system's response was slow, it would be attributed to the Internet and not the system.

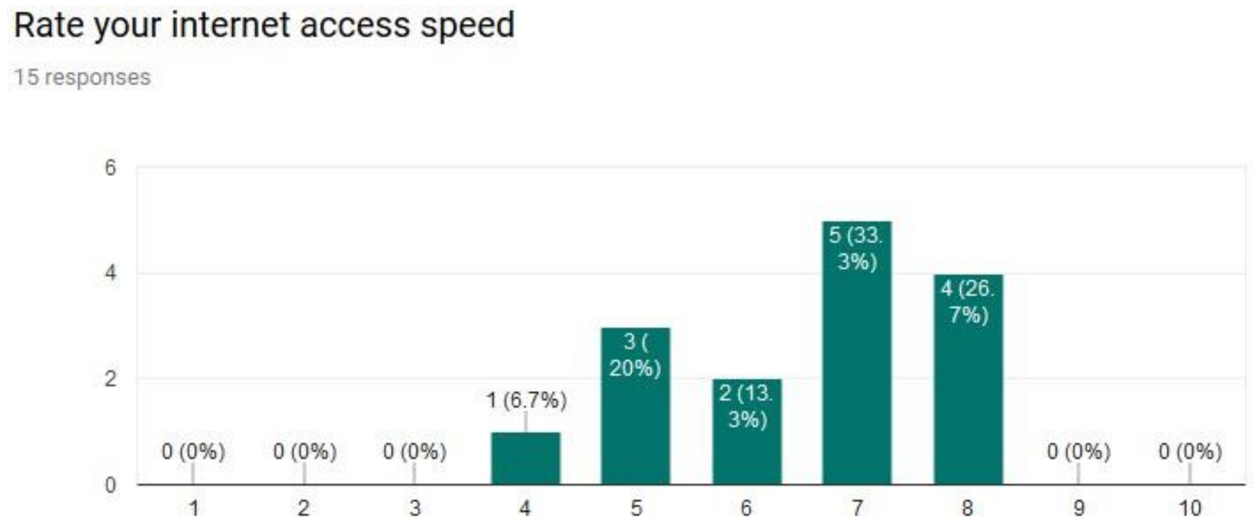


Figure 5.15 Test Users Internet Access Speed Ratings

Figure 5.15 shows the responses on Internet speed on a scale of one to ten where five of the fifteen users, who form the majority rated their Internet access speed as seven while four testers rated the access speed as eight. A total of nine out of fifteen total testers rated their Internet as being fast which formed the conclusion that the test user's Internet access speeds were fast enough to access web resources, which was a prerequisite for testing the system's network performance.

Figure 5.16 shows the same scale as before that the respondents used to rate the speed at which the system returned the requested resource. Seven of fifteen testers gave the response speed as seven which formed 46.7% of the total users. This showed that the system was usable enough on a live network environment which was confirmed by Figure 5.17 which was the next question asking whether the system overwhelmed the users' network, a question which 100% of the respondents answered 'No'.

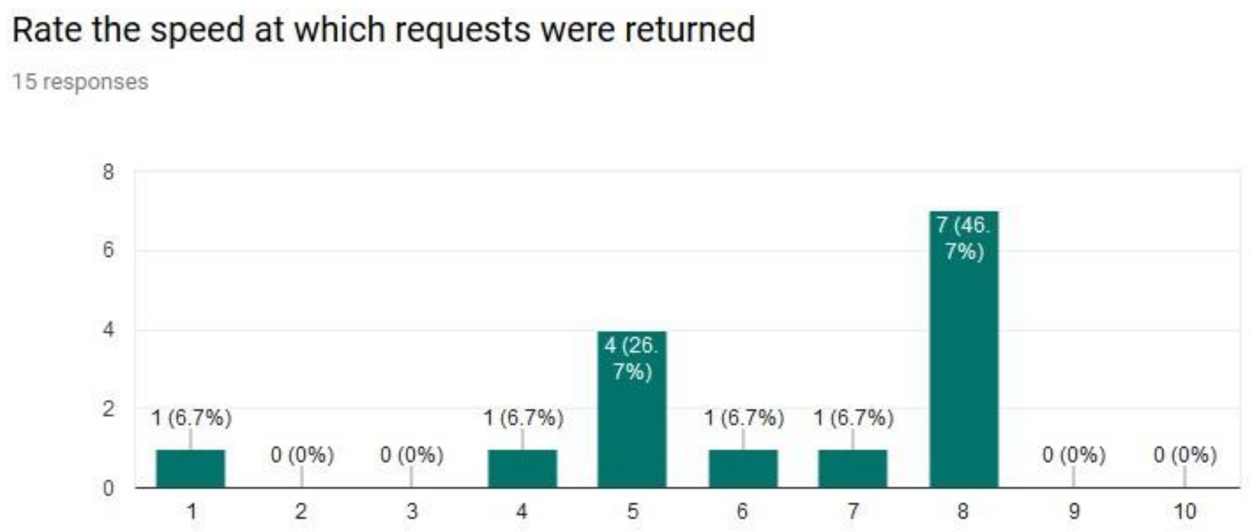


Figure 5.16 System Resource Response Rate

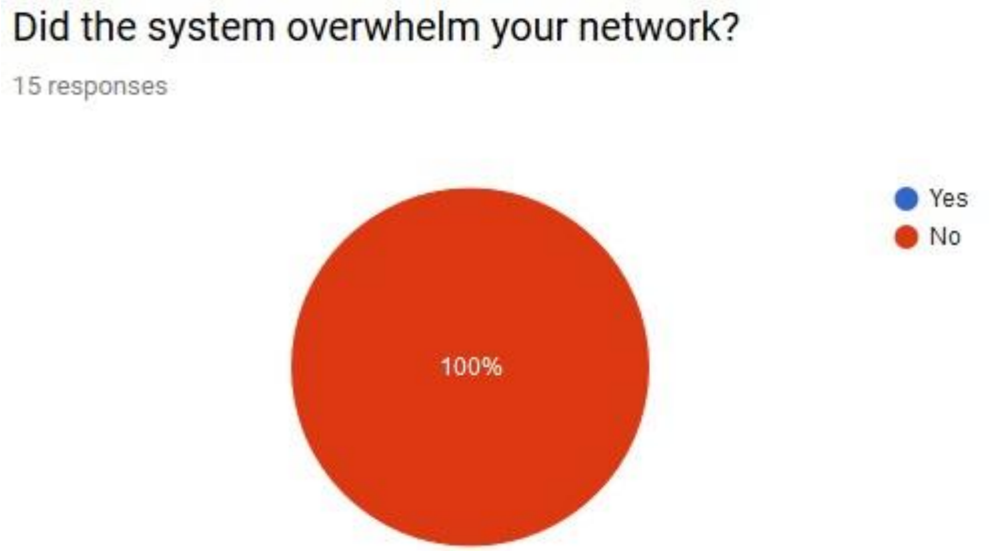


Figure 5.17 System's Compatibility with Network

User Usability Test

The system's usability was tested based on User Interface and Navigability. For the User Interface all test users rated it as being seven and above which indicated that the interface was appealing while the system's navigability, which represents ease of accessing resources, evaluation showed that eleven out of the total fifteen testers could access the intended pages with ease and access the intended resource. These results are shown by figures 5.18 and 5.19.

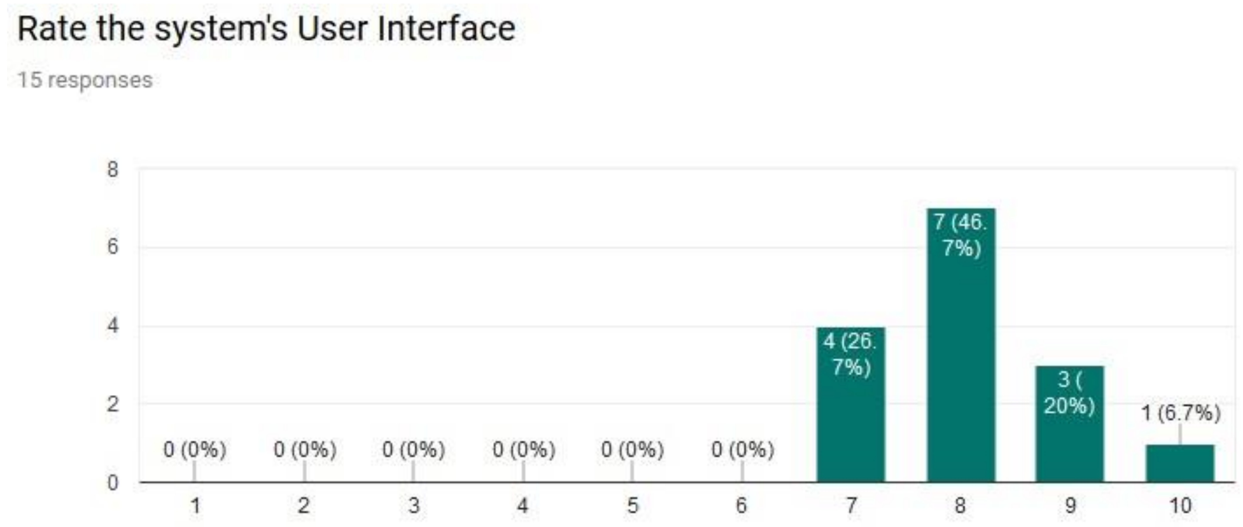


Figure 5.18 System User Interface Rating

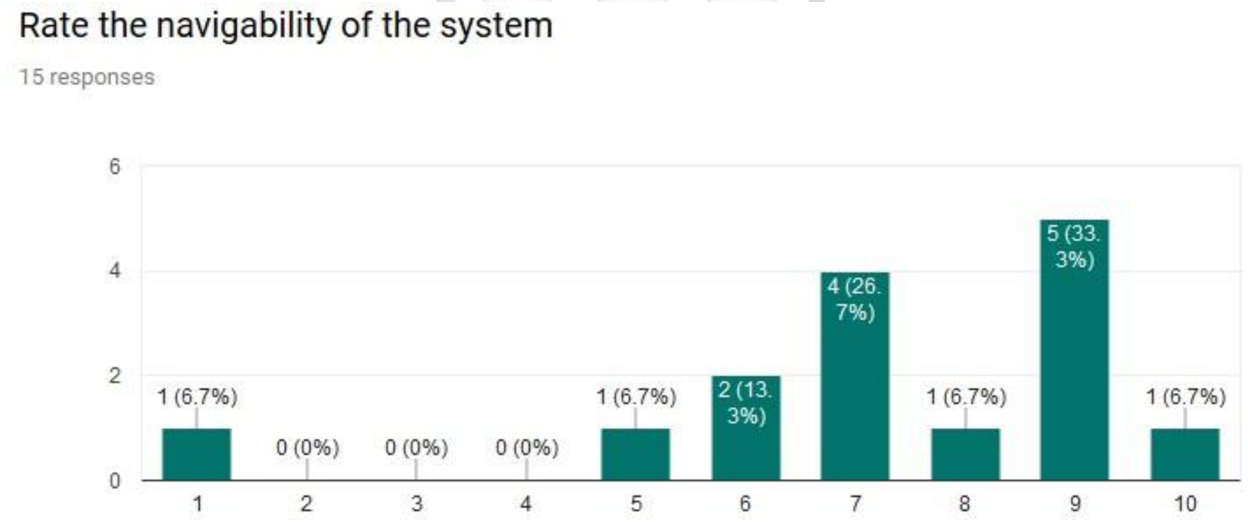


Figure 5.19 System Navigability Rating

User Functionality Test

The final tests included evaluating the system's functionality such as ability to stream videos and level at which the stream is protected by the system. The first question was evaluation of whether the testers could stream a sample video on the system, which showed 93.3% of the respondents could accomplish this task as confirmed by Figure 5.20.

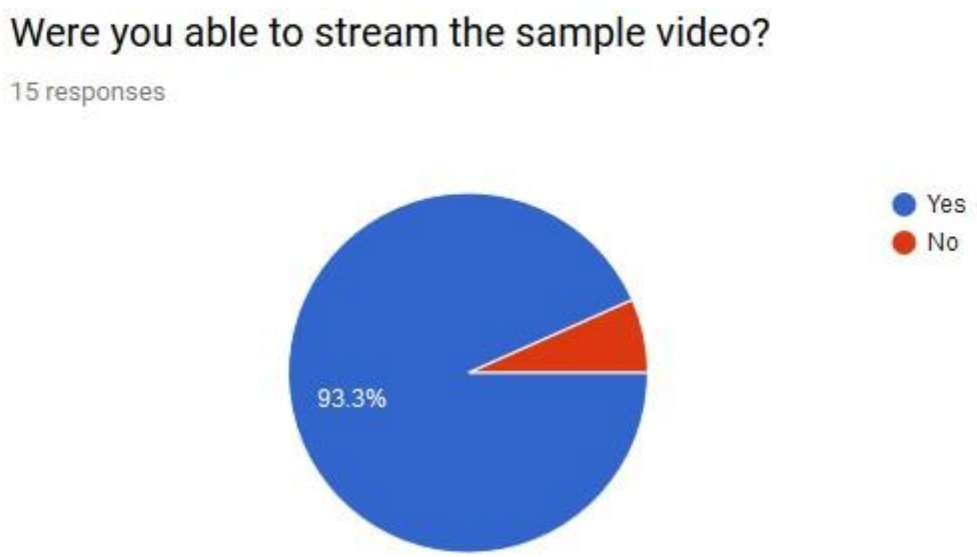


Figure 5.20 System's Stream Functionality

The respondents were also asked whether they had a file grabber installed on their computers, where 66.7% of the fifteen had at least one installed as shown by figure 5.21. Of the ones who had a file grabber installed 60% of them were using Internet Download Manager while 10% had Eagleget and ‘DAM’ downloaders installed and 20% were using Video Prime.

