FLEXIBLE CONTENT AUTHORIZATION USING DIGITAL RIGHTS MANAGEMENT IN CLOUD COMPUTING

ALI HUSSAIN

FACULTY OF COMPUTER SCIENCE
& INFORMATION TECHNOLOGY
UNIVERSITI MALAYA
KUALA LUMPUR
2021

FLEXIBLE CONTENT AUTHORIZATION USING DIGITAL RIGHTS MANAGEMENT IN CLOUD COMPUTING

ALI HUSSAIN

DISSERTATION SUBMITTED IN FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF COMPUTER SCIENCE

**FACULTY OF COMPUTER SCIENCE &
INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR**

2021

UNIVERSITY OF MALAYA

ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: ALI HUSSAIN

Matric No: 17028437 / WGA160010

Name of Degree: Master of Computer Science

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"):

Flexible Content Authorization Using Digital Rights Management in Cloud Computing

Field of Study: Cloud Computing

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This Work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature Date: 11th August 2021

Subscribed and solemnly declared before,

Witness's Signature Date: 11th August 2021

Name:

Designation:

FLEXIBLE CONTENT AUTHORIZATION USING DIGITAL RIGHTS MANAGEMENT IN CLOUD COMPUTING

ABSTRACT

Cloud storages are popular for storing the user's data. For the storage provider, complying with all aspects of user privacy agreement and safeguarding the user's personal data is tough. In order to protect the data from security breaches and unauthorized access, Digital Rights Management (DRM) is used for controller access. Applying DRM enable content author of data to have more control over its published or shared content. The use of Cloud storage is common and therefore it is important to improve DRM technology to apply the copyrights policies over Cloud data. This is also important in protecting user's content and providing addition data integrity and intellectual property protection feature as provided by Cloud storage platform. In easy online redistribution model, even authorized user can download the file from Cloud Storage and could easily republish it without prior permission. However, this can pose threat to Intellectual property, may violate copyright policy and may infringe public reputation by propagating false information. This problem is mainly due to the open and inclusive nature of Internet. And more prominent in online social media platform due to their flexible sharing feature which can make false information viral in negligible time. Digital Rights Management (DRM) tends to solve this problem by leveraging more access control to authors of content. Complex encryptions make DRM service difficult to achieve flexibility, interoperability, Cloud deployment and efficient serving. DRM pertains to solve the issue via strong encryption but most DRM authorization mechanisms directly depending on public-key certificates are relatively less suitable to the Cloud. This study presents a review of Cloud DRM technologies available, their features and limitations. This study also represents Macaroons as an alternative method for temper proof and flexible sharing of data over distributed computing. The study demonstrates that the proposed method can provide the immutable data integrity protection with flexible policy definition to limit the access. The integrity of data is verified with the use of HMAC algorithm chain using the verify function of versifier in Macaroon. The study also presents comparison on Macaroon DRM with related studies and performance benchmarking. The proposed method can be added on top of any Cloud storage's and server to achieve controlled sharing in Cloud DRM. The proposed method is found to be flexible, platform independent and easy integration with third party for controlled sharing with an possible unlimited set of authorization conditions.

Keywords: Cloud Computing, Digital Rights Management, Content Protection, Data Security, Distributed Authorization