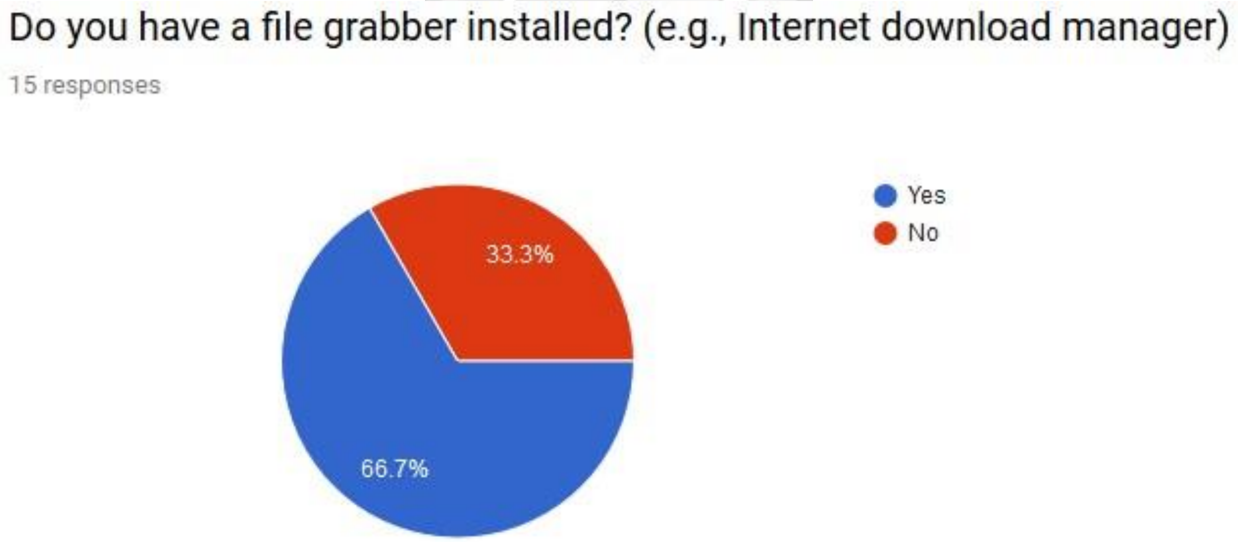


Figure 5.21 Presence of File Grabbers

Interestingly, 70% of the respondents who had file grabbers installed confirmed that their tools could not download the video stream, which meant 30% of the tools could actually download the file segments. Unfortunately, the survey did not capture whether the individuals who were able to download the stream, could play it back on their devices. However, ability to playback the segments formed part of the system's validation. Figure 5.22 shows these findings.

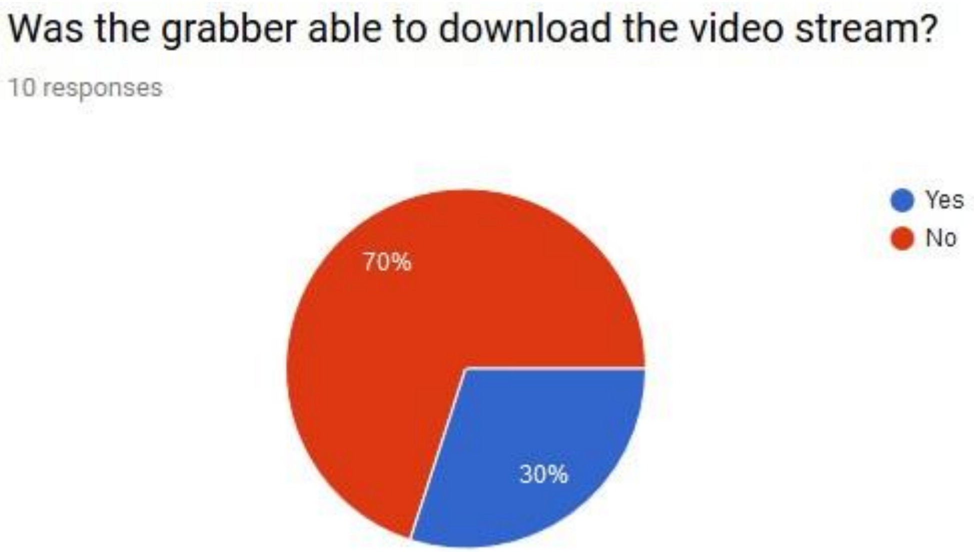


Figure 5.22 File Grabber Effectiveness

The survey also asked whether the respondents were able to download the video stream using any other method, a question that 100% of them responded to as 'No'. Figures 5.22 shows this feedback.

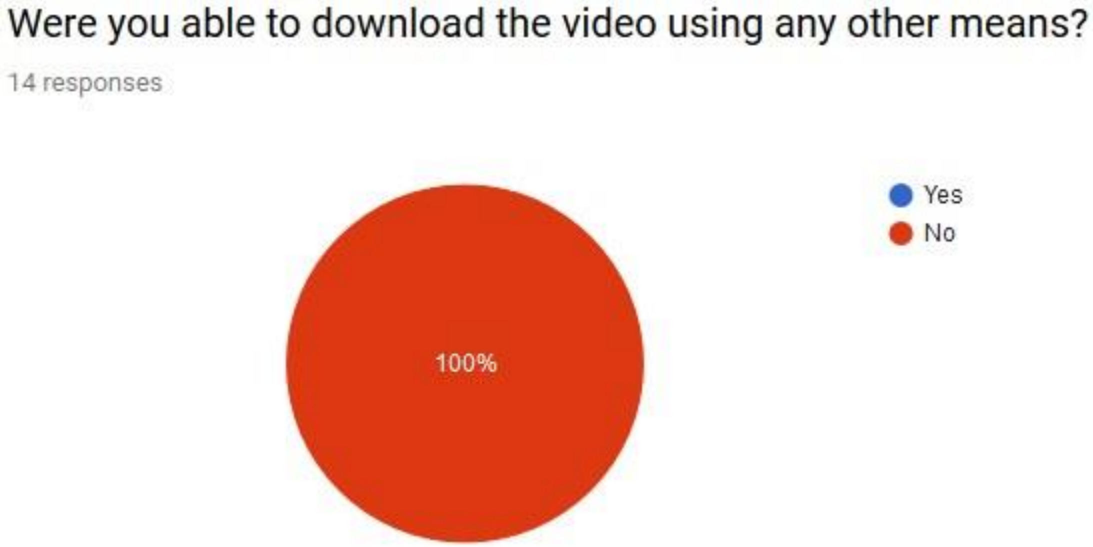


Figure 5.23 Alternate Download Means

Users were then asked to contribute any other feedback where a highlighted one was that the system was user friendly and the video ‘almost impossible to download.’ Using this premise, the developer was satisfied that the system had delivered on its key goal.

5.4 System Validation

The most logical method that the system could be validated was through an evaluation from an experienced hacker with an aim of breaking into the system. The evaluation was carried out by an experienced expert on the field with certifications in CEH – Certified Ethical Hacker. The developer was therefore satisfied that the findings would be accurate.

Validation took two approaches; the first was an outward shell approach where the system was presented to the ethical hacker who was asked to acquire a copy of the video stream using traditional methods (without employing any hacking technique/tools that are at his disposal). The video stream was safe as there was no means of acquiring the video with no tool. Unfortunately, in today’s world, tools are abundantly present, therefore this test would not suffice. Using expert knowledge, the hacker used Mozilla Firefox’s web console to observe web traffic. Every browser comes with a Web Console which logs information associated with a web page: network requests, JavaScript, CSS, security errors and warnings as well as error, warning and informational messages explicitly logged by JavaScript code running in the page context (mozilla, 2018). By playing the video, it was observed that the browser requested for the key file each time it played a new segment of the video. By taking a closer observation of the key file GET request, it was revealed that the browser revealed the location of the key file on the server. It is worth noting that system, at the time of validation, was not hosted on a secure sever, meaning all requests were served over HTTP as opposed to HTTPS, meaning the key file could be intercepted. Already having the location of the key, the hacker used a browser plugin that listens for each segment and lists them. The plugin allows download of these segments thereafter. Using AES in CBC mode however meant that every segment had to be downloaded and the Initialisation vector known. A two-minute video for example that was segmented after every thirty seconds would have four segments that are all related to each other. Downloading the third segment and ignoring the rest would make decryption difficult as the previous encrypted segment was also used as input during the encryption process (XORed with the key file before encryption). Having assembled the segments and key file, the tester suggested that a driven attacker could write a script that uses this information to decrypt the segments. Though this avenue was not explored further, the hacker noted it was very possible.

The other penetration test was examining the browser behaviour. During streaming, to maximise on user experience, browsers buffer the entire video and store this data on the user's computer under a storage path that is browser-dependent. This ensures that users have a seamless experience when streaming content and not experience delays or lags mid content. This behaviour is however dependent on the user's network speed. Therefore, in theory, an attacker could simply wait for the system to load the entire video and access the decrypted version on their local machine. However, using Firefox v59.0.2 (64-bit), an examination of '*C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\profile.default\Cache'* directory showed no evidence of a cached stream.

In summary, the validation proved that the system would be viable in protecting the video under normal conditions, however more steps should be taken to protect it under extreme conditions. The findings of validation phase offered valuable insights to guide system implementation which shall be discussed under chapter seven of this document.

Chapter 6 Discussion of Results

6.1 Overview

This chapter analyses the findings in relation to the research objectives and extent to which the findings agree with the literature review.

6.2 Objective One

The first objective was to find out about the application of digital videos in the Kenyan education industry and understand the online video streaming piracy issue. The literature revealed that the sphere of digital learning is one that is still growing and yet to fully mature in the Kenyan education industry. Educators have been using text books to impart knowledge on their students for several years post incarnation of the new millennium, however, the decision by the Kenyan government to start digitising the industry is set to revolutionise learning in the country. The amount of financial investments that has been put in also provides a clear indication of the potential of growth in the industry. This has provided enough incentive for a lot of entities to get involved. These entities include universities, book publishers and curriculum developers.

The decision by Kenyatta University to launch their digital platform that has content mostly in video format is also an indication that videos have been embraced by Kenyan educators as a means of conveying their content; this is backed by the Kenya Institute for Curriculum Development's DigiSchool program that is also advocating for the development of content in text, audio and video format.

Digital videos however face a huge piracy threat in the Internet domain. The threat coincides with the growth in popularity and proliferation of VoD services and streaming sites where malicious users can obtain copies for redistribution with minimum effort. The reports in section 2.1.3 shows the trend is just gaining momentum and is proving to be a major issue for owners of these videos. Kenya is yet to give piracy the attention it deserves. Most of the anti-copyright laws are precolonial and cannot be applied in today's technology dominated environment. They have proved to be unreliable which offers little encouragement for copyright owners.

A questionnaire sent out to ten Kenyan content creators confirms the accuracy of the above findings. According to the questionnaire, whose findings are displayed under Appendix C of this document, eight out of the ten respondents use the Internet to distribute their content, and although seven out ten confirm that they receive a profit from their content, only half are confident that it is consumed via legal means. The survey also noted that only five out of the ten had not had an encounter with piracy while six out of the ten claimed that piracy affected their brand financially. Nine out of ten correspondents also felt that the Government was not doing enough to curb piracy with six of them resulting to personal measures to protect their content. This status quo provided the researcher with enough incentive to develop a DRM system to fill the gaps, moving forward.

6.3 Objective Two

The second objective was to find out about the video encryption techniques and existing Digital Rights Management (DRM) solutions. This objective was intended on gaining an insight on encryption techniques that can be used to secure digital videos and the current existing platforms that can achieve this. The research revealed that encryption techniques to be applied on any video largely depend on the purpose of use of the video. The two main categories were for entertainment purposes where Netflix falls under and for use in sensitive applications. Other considerations included the amount of overhead on the machine that the technique generate. For use in a live environment, Fully Layered techniques are not practical due to the heavy computation they demand, however, they offer the best solution in terms of securing the content. These techniques met the objectives for the developed system and hence were used.

For Existing solutions that offer DRM, the research revealed several options that are in use today. These options are developed by well-known international brands and offer a lot in terms of security. Perhaps their biggest undoing (for the Kenyan market) is their proprietary nature. For the Kenyan content creators, these solutions require heavy investments in terms of licensing fees which are also accompanied with tonnes of bureaucracy to acquire them. This fact, while it might not raise any eyebrows for established large corporates and institutions, may prove to be a stumbling block for smaller independent entities who would like to also have their content consumed. These solutions are also yet to acquire a foothold in the Kenyan market so are highly unpopular. This can be attributed to such factors as payment options (use of credit cards) and limited use of supported devices. Apple's Fairplay for example only works on the company's range of devices which, in a country of individuals with an income that barely gets them through life, may prove to be too much of a luxurious undertaking. The only open source solution, OMA, is limited to Android devices; which, unfortunately, fell out of bounds of this research.

6.4 Objective Three

The third objective was to design, develop and test a system that enforces rights for digital video stream owners. This objective was achieved through the design, implementation and testing of the system. It was developed by incorporating two main libraries, namely FFmpeg and Video.js. The user tests indicated that a majority of popular file downloading tools such as Internet Download Manager were unable to download a copy of the encrypted video stream, however, some users had indicated that their versions were able to carry out this task. While the developer was very confident that the users were merely downloading encrypted segments, which could not be played on the users' devices without first undergoing decryption, the test result highlighted the importance of secrecy of the key.

6.5 Objective Four

The fourth objective was to validate the effectiveness of the developed solution and verify that its objective, which was to secure video streams, was met. Validation of the system was carried out by an experienced penetration tester under @iLabAfrica's security department, whose findings have been discussed in section 5.4. These findings indicate that the system fully meets its design objective under the prescribed scope, which was users with up to intermediate level of computer skills/knowledge. However, for a well driven individual with all the required skills and tools, the penetration tester indicated that they would be able defeat the system, provided they had access to all file segments and the decryption key. The penetration tester also noted that use of Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode was appropriate as it greatly increased the difficulty of 're-joining' the segments into a complete video, if the key was obtained. These findings offered valuable insights into the direction that the system should take in the future. These insights are discussed in the third section of chapter seven.

Chapter 7 Conclusions, Recommendations and Future Work

7.1 Conclusions

This research's focus was on the development of a platform that would allow for streaming of videos while securing their integrity. This was intended to as an aid for local content creators to ensure that they can safeguard their intellectual property from abuse in the new age of digital transformation in Kenya's education sector. The system was developed, and it was able to fulfil this requirement successfully. The solution was able to make use of open-source libraries for this task and was integrated with PesaPal to allow for potential learners to pay for content, which provides the incentive required by the creators to carry on creating content.

7.2 Recommendations

The system is best suited to be used in a school setting with students being its primary userbase. The server used to host the system should have a Secure Server Certificate to ensure that every transaction between the server and client is encrypted in order to guarantee a level of security for the key. Additionally, the key could be stored on a separate secure server that is specially built for this purpose and can hamper attackers from accessing the key file.

7.3 Future Work

Future work for this project may include areas such as optimisation of resource usage, key security, use of metadata and access control rules.

For resource usage, as evidenced by the compatibility test, the encryption process using FFmpeg library is quite resource intensive and uses up a lot of the host computer’s CPU time. The term host computer in this scenario has been used to refer to the server where the system has been installed. The computer being used by a provider to upload a video file does not suffer from the same amount of resource usage. The system should be optimised in such a manner that the encryption process can only take up a specified amount of the computer’s resources to allow other system processes to operate optimally.

It is also evident from the study that the security of all the video streams depends on the security of the key file. Future work could focus on further concealing the key either by using the logged in user’s session ID as part of the decryption process, which expires after a specified duration, rendering the key invalid for future use or using JavaScript to process the contents of the key file rather that returning the actual file.

The third area of focus could be on the use of Public Key Infrastructure to securely distribute keys to users to verify their identity and securely exchange data over the network. The Public Keys may further be used to specify Access Control measures such as the duration of validity, i.e., the duration of time that users have before access to the videos expires.

User’s metadata such as user id, name and email could also be appended to each segment when they are streaming the video to act as a fall-back plan if copies of the videos are found on the Internet. This might act as a deterrent for expert users who might have figured out ways of bypassing the security implementations.

The final recommendation for focus of future work is for content providers to be allowed to define their own access rules depending on type of content. For example, they may prefer for certain videos to be downloadable and sharable and certain videos to be only played when certain conditions are met (for example, time of day, after a certain duration of time, etc.).

References

Adam, J. S. (2018). *Known-Plaintext Attack Against a Permutation Based Video Encryption Algorithm*. Retrieved 15th March, 2018 from http://eprint.iacr.org

Angelides, M. C., & Agius, H. (2010). *The Handbook of MPEG Applications.* Chichester: John Wiley & Sons, Ltd.

apple. (2018). *FairPlay Streaming*. Retrieved 15th March 2018 from apple: https://developer.apple.com/streaming/fps/

Bhat, S. (2016). *Digital Content Protection: Challenges, Opportunities & Solutions*. Retrieved 19th January, 2018 from tcs: https://securitycommunity.tcs.com/infosecsoapbox/articles/2016/01/29/digital-contentprotection-challenges-opportunities-solutions

Boyce, C., & Neale, P. (2006). *Conducting in-depth Interviews: A Guide for Designing and Conducting In-Depth Interviews.* Pathfinder International Tool Series. Retrieved 16th April, 2018 from https://research-methodology.net/research-methods/qualitativeresearch/interviews/

Broomfield, H. (2009, September 5). *Intellectual Property rights*. Retrieved 20th March, 2018 from innovasjonnorge: http://www.innovasjonnorge.no/no/Eksporthandboken/manedenstema/What-are-Intellectual-Property-rights/

Ce, Z., Yuenan, L., & Xiamu, N. (n.d.). Streaming Media, Architectures, Techniques, and Applications. 2011: IGI Global.

Choosing DSDM as your Agile Approach. (2014). Retrieved 21st March, 2018 from agilebusiness: https://www.agilebusiness.org/content/choosing-dsdm-your-agileapproach-0

Cohen, B. (2008). *BitTorrent Protocol Specification*. Retrieved 1st March, 2018 from bittorrent: http://bittorrent. org/beps/bep_0003.html

collinsdictionary. (2018, January 29). Retrieved 15th February, 2018 from https://www.collinsdictionary.com/dictionary/english/video-piracy

Deloitte. (2015). *Digital Media: Rise of On-demand Content.* Deloitte Touche Tohmatsu India Private Limited.

Digital Content Protection, L. (2018). *About DCP*. Retrieved 30th January, 2018 from digital-cp: https://www.digital-cp.com/about_dcp

Digital Learning Programme. (2018). Retrieved 29th January, 2018 from education.go.ke: http://www.education.go.ke/index.php/programmes/digital-learning-programme

Digital Rights and Intellectual Property. (n.d.). Retrieved 3rd February, 2018 from archive: https://archive.org/stream/DigitalRightsAndIntellectualProperty/DigitalRights#page/n0/mode/1up

Digital School. (2018). Retrieved 30th January, 2018 from ku: http://ku.ac.ke/dsvol/ Digital
Video. (n.d.). Retrieved 3rd February from techopedia: https://www.techopedia.com/definition/5505/digital-video-dv

Divx. (2018). *Content Protection*. Retrieved 15th March 2018 from divx: http://www.divx.com/en/node/90

Drmtoday. (2018). *FairPlay Streaming DRM by Apple*. Retrieved 15th March 2018 from drmtoday: https://drmtoday.com/fairplay/

Dutton, S. (2018). *What is EME*. Retrieved 15th March, 2018 from developers.google: https://developers.google.com/web/fundamentals/media/eme

Encoding. (2018). Retrieved 15th March 2018 from The Complete Guide to Apple Fairplay: https://www.encoding.com/apple-fairplay/

Encoding. (2018). *The Complete Guide to Widevine Google's DRM Platform*. Retrieved 15th March 2018 from encoding: https://www.encoding.com/widevine/

Esourceresearch. (2018). *Sample Surveys*. Retrieved 1st April 2018 from esourceresearch: http://www.esourceresearch.org/eSourceBook/SampleSurveys/6DevelopingaSurveyInstrument/tabid/484/Default.aspx

Eugene, L. T., Gregory, C. W., Paul, S., & Edward, J. D. (2001). An over view of Security Issues in Streaming Video. *IEEE Xplore*.

Functional Testing Tutorial. (2018). Retrieved 30th January 2018 from guru99: https://www.guru99.com/functional-testing.html

Gaur, R. (2018). *Software Architecture: One-Tier, Two-Tier, Three Tier, N Tier*. Retrieved 15th March 2018 from techynews4u: http://techynews4u.com/software-architecture-one-tiertwo-tier-three-tier-n-tier/

Green, R. (2012). *Cisco Unified Customer Voice Portal: Building Unified Contact Centers.* Indianapolis: Cisco Press. Retrieved 15th March 2018 from http://books.google.co.uk/books?id=NvsqLlbSAbQC&pg=PT310&dq=streaming+definition&hl=en&sa=X&ei=ZZ gFUN_YDMTBhAf16K3TBw&ved=0CGUQ6wEwBjge#v=onepage&q=streaming%20definition&f=false

Hao, W., & Chong-Wei, X. (1998). Light Weight MPEG video Encryption Algorithm. *International Conference on Multimedia*, (pp. 55-61).

Haskell, B., Puri, A., & Netravali, A. (1996). Digital video: an introduction to MPEG2. *ISBN 0412084112*.

Helberger, N. (2005). Controlling Access to Content: Regulating Conditional Access in Digital Broadcasting. *ISBN-13:9041123458*

Helpnetsecurity. (2009, September 11). *OMA DRM 1.0 Client for Android*. Retrieved 15th March 2018 from helpnetsecurity: https://www.helpnetsecurity.com/2009/09/11/oma-drm-10client-for-android/

Intertrust. (2018). *Marlin DRM*. Retrieved 15th March 2018 from intertrust: https://www.intertrust.com/marlin-drm/

Kaliski, B. (1993). A survey of encryption standards. *Micro, IEEE, vol. 13, no. 6,* 74-81.

Kania, B., & Gusukuma, L. (2018). *HTTP Live Streaming*. Retrieved 15th March 2018 from vtechworks.lib: https://vtechworks.lib.vt.edu/bitstream/handle/10919/18662/Instructions%20for%20HTTP%20Live%20Streaming%20Final.pdf

Kenyatta University Digital School. (2018). Retrieved 30th January 2018 from softkenya: https://softkenya.com/education/kenyatta-university-digital-school/

laravel. (2018). *Laravel Philosophy*. Retrieved 16th March 2018 from laravel: https://laravel.com/docs/4.2/introduction

Layton, J. (n.d.). *How Digital Rights Management Works*. Retrieved 17th March 2018 from howstuffworks: https://computer.howstuffworks.com/drm1.htm

Lessing, L. (2004). In L. Lessing, *How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* (p. 298). The Penguin Press.

Liu, F., & Koenig, H. (2010). A survey of video encryption algorithms. Computers & Security. *ISBN 01674048,* 3–15.

Longhorn Publishers. (2016). *Longhorn Publishers Annual Report & Financial Statements.* Nairobi: Longhorn Publishers.

Maciejewski, M., Fischer, N. I., & Roginska, Y. (2014). *Streaming and online access.* Brussels: Directorate General for Internal Policies.

Marpe, D., Wiegand, T., & Sullivan, G. J. (2006). *The H.264/MPEG4 advanced video coding standard and its applications*. Retrieved 2nd April 2018 from ieee: http://ieeexplore.ieee.org/document/1678121/?reload=true

Matinde, V. (2017). Retrieved 20th January 2018 from itwebafrica: http://www.itwebafrica.com/security/515-kenya/237437-kenyan-publishers-launch-newsystem-to-fight-piracy

Microsoft. (2018). *Microsoft: Microsoft PlayReady Content Access Technology White Paper*. Retrieved 15th March 2018 from microsoft: http://download.microsoft.com/download/b/8/3/b8316f44e7a9-48ff-b03a-44fb92a73904/Microsoft%20PlayReady%20Content%20Access%20TechnologyWhitepaper.docx

Mir, M. A., Abu, H. S., & Asadul, A. (2010). Digital Rights Management. *International Journal of Computer Science and Network Security*, 24-32.

Motionelements. (2013, September 9). *5 Most Common Video File Formats*. Retrieved 23rd March, 2018 from motionelements: https://www.motionelements.com/blog/articles/whatyou-need-to-know-about-the-5-most-common-video-file-formats

MUSO Global Piracy Report. (2017). Retrieved 21st January 2018 from muso: https://www.muso.com/wp-content/uploads/2017/04/MUSO_2017_Global_Sample_Market_Insights_report.pdf

Object-Oriented Languages and Systems. (n.d.). Retrieved 1st April 2018 from ncsu: https://people.engr.ncsu.edu/efg/517/f01/syllabus/lectures/lec6.pdf

Odero, K. (2016). *Digital Learning Project*. Retrieved 14th February 2018 from iafrikan: https://www.iafrikan.com/2016/10/04/kenya-laptop-project/

Ooyala. (2018). *PlayReady Content Protection*. Retrieved 15th March 2018 from ooyala: http://help.ooyala.com/video-platform/concepts/player_v3dev_playreadyintro.html Peer-to-Peer File Sharing. (2014). Retrieved 20th February 2018 from zonealarm: https://www.zonealarm.com/blog/2014/06/what-need-know-about-peer-to-peer-filesharing/

Philippe, K. (2009). *The Impact of Digital Distribution – A Contribution.* KEA European Affairs.