KEBENARAN KANDUNGAN FLEKSIBEL MENGGUNAKAN PENGURUSAN HAK DIGITAL DALAM PENGKOMPUTERAN AWAN

ABSTRAK

Masa kini, storan-storan Cloud sangat popular untuk menyimpan data pengguna. Bagi penyedia storan, mematuhi semua aspek perjanjian privasi pengguna dan melindungi data peribadi pengguna adalah tugas yang mencabar. Untuk melindungi data dari akses yang tidak dibenarkan dan akses pengawal terdapat teknologi yang dipanggil Digital Rights Management (DRM). DRM membolehkan pengarang data asal mempunyai lebih banyak kawalan terhadap kandungannya yang diterbit dan/atau yang dikongsi. Penggunaan storan Cloud merupakan perkara biasa dan oleh itu penting untuk meningkatkan teknologi DRM bagi menguatkuasakan dasar hak cipta ke atas data Cloud dan melindungi kandungan pengguna selain dari ciri perlindungan privasi dan harta intelek yang disediakan oleh platform storan Cloud. Dalam model pengagihan semula atas talian mudah, pengguna yang dibenarkan boleh memuat turun fail dari storan Cloud dan menerbitkannya semula dengan mudah di tempat lain tanpa kebenaran. Namun, ini dapat menimbulkan ancaman terhadap harta intelektual, kemungkinan melanggar polisi hakcipta dan kemungkinan melanggar reputasi awam dengan penyebaran maklumat palsu. Masalah ini disebabkan oleh sifat Internet yang terbuka dan inklusif. Dan ianya lebih jelas di platform media sosial disebabkan ciri perkongsian fleksibel yang dapat menviralkan maklumat palsu dalam masa yang singkat. Digital Rights Management (DRM) cenderung menyelesaikan masalah ini dengan memanfaatkan lebih banyak kawalan akses kepada pengarang-pengarang kandungan. Penyulitan yang rumit menjadikan perkhidmatan DRM sukar dicapai secara fleksibel, interoperable, pelaksanaan Cloud dan perkhidmatan yang cekap. DRM dilihat dapat menyelesaikan masalah ini melalui penyulitan kuat, namun kebanyakan mekanisme kebenaran berdasarkan sijil kunci awam tidak sesuai dengan Cloud. Kajian ini memberikan tinjauan teknologi ke atas Cloud DRM semasa, ciri-ciri dan batasan-batasannya. Kajian ini juga mencadangkan untuk mengguna Macaroons sebagai kaedah alternatif bagi bukti tahan dan perkongsian data yang fleksibel berbanding pengkomputeran teragih. Kajian menunjukkan bahawa kaedah yang dicadangkan dapat memberikan perlindungan data integriti dengan definisi dasar fleksibel untuk membatasi akses. Integriti data disahkan dengan penggunaan rantaian algoritma HMAC menerusi fungsi verifikasi verifier dalam Macaroon. Kajian ini juga menunjukkan penilaian prestasi sub-operasi Macaroon di dalam bahasa pengaturcaraan yang berbeza. Penyelesaian yang dicadangkan dapat ditambah pada mana-mana storan dan pelayan Cloud untuk mencapai perkongsian terkawal dalam Cloud DRM. Pendekatan yang dicadangkan didapati fleksibel, bebas platform dan mudah disatukan dengan pihak ketiga bagi perkongsian terkawal dengan set syarat kebenaran yang tidak terhad.

Katakunci: pengkomputeran Cloud, Digital Rights Management, Perlindungan Kandungan, Keselamatan Data, Distributed Authorization

ACKNOWLEDGEMENTS

My stay in University of Malaya for this Master’s degree has been the most interesting, challenging, and rewarding years of my life. First of all, I would like to express my sincere gratitude to my supervisor Professor Ts. Dr. Miss Laiha Mat Kiah for her patience and guidance during this journey; the journey that began at the commencement of my Master’s degree. Prof. Miss has been a devoted mentor not only in research, but in many aspects of life. I am grateful for Prof. Miss and the faculty for their tremendous academic support, and for giving me wonderful opportunities during these years.

Of course, this work would not be possible without the support of my beloved parents, siblings and my friends. Their continuous support has given me the strength to finish this study.

Above all, I want to thank Almighty Allah for all the blessings bestowed upon me. HIS benevolence and grace enabled me to accomplish this study.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS AND ABBREVIATIONS

DRM	:	Digital Rights Management l
CC	:	Cloud Computing
HMAC	:	Hash-Based Message Authentication Code
IoT	:	Internet of Things
PKI	:	Public Key Infrastructure

CHAPTER 1: INTRODUCTION

The increasing popularity and use of the Internet, results in huge amount of personalized content being stored in Cloud storage. This leads to private data being accessed as well as shared using heterogeneous devices such as mobile, web, and IoT (Salman et al., 2018). The open and inclusive nature of the Internet allows content to be redistributed, without explicit consent, which may infringe Intellectual property rights. With recent growth in utilizing the cost effective and easy to scale feature of Cloud computing, it is the among popular way of storing online content. However, the protocol and mechanism in Cloud computing are questioned for the greater safety and security of content they store. This is because of paradigm shift from client server to distributed nature of Cloud protocols, which bring new challenges for content security. Digital Rights Management (DRM) is a technology, applied to safeguard the data usually over the application layer so as to prevent illicit usage. Encryptions is usually applied over the data forming a safeguard policy. DRM technologies for Cloud content need to be explored to protect Cloud data from unauthorized usage and efficient revocation. (Q. Huang et al., 2013; Koulouzis et al., 2018; Xu et al., 2017). The unauthorized Cloud content sharing or maneuvering access license may infringe copyrights and online content security policies.

It is necessary to apply technical solutions to mitigate this content misuse threat to online safety. However, implementing strong and computation exhaustive encryption in the distributed mode as well as content serving introduces many performance bottlenecks and constraints such as synchronization, latency, low processing and storage at client and communication overhead (Das et al., 2015; Ma, Jiang, et al., 2018). This overhead needs to be reduced by researching on robust encryption in DRM solutions so as to meet the practical and flexible need for content protection in Cloud computing.