Queensland, T. U. (2018). *Pedagogical benefits*. Retrieved 15th March 2018 from uq: http://www.uq.edu.au/teach/video-teach-learn/ped-benefits.html

Rayburn, D. (2007). *Streaming and Digital Media: Understanding the Business and Technology.* Focal Press.

Rehorn, L. (2016, December 12). *VOD Education*. Retrieved 15th March 2018 from borgenproject: https://borgenproject.org/vod-education-in-kenya/

Rouse, M. (2009, January). *Digital Rights Management*. Retrieved 27th January 2018 from techtarget: http://searchcio.techtarget.com/definition/digital-rights-management Sebok. (2017). *System Implementation*. Retrieved 20th March 2018 from sebokwiki: http://www.sebokwiki.org/wiki/System_Implementation

Shi, C., & Bhargava, B. (1998). A Fast MPEG Video Encryption Algorithm. *6th ACM International Conference on Multimedia*, (pp. 81–88).

Shi, C., & Bhargava, B. (1998). Light Weight MPEG video Encryption Algorithm. *the International Conference on Multimedia*, (pp. 55-61).

Shiguo, L. (2008). *Multimedia Content Encryption: Algorithms and Application.* CRC Press.

Shunjun, L., Guanrong , C., Albert , C., Bharat , B., & Kwok-Tung , L. (2007). On the Design of Perceptual MPEG Video Encryption Algorithm. IEEE Transactions on Circuits and Systems for Video Technology.

Sikarwar, R. (2016). *Definition of Digital Media.* Retrieved 20th January 2018 from linkedin: https://www.linkedin.com/pulse/definition-digital-media-rahul-sikarwar-digitalmarketing-expert

Singh, P., & Hooda, D. (2012). A Comprehensive Survey of Video Encryption Algorithms. *International Journal of Computer Applications*.

Socek, D., Kalva, H., Magliveras, S. S., Marques, O., Culibrk, D., & Furht, B. (2006). A Permutation-based CorrelationPreserving Encryption Method for Digital Videos. *International Conference on Image Analysis and Recognition* (pp. 547-558). LNCS 4141.

Sohn, D. (2006). *Evaluating DRM: Building a Marketplace for the Convergent World.* Retrieved 15th March 2018 from cdt.org: https://www.cdt.org/files/copyright/20060907drm.pdf

Stats, I. w. (2018). *Internet Usage Statistics*. Retrieved 15th March 2018 from internetworldstats: https://www.internetworldstats.com/af/ke.htm

Svantesystems. (2018). *Software Development Methodologies*. Retrieved 15th March 2018 from svantesystems: https://www.researchgate.net/figure/Rapid-Application-Development-RAD-process-structure_fig2_262067303

Tang, L. (1996). For Encrypting and Decrypting MPEG Video Data Efficiently. *Forth ACM International Multimedia Conference,* (pp. 219-230).

Techopedia. (2018). *Torrent*. Retrieved 15th March 2018 from techopedia: https://www.techopedia.com/definition/5263/torrent

Techopedia. (n.d.). *PHP*. Retrieved 27th March 2018 from techopedia: https://www.techopedia.com/definition/24406/php-hypertext-preprocessor-php

Telecomabc. (n.d.). *MPEG-2.* Retrieved 27th March 2018 from http://www.telecomabc.com/m/mpeg-2.html

The International Chamber of Commerce. (2013). *Promoting and Protecting Intellectual Property in Kenya.* Paris: The International Chamber of Commerce.

Tredger, C. (2016). *The right time for VoD in Kenya*. Retrieved 27th March 2018 from itwebafrica: http://www.itwebafrica.com/kenya/236956-the-right-time-for-vod-in-kenya Trouble in Our Digital Midst. (2017). *Trouble in Our Digital Midst.* digital citizens alliance.

Uhl, A., & Pommer, a. (2005). Image and video encryption: from digital rights management to secured personal communication. *Advances in Information Security*.

US Chamber of Commerce. (2017). *The Roots of Innovation.* Washington: U.S. Chamber International IP Index.

Vrechek, A. (2010). *UltraViolet*. Retrieved 15th March 2018 from businesswire: https://www.businesswire.com/news/home/20100719006854/en/Digital-EntertainmentContent-Ecosystem-Unveils-UltraViolet%E2%84%A2-Brand

W3C. (2016). *Media Source Extensions*. Retrieved 7th April 2019 from w3: https://www.w3.org/TR/media-source/

What is Rapid Application Development. (2000). *What is Rapid Application Development.* Retrieved 13th March 2018 from CASEMaker Inc: http://www.iro.umontreal.ca/~dift6803/Transparents/Chapitre1/Documents/rad_wp.pdf.

World Intellectual Proprety Organization [WIPO]. (2004). *Intellectual Property*. WIPO Publication.

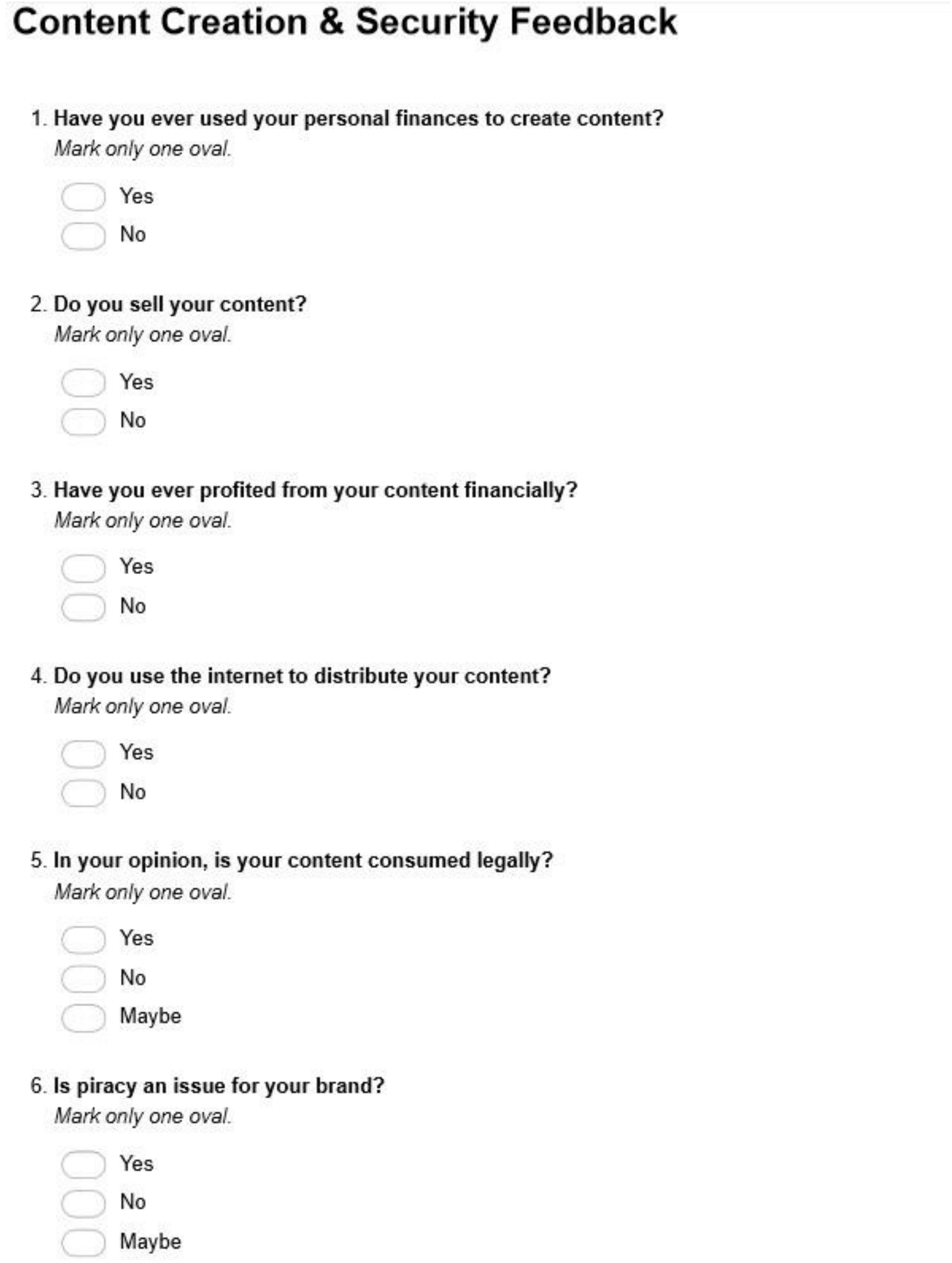
Wu, C. P., & Kuo, C. j. (2005). Design of integrated multimedia compression and encryption systems. *IEEE transaction on multimedia*, 828-839.

Xiao, Z. (2018). *A Survey of Digital Rights Management Technologies*. Retrieved 27th March 2018 from wustl: http://www.cse.wustl.edu/~jain/cse571-11/ftp/drm/

Zaneeducation. (2018). *Benefits of Using Educational Video in The Classroom*. Retrieved 27th March 2018 from zaneeducation: http://www.zaneeducation.com/educationalvideo/education-and-video.php

Appendices

Appendix A Content Creators Questionnaire



Content Creation & Security Feedback

1. **Have you ever used your personal finances to create content?**
Mark only one oval.

○ Yes
○ No

2. **Do you sell your content?**
Mark only one oval.

○ Yes
○ No

3. **Have you ever profited from your content financially?**
Mark only one oval.

○ Yes
○ No

4. **Do you use the internet to distribute your content?**
Mark only one oval.

○ Yes
○ No

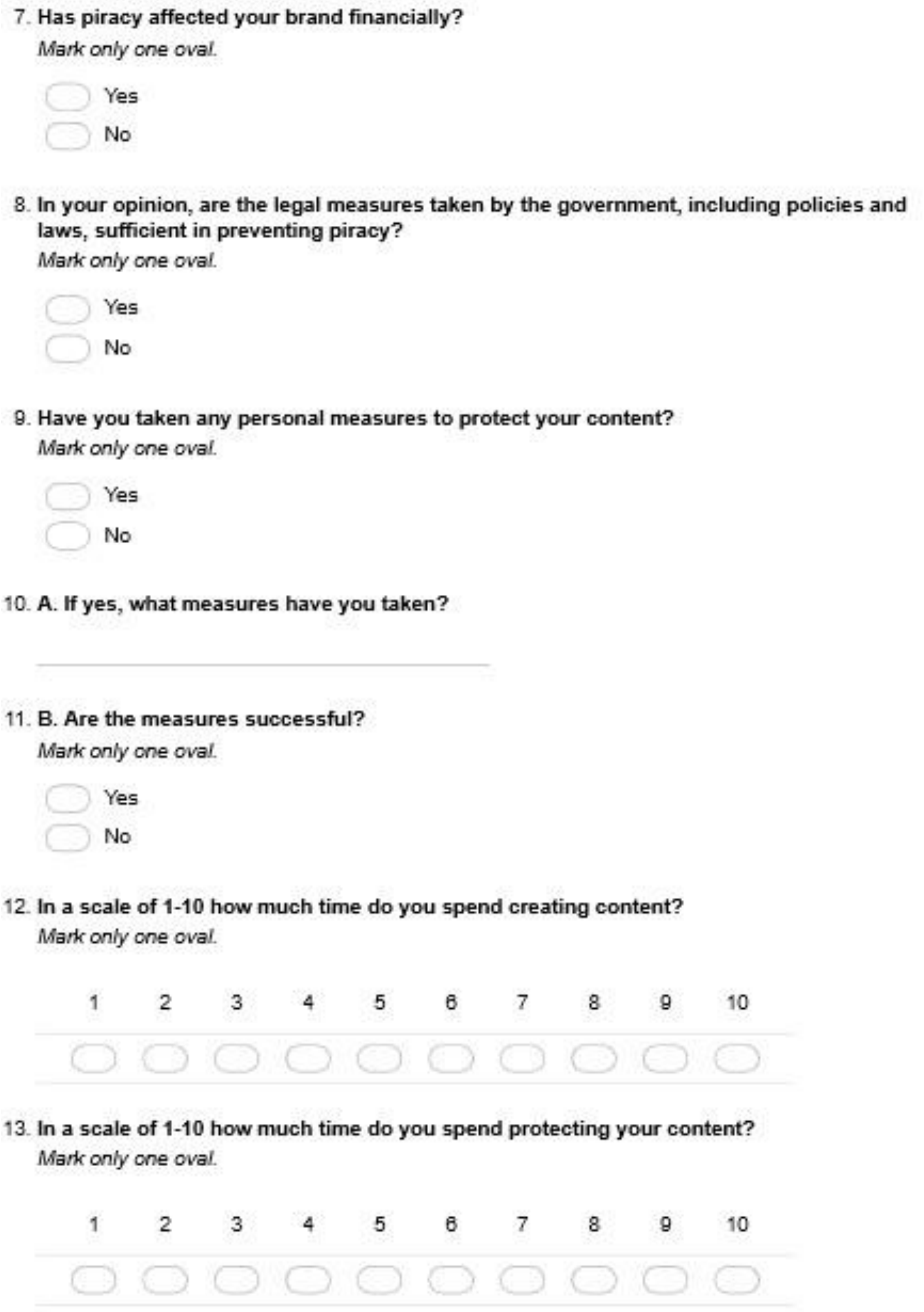
5. **In your opinion, is your content consumed legally?**
Mark only one oval.