1.1 Research Background

In the recent past, access of online digital media has been the focus of research and it has gained significant importance. Whereas the content protection with optimal performance and flexibility is an emerging challenge. This is because of, the volume of digital data consumed by end user is also increasing tremendously. Which in turn cause rapid improvement in the networking infrastructure, that boosts the usage of information technologies such as audio, video, social media, and Cloud storages as a collaboration platform. This increasing popularity and use bring copyright and data security changes. This is because the traditional security mechanism, at application layers, are not directly applicable Cloud. Therefore, the content security mechanisms are necessary for the safety and security of Internet content in protecting users digital content, protecting confidentiality, data integrity, and prevent unauthorized data access which should meet the practical application requirements such as lightweight and flexibility.

The growing use of DRM is evident for its global adoption and market share. In 2012, the Global DRM market volume was about 1290 million USD and is predicted to increase to 2024 million USD by 2024. The DRM increasing market volume is due to its increasing use in Software, automation, and security layer by implementing it (in office and offshore collaboration storage), by the Public, private as well as industrial scale applications. The benefits of DRM need to be leveraged in the modern applications overs Cloud computing, content storage for large volumes of multimedia files and documents. In the Cloud, extending DRM features requires more stringent technology, to protect digital assets such as e-book, music, movie, etc. Heterogeneous devices accessing the Cloud content suffer poor quality of service due to many protocol bottlenecks. Modern Cloud storage such as Google Drive, OneDrive, Dropbox, and Box and commonly being used as content storage. These Cloud technologies and smart devices are being used for storing and sharing user's online digital content (H. Lee et al., 2016b). DRM in Cloud will allow content owners to share the content with different users and the consumers can access the data according to the access policy attached to it.

This delegation of access in Cloud computing became important due to its many benefits including flexibility and safety. As DRM in Cloud is applied to safeguard the Cloud data as an extra wall of defense from security breaches. The encryption in DRM helps to save unencrypted data exposure and limit its risk of being exposed in case of large scale data theft. The addition of DRM features would help organizations to effectively manage access to business critical personal data held and controlled by Cloud storage. The risk of unencrypted content exposed to unauthorized entities can be reduced by applying digital rights management technology (De Angelis & Di Marzo Serugendo, 2017; C. C. Lee et al., 2018; Munier et al., 2012; Torres et al., 2008).

Data integrity along with immutable licenses is also an important feature of DRM. This makes sure the content is not modified while ongoing communication over the Internet. As DRM encrypts the content data and applies access control mechanisms. Policies are enforced to implement legal access and avoid unauthorized content consumption. This way of saving content inherits the challenges of Cloud computing. Cloud computing suffers from new challenges of lightweight approach flexibility which makes it less suitable for Cloud DRM applications. This requires the Cloud DRM to meet the new requirement of multiple heterogeneous devices such as Smart TV, Smart Watches, Desktop, and many other distributed computing methods (Sicari et al., 2015). The author also proposed (Kishigami et al., 2015; Ma, Jiang, et al., 2018; Zhaofeng et al., 2018) Cloud DRM solution to address this problem.

In all the solutions proposed the strong encryption and integrity chain is complex to realize. However, efficient content protection is necessary to preserve the data ownership and copyright. Thereby, preventing content consumer entity from unauthorized consumption of the shared data in Cloud. The integrity protection mechanism should also give reasonable performance, low overhead, and lightweight operation to meet practical Cloud DRM requirements.

The data serving from Cloud technologies suffer from glitches and delays (Puliafito et al., 2019). The Cloud DRM services which safeguard data, also need to provide optimal performance (Bedi et al., 2018; Chokngamwong & Jirabutr, 2015; Puliafito et al., 2019). This will serve in protecting DRM content in resource constrained distributed computing environment. The latency is mainly due to the geographically distributed nature of the spread of data in the Cloud. Fog computing being an extension of Cloud computing and is emerging paradigm, proposed by the researcher which aim to address the practical limitation of Cloud computing. Fog Computing improves the latency in Cloud computing technologies so that, it satisfies the requirements of delay sensitive applications. Therefore, it is important to discuss the Fog computing paradigm in Cloud DRM to efficiently serve protected data, such as geographically distributed healthcare information effectively (Z. Y. Zhang et al., 2015). Fog computing is hereby introduced to improve the service of delay sensitive Cloud applications. The improved service gives better mobility, and lower communication complexity by moving communication and storage near to the core network of the end user. This would enable the devices and end-users to have better support for low latency application and mobility, by taking the communication near to the edge of their networks.