○ Yes
○ No
○ Maybe

6. **Is piracy an issue for your brand?**
Mark only one oval.

○ Yes
○ No
○ Maybe

Figure A.1 Content Creators Questionnaire - Part A



7. **Has piracy affected your brand financially?**
Mark only one oval.

○ Yes
○ No

8. **In your opinion, are the legal measures taken by the government, including policies and laws, sufficient in preventing piracy?**
Mark only one oval.

○ Yes
○ No

9. **Have you taken any personal measures to protect your content?**
Mark only one oval.

○ Yes
○ No

10. **A. If yes, what measures have you taken?**

____

11. **B. Are the measures successful?**
Mark only one oval.

○ Yes
○ No

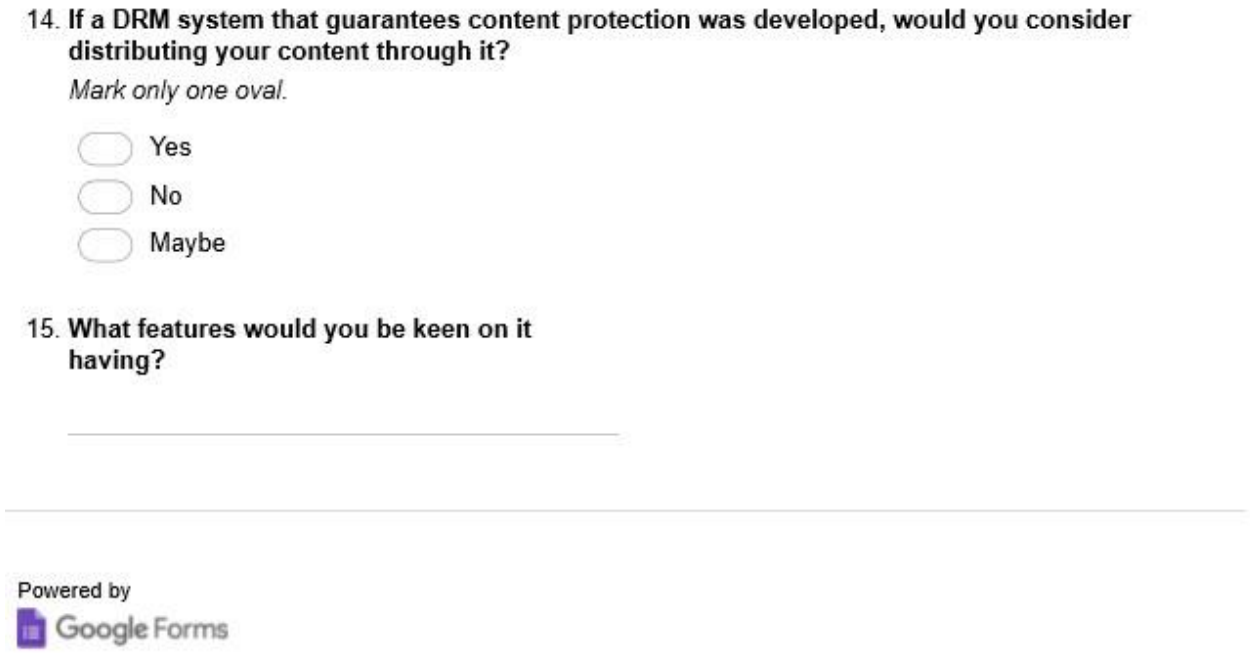
12. **In a scale of 1-10 how much time do you spend creating content?**
Mark only one oval.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

13. **In a scale of 1-10 how much time do you spend protecting your content?**
Mark only one oval.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

Figure A.2 Content Creators Questionnaire - Part B



14. **If a DRM system that guarantees content protection was developed, would you consider distributing your content through it?**

Mark only one oval.

○ Yes

○ No

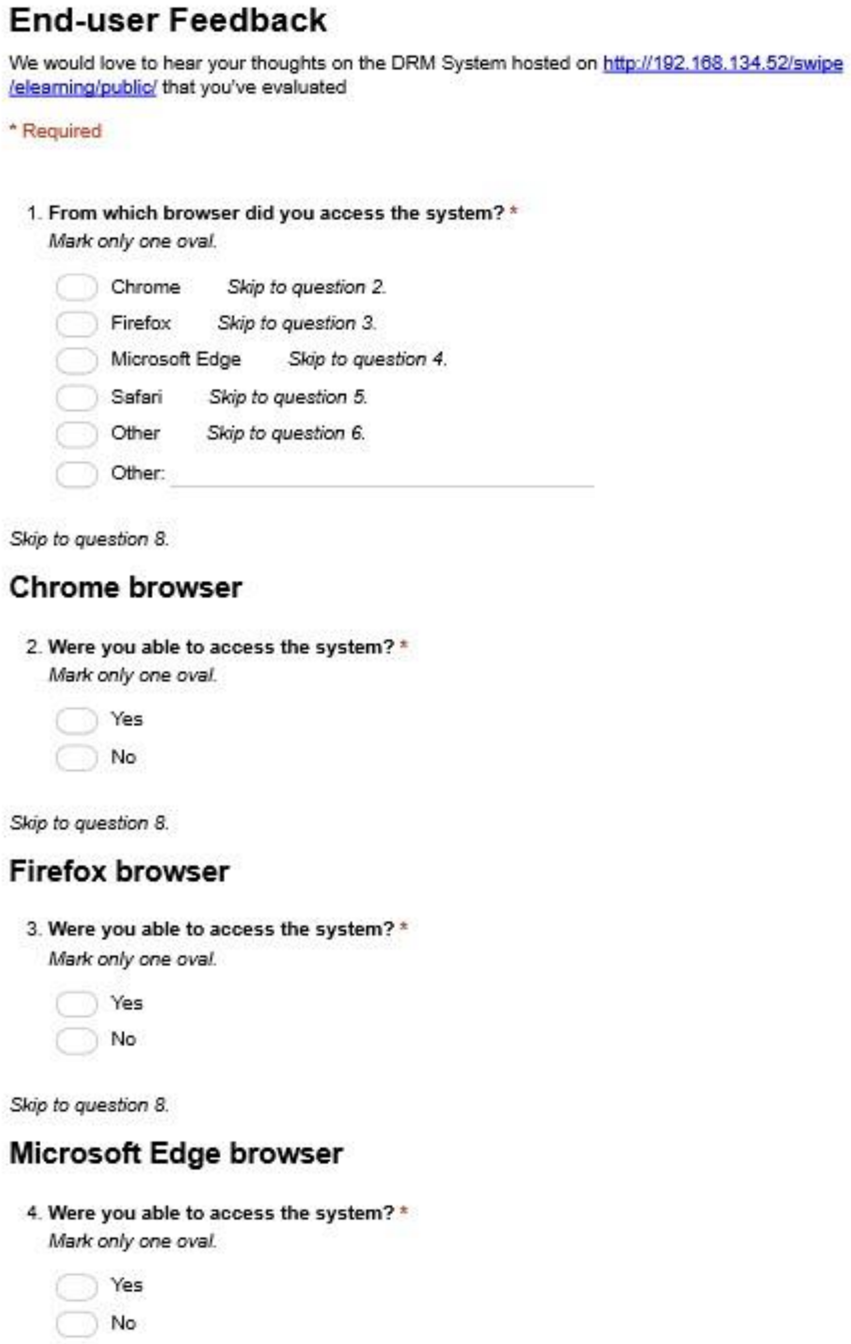
○ Maybe

15. **What features would you be keen on it having?**

____

Figure A.3 Content Creators Questionnaire - Part C

Appendix B Test User Questionnaire



End-user Feedback

We would love to hear your thoughts on the DRM System hosted on http://192.168.134.52/swipe/elearning/public/ that you've evaluated

* Required

1. **From which browser did you access the system? ***
   Mark only one oval.

   ○ Chrome *Skip to question 2.*
   ○ Firefox *Skip to question 3.*
   ○ Microsoft Edge *Skip to question 4.*
   ○ Safari *Skip to question 5.*
   ○ Other *Skip to question 6.*
   ○ Other: ____________________

Skip to question 8.

Chrome browser

2. **Were you able to access the system? ***
   Mark only one oval.

   ○ Yes
   ○ No

Skip to question 8.

Firefox browser

3. **Were you able to access the system? ***
   Mark only one oval.

   ○ Yes
   ○ No

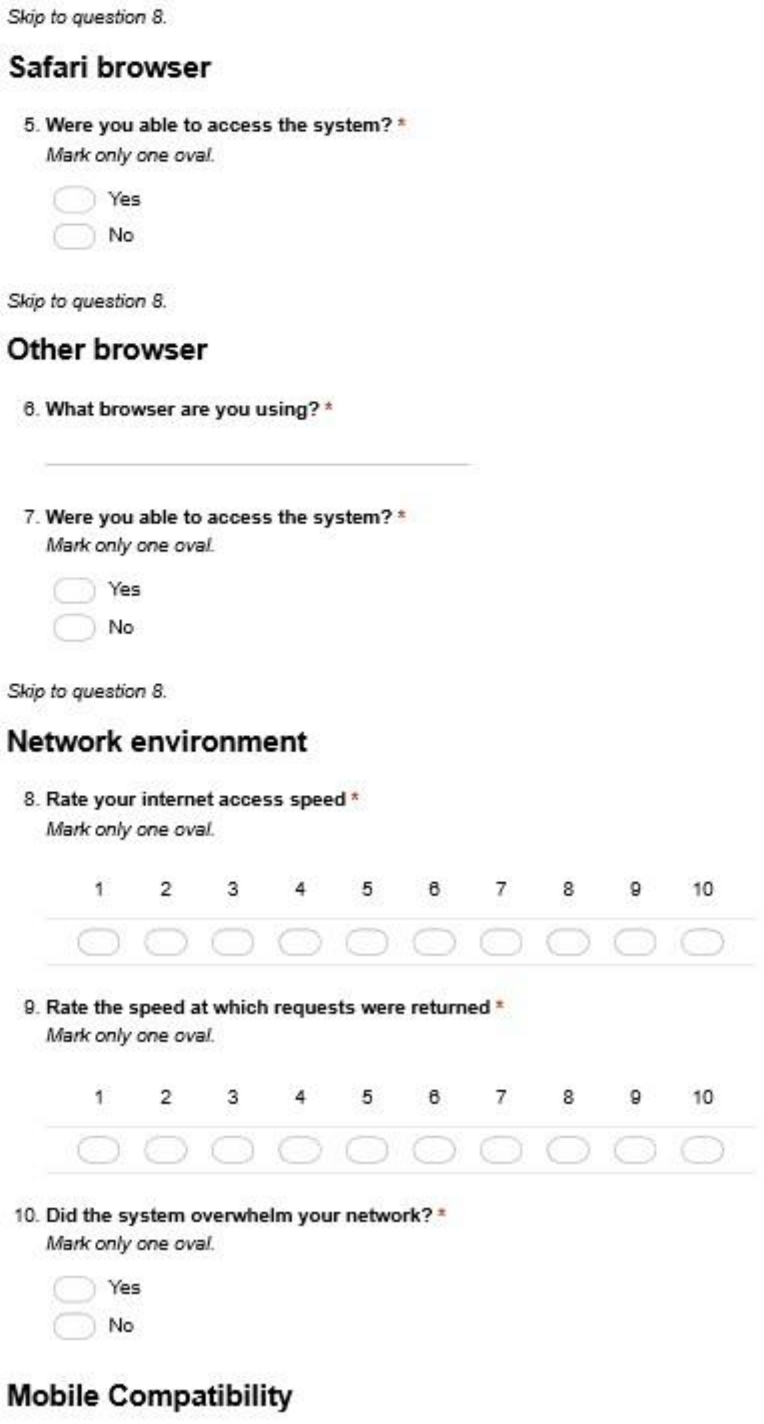
Skip to question 8.

Microsoft Edge browser

4. **Were you able to access the system? ***
   Mark only one oval.

   ○ Yes
   ○ No

Figure B.1 Test User Questionnaire - Part A



Skip to question 8.

Safari browser

5. **Were you able to access the system? ***
Mark only one oval.

○ Yes
○ No

Skip to question 8.

Other browser

6. **What browser are you using? ***

____

7. **Were you able to access the system? ***
Mark only one oval.

○ Yes
○ No

Skip to question 8.

Network environment

8. **Rate your internet access speed ***
Mark only one oval.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

9. **Rate the speed at which requests were returned ***
Mark only one oval.

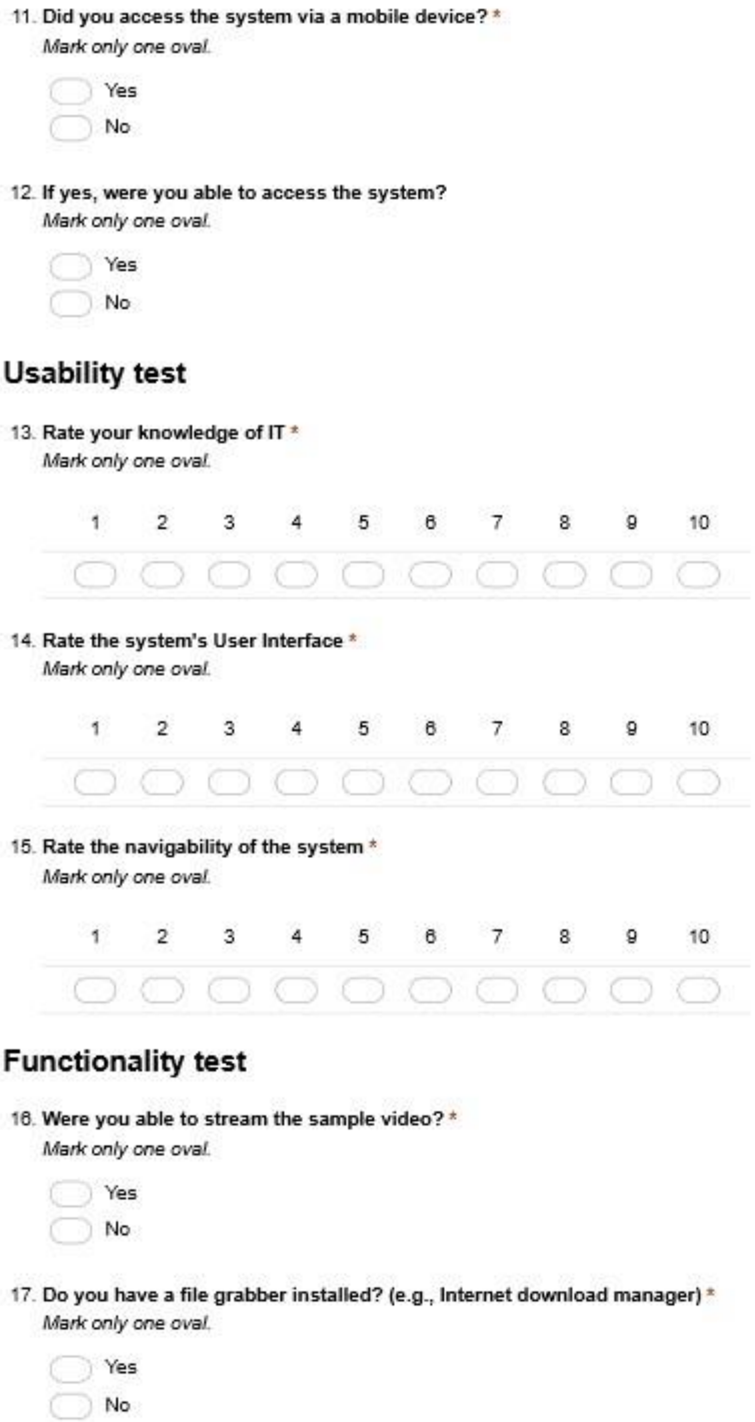
1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

10. **Did the system overwhelm your network? ***
Mark only one oval.

○ Yes
○ No

Mobile Compatibility

Figure B.2 Test User Questionnaire - Part B



11. **Did you access the system via a mobile device?** *

Mark only one oval.

○ Yes
○ No

12. **If yes, were you able to access the system?**

Mark only one oval.

○ Yes
○ No

Usability test

13. **Rate your knowledge of IT** *

Mark only one oval.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

14. **Rate the system's User Interface** *

Mark only one oval.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

15. **Rate the navigability of the system** *

Mark only one oval.

1	2	3	4	5	6	7	8	9	10
○	○	○	○	○	○	○	○	○	○

Functionality test

16. **Were you able to stream the sample video?** *

Mark only one oval.

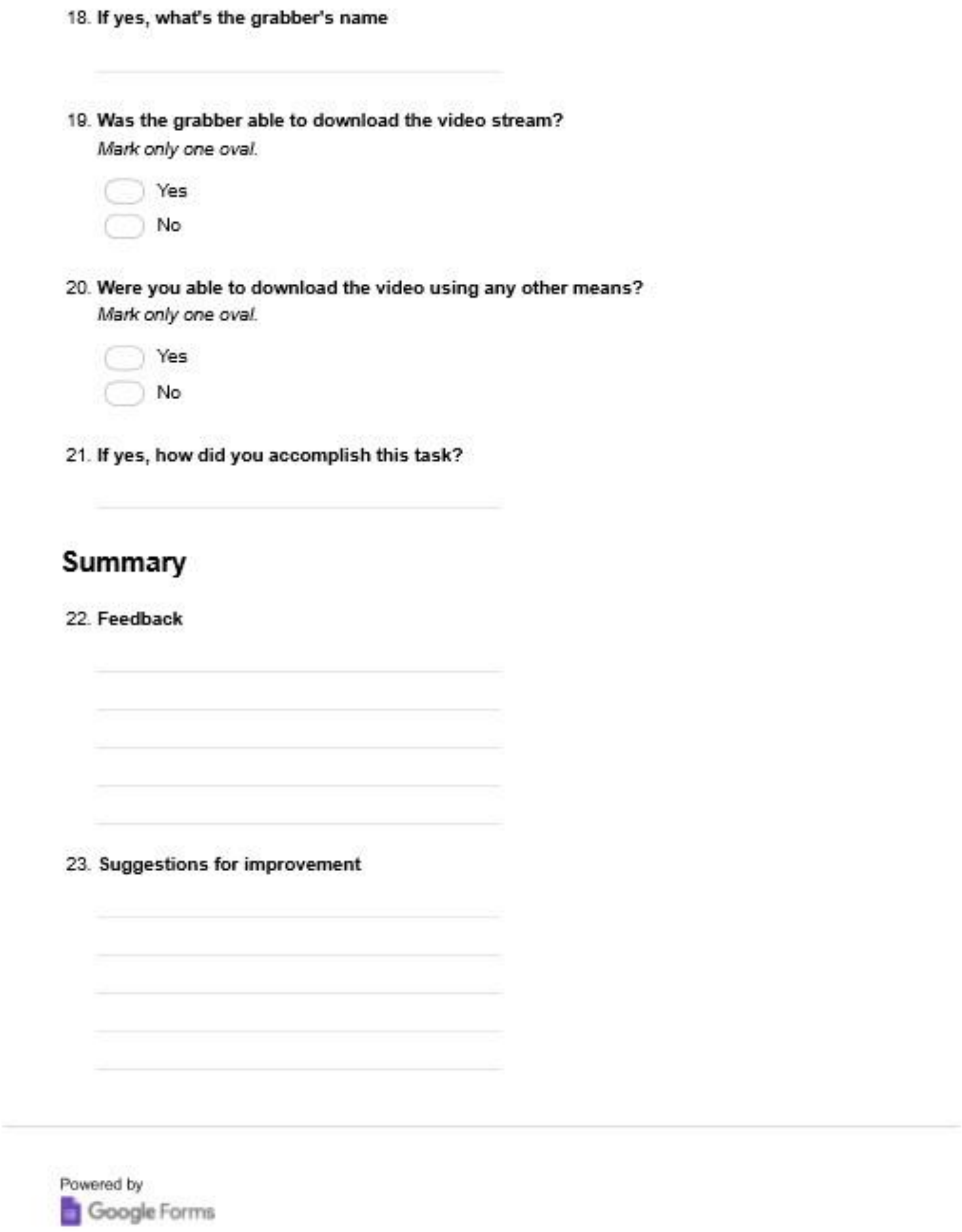
○ Yes
○ No

17. **Do you have a file grabber installed? (e.g., Internet download manager)** *

Mark only one oval.

○ Yes
○ No

Figure B.3 Test User Questionnaire - Part C



18. **If yes, what's the grabber's name**

19. **Was the grabber able to download the video stream?**
Mark only one oval.

○ Yes
○ No

20. **Were you able to download the video using any other means?**
Mark only one oval.

○ Yes
○ No

21. **If yes, how did you accomplish this task?**

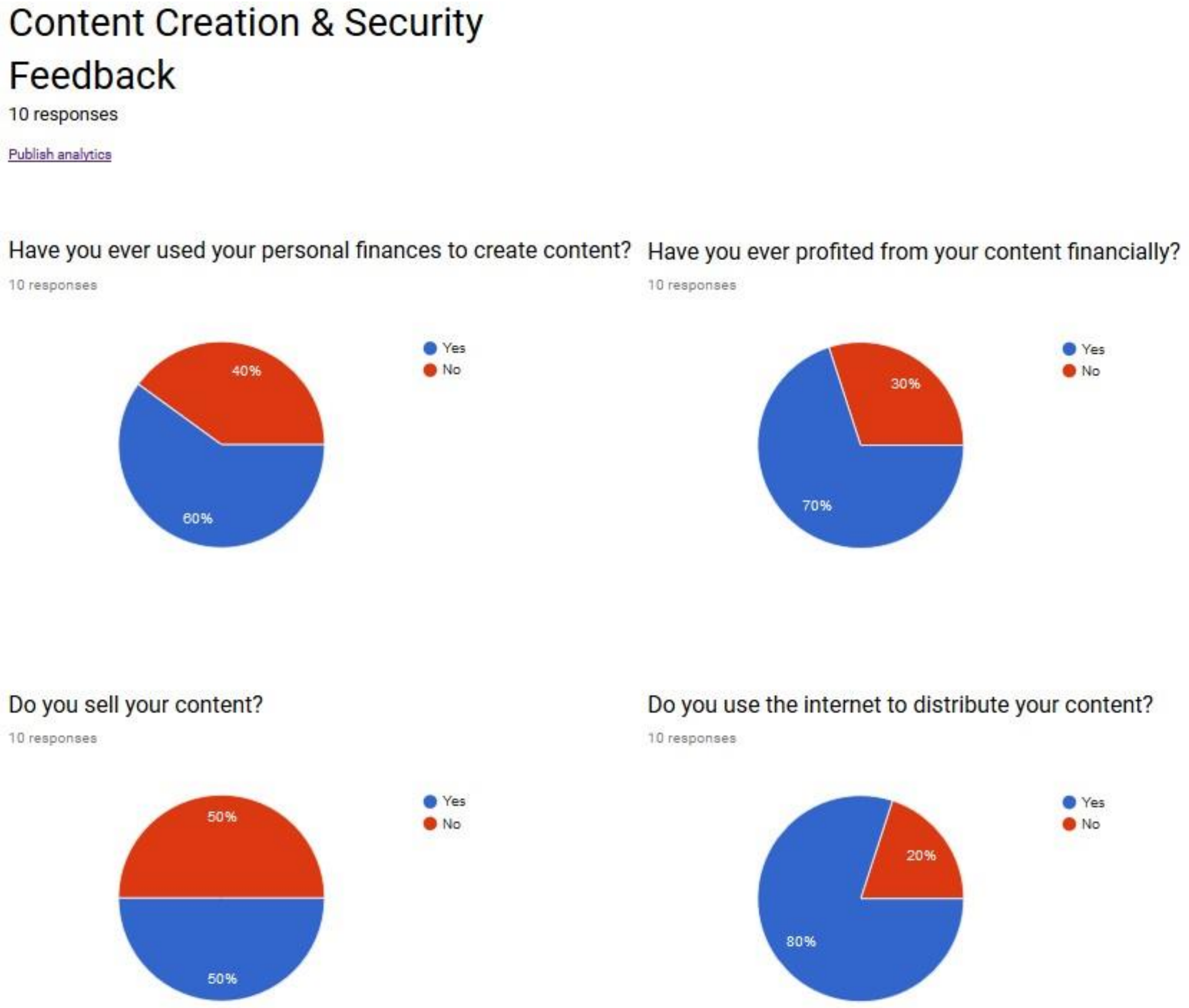
Summary

22. **Feedback**

23. **Suggestions for improvement**

Figure B.4 Test User Questionnaire - Part D

Appendix C Content Creator Responses



Content Creation & Security Feedback

10 responses

Publish analytics

Have you ever used your personal finances to create content?

10 responses

Have you ever profited from your content financially?

10 responses

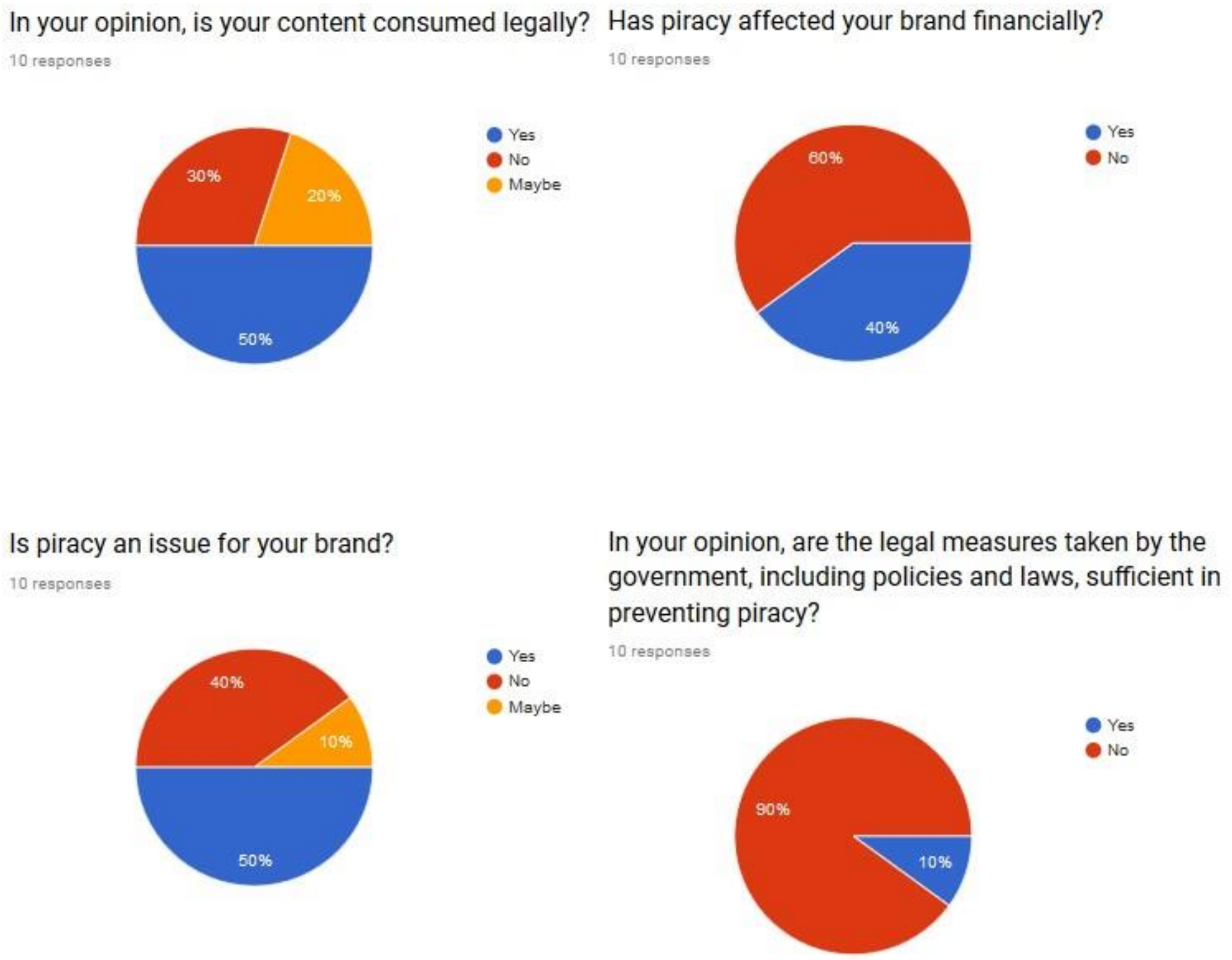
Do you sell your content?

10 responses

Do you use the internet to distribute your content?

10 responses

Figure C.1 Content Creator Responses - Part A



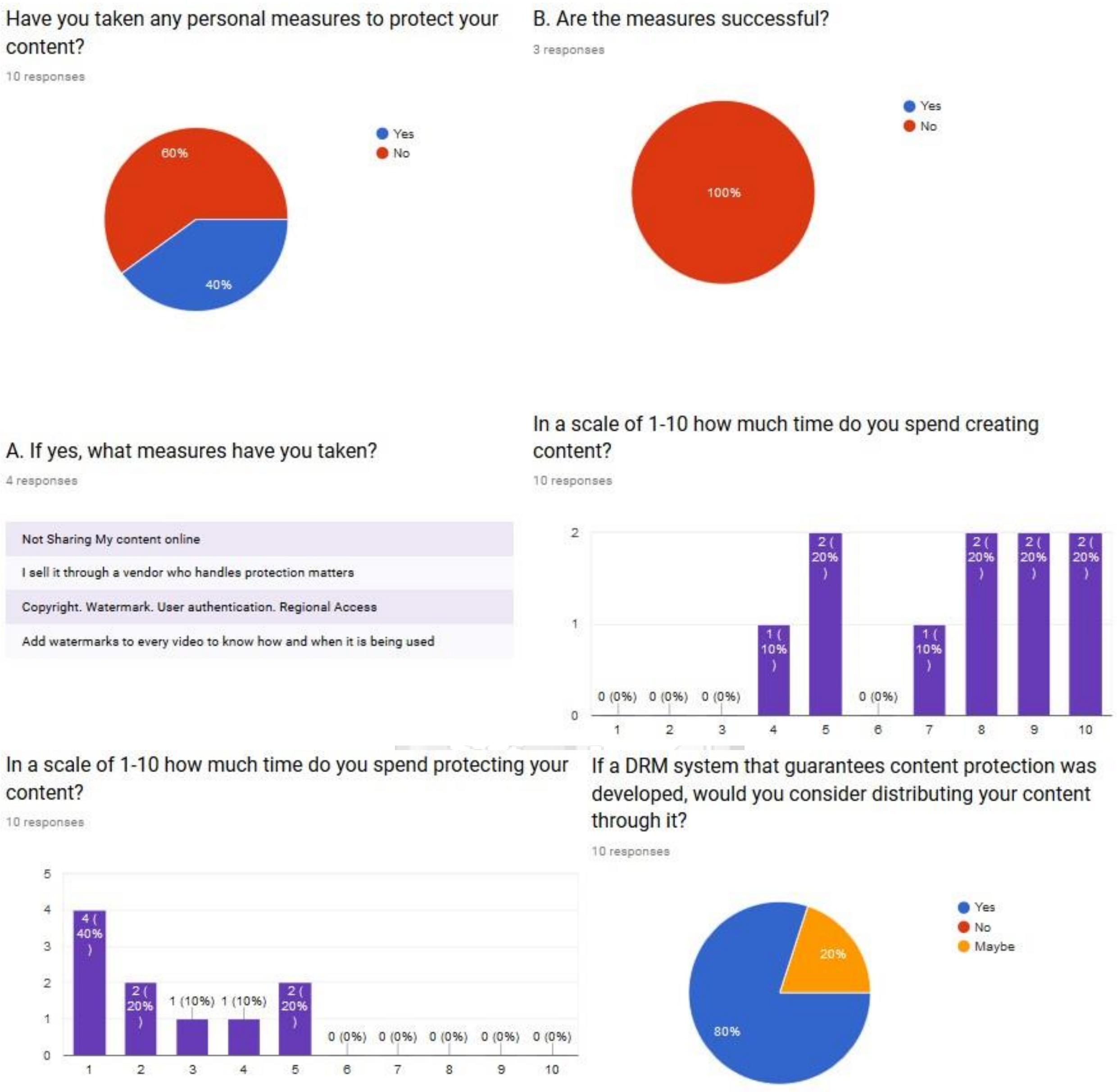
In your opinion, is your content consumed legally?

Has piracy affected your brand financially?

Is piracy an issue for your brand?

In your opinion, are the legal measures taken by the government, including policies and laws, sufficient in preventing piracy?

Figure C.2 Content Creator Responses - Part B



Have you taken any personal measures to protect your content?

10 responses

B. Are the measures successful?

3 responses

A. If yes, what measures have you taken?

4 responses

Not Sharing My content online

I sell it through a vendor who handles protection matters

Copyright. Watermark. User authentication. Regional Access

Add watermarks to every video to know how and when it is being used

In a scale of 1-10 how much time do you spend creating content?

10 responses

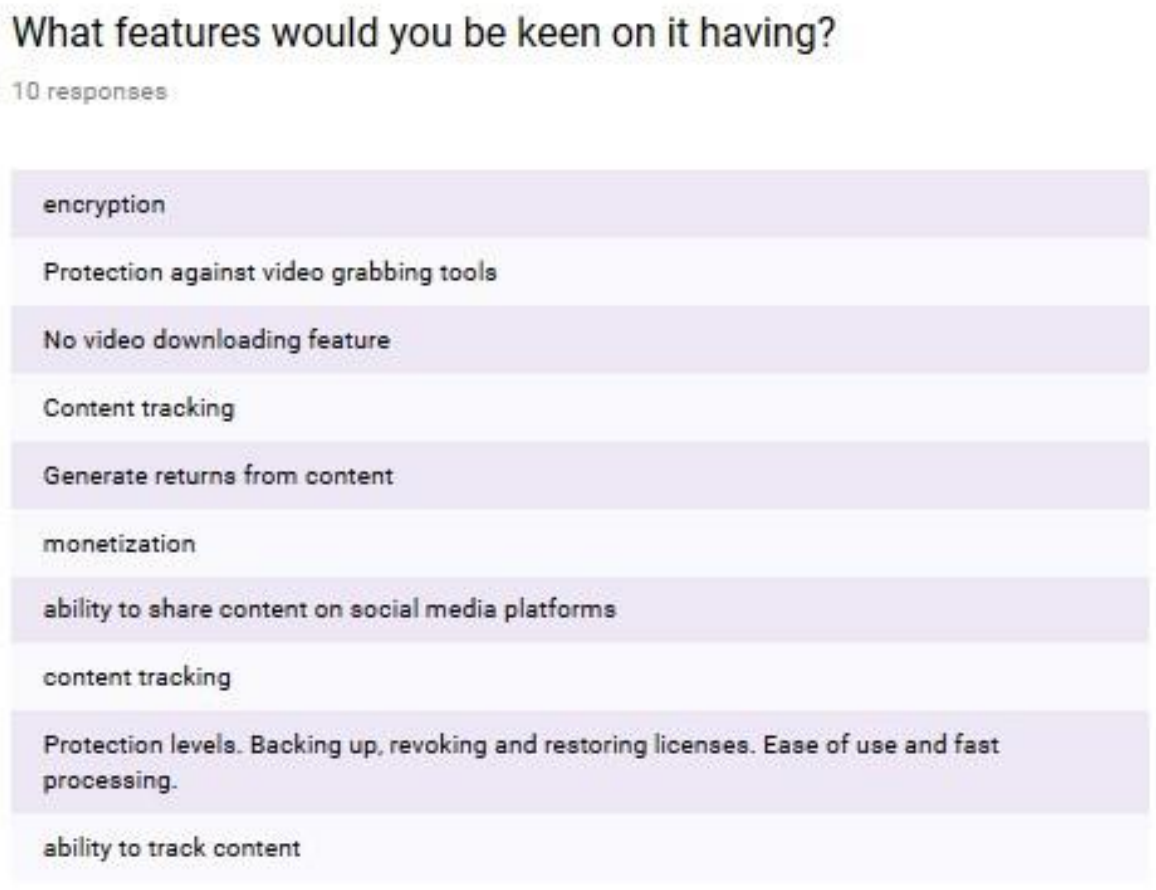
In a scale of 1-10 how much time do you spend protecting your content?

10 responses

If a DRM system that guarantees content protection was developed, would you consider distributing your content through it?

10 responses

Figure C.3 Content Creator Responses - Part C



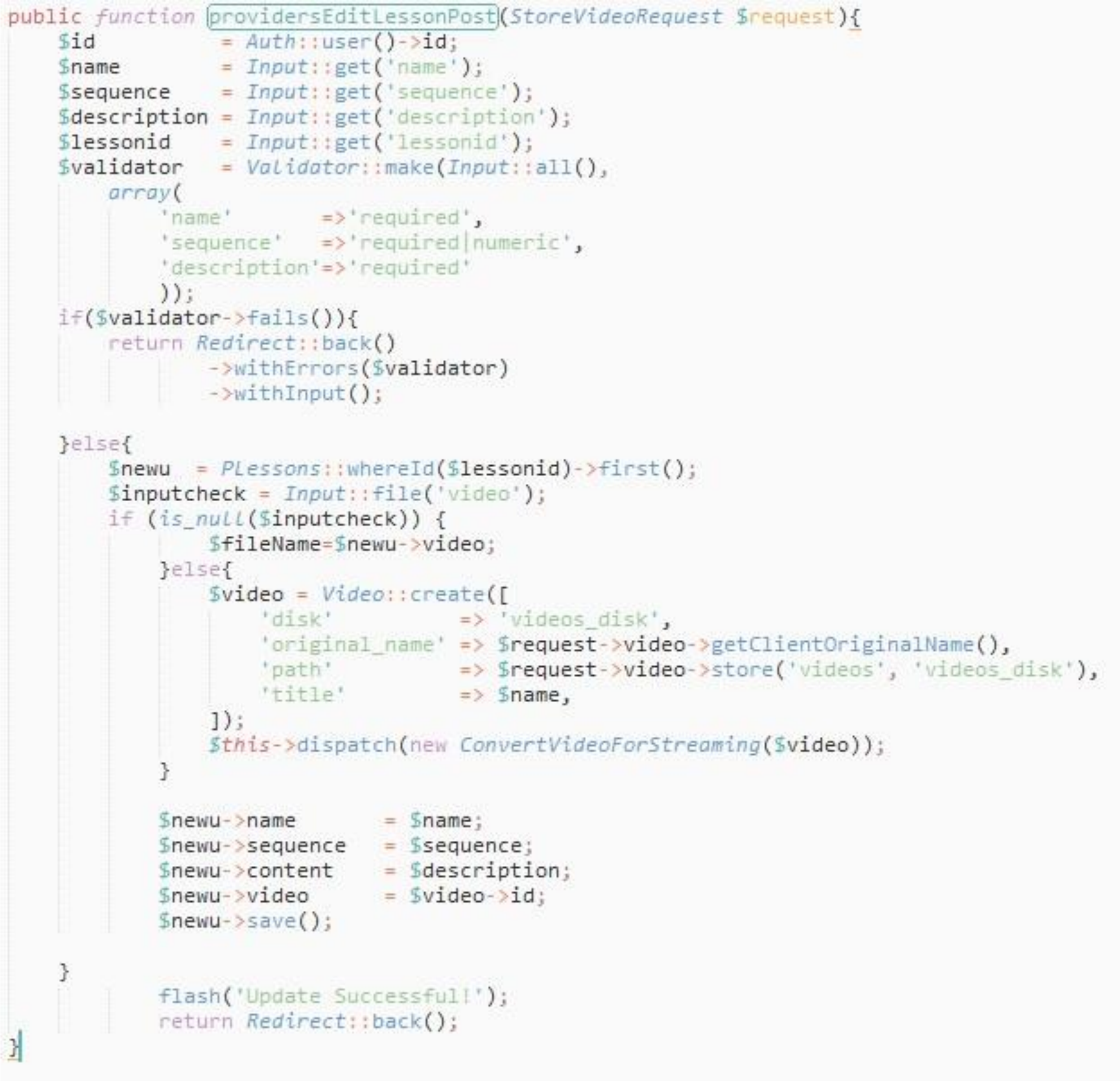
What features would you be keen on it having?

10 responses

- encryption
- Protection against video grabbing tools
- No video downloading feature
- Content tracking
- Generate returns from content
- monetization
- ability to share content on social media platforms
- content tracking
- Protection levels. Backing up, revoking and restoring licenses. Ease of use and fast processing.
- ability to track content

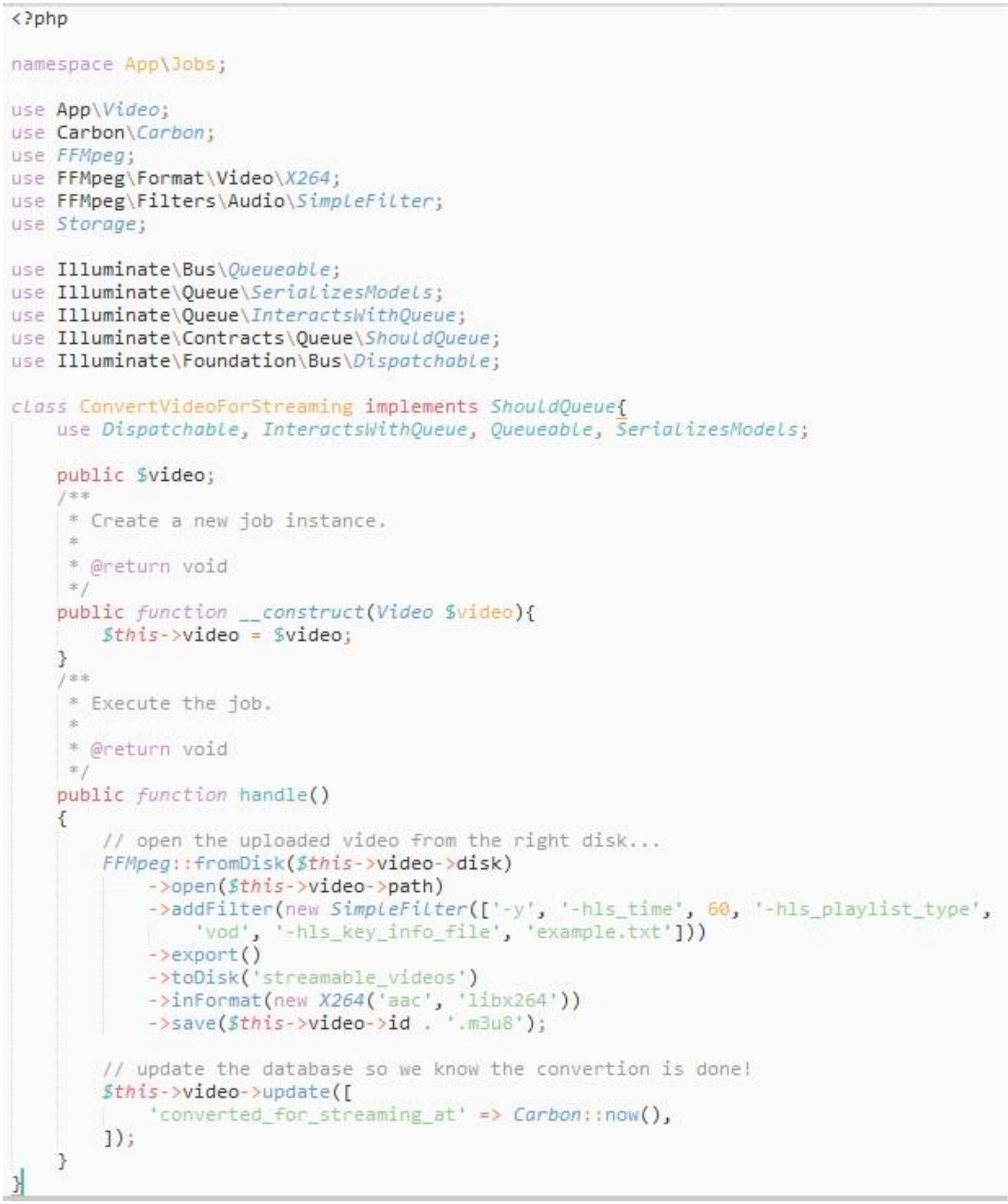
Figure C.4 Content Creator Responses - Part D

Appendix D System Code



```php
public function providersEditLessonPost(StoreVideoRequest $request){
    $id          = Auth::user()->id;
    $name        = Input::get('name');
    $sequence    = Input::get('sequence');
    $description = Input::get('description');
    $lessonid    = Input::get('lessonid');
    $validator   = Validator::make(Input::all(),
        array(
            'name'       =>'required',
            'sequence'   =>'required|numeric',
            'description'=>'required'
            ));
    if($validator->fails()){
        return Redirect::back()
                ->withErrors($validator)
                ->withInput();

    }else{
        $newu  = PLessons::whereId($lessonid)->first();
        $inputcheck = Input::file('video');
        if (is_null($inputcheck)) {
                $fileName=$newu->video;
            }else{
                $video = Video::create([
                    'disk'          => 'videos_disk',
                    'original_name' => $request->video->getClientOriginalName(),
                    'path'          => $request->video->store('videos', 'videos_disk'),
                    'title'         => $name,
                ]);
                $this->dispatch(new ConvertVideoForStreaming($video));
            }

            $newu->name       = $name;
            $newu->sequence   = $sequence;
            $newu->content    = $description;
            $newu->video      = $video->id;
            $newu->save();

    }
            flash('Update Successful!');
            return Redirect::back();
}
```

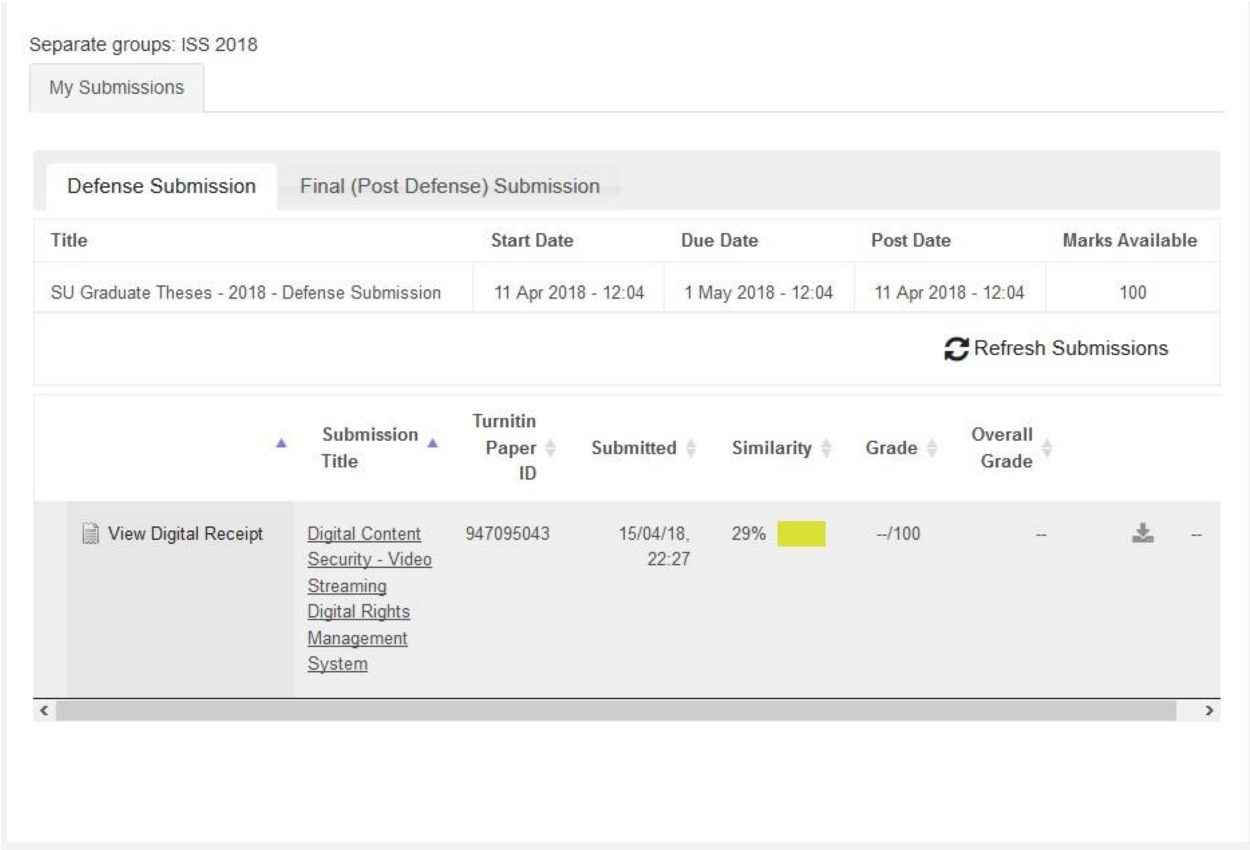
Figure D.1 Lesson Post Function



```php
<?php

namespace App\Jobs;

use App\Video;
use Carbon\Carbon;
use FFMpeg;
use FFMpeg\Format\Video\X264;
use FFMpeg\Filters\Audio\SimpleFilter;
use Storage;

use Illuminate\Bus\Queueable;
use Illuminate\Queue\SerializesModels;
use Illuminate\Queue\InteractsWithQueue;
use Illuminate\Contracts\Queue\ShouldQueue;
use Illuminate\Foundation\Bus\Dispatchable;

class ConvertVideoForStreaming implements ShouldQueue{
    use Dispatchable, InteractsWithQueue, Queueable, SerializesModels;

    public $video;
    /**
     * Create a new job instance.
     *
     * @return void
     */
    public function __construct(Video $video){
        $this->video = $video;
    }
    /**
     * Execute the job.
     *
     * @return void
     */
    public function handle()
    {
        // open the uploaded video from the right disk...
        FFMpeg::fromDisk($this->video->disk)
            ->open($this->video->path)
            ->addFilter(new SimpleFilter(['-y', '-hls_time', 60, '-hls_playlist_type',
                'vod', '-hls_key_info_file', 'example.txt']))
            ->export()
            ->toDisk('streamable_videos')
            ->inFormat(new X264('aac', 'libx264'))
            ->save($this->video->id . '.m3u8');

        // update the database so we know the convertion is done!
        $this->video->update([
            'converted_for_streaming_at' => Carbon::now(),
        ]);
    }
}
```

Figure D.2 Video Conversion Class

Appendix E Turn it in Report



Separate groups: ISS 2018

My Submissions

Defense Submission | Final (Post Defense) Submission

Title	Start Date	Due Date	Post Date	Marks Available
SU Graduate Theses - 2018 - Defense Submission	11 Apr 2018 - 12:04	1 May 2018 - 12:04	11 Apr 2018 - 12:04	100

Refresh Submissions

	Submission Title	Turnitin Paper ID	Submitted	Similarity	Grade	Overall Grade		
View Digital Receipt	Digital Content Security - Video Streaming Digital Rights Management System	947095043	15/04/18, 22:27	29% 🟨	--/100	--	⬇	--