In general, confidentiality, completeness, and availability of Internet platforms are still a problem with new and evolving online Internet technologies. Constructing scenarios of integrity protection with a focus on flexible protection an active research topic. In the case of Facebook, users may combine these attributes to form privacy management strategies and relies various the personal data privacy strategies. These strategies may differ in terms of local and regional perceptions and demographics for privacy concern, usefulness, and age, gender, and professional experience (Lankton et al., 2017). But DRM features offered by the current DRM technology landscape lacks flexibility to apply them in wider application domain. This is because DRM pertain to solve complex problem. Even authorized users could tamper or potentially fake the content and easily republish it. In a super re-distribution model such as social media, this can pose threat to public reputation and propagate false information (Cheng et al., 2016). This problem is more prominent in online social media platforms and Cloud services due to the sharing feature and social networks are among the most popular services (Serrao et al., 2018). A DRM framework for online social networks (OSNs) was proposed (HUANG et al., 2014) to cater to the need for user privacy protections and control the unauthorized content re-distribution. Critical and confidential business documents are being stored and shared via online Cloud storage and social media platforms (Cook et al., 2017). The use of Cloud storage is very common today and therefore it is important to study DRM technology to enforce the copyrights policies over data. This is necessary to protect the user data integrity in addition to the integrity protection feature provided by Cloud storage platform. Controlled sharing is intrinsic feature of distributed systems; yet, on the Web, and in the Cloud, sharing is still based on basic mechanisms (Joshi & Petrlic, 2013). Most DRM authorization mechanisms are not quite suited to the Cloud scenarios, since they are based on more expensive methods that can be difficult to implement lightweight approach in verifying data integrity.

1.2 Motivation of Research

In the recent years, the research trend on Internet security, more focused on securing the Internet Backbone and Cloud as an infrastructure; however, the content security is potential area to be researched further. The content security domain could help in securing the content in extreme data theft scenarios. For example, in the scenario of a data breach, after the data breach happened, the end user data would be left as it is for malicious users. DRM could help to prevent unencrypted data disclosure by employing the content protection mechanism. Through this, DRM could also provide an extra layer of content security.

Current DRM landscapes have many content protection techniques. The popular one uses the methodologies of watermarking (Hou et al., 2018; Iftikhar et al., 2017; Kwon et al., 2016; Ma et al., 2016; Subramanyam et al., 2012), steganography (De Angelis & Di Marzo Serugendo, 2017; Mtech, 2015), image and video encryption (Thanh & Iwakiri, 2016) and Blockchain (Ma, Huang, et al., 2018; Ma, Jiang, et al., 2018). All of these methodologies have a bottleneck of performance and especially, in the case of large scale deployment and serving such as Cloud computing. This is mainly because of the complex encoding and decoding algorithm. The small handheld devices have relatively low computational, storage, and internet capabilities. Therefore, the protected content distribution and consumption suffer from bad performance thereby leaving relatively less room for flexibility. This performance further degrades, when serving scattered and large amounts of time-sensitive critical data for Cloud. Currently, a large amount of user's data is being stored on Cloud based storage providers in multi service model. The strong encryption based mechanism is insufficient to deliver the optimal DRM services (Singh et al., 2019). A recent study attempt to address this problem through efficient Key-Aggregate Cryptosystems with Broadcast DRM techniques for Cloud computing. Aggregate Keys Users would be able to decode many classes of data using only one key. That key is also of fixed size, so it could be easily sent to many users (Sachan et al., 2012). Many researchers have proposed DRM technologies, so that, they would be suitable for heterogeneous smart devices and the interoperability among various DRM technologies (H. Lee et al., 2016a). These techniques lacks practicality, and the proposed solutions are not applicable to meet the next generation performance needed. Therefore, more stagnant

Cloud DRM technologies are needed. Currently, the Fog paradigm is rapidly adopted to provide multi-tier, on-demand, flexible, and cost effective services to users. Legacy client server data and database hosting are being replaced with Cloud hosting, to enjoy these benefits. The Fog computing will solve latency problem in Cloud computing which will in turn ease out lightweight cloud DRM. Hance, DRM in Cloud would grow more and more important; especially for protecting content (P. Hu et al., 2017). The trustworthiness of the computing unit which is responsible to process the data is also important and could be assessed, if data integrity is safeguard. As in, software as a service (SaaS) model, the computing devices of service provider consumes the critical and confidential data of the source organization. The data source organization losses direct control over the data they provided (Zafar, Khan, Suhail, et al., 2017). This leaves data owner at risk of data theft or data misuse. In service-oriented architecture, it is possible to authenticate the integrity of untrusted middleware data processing element (J. Huang et al., 2014). Due to this data immutability demand has gained as security by design. The research on Blockchain based method for leveraging content immutable benefits is growing. The proposed methods utilize elliptic curve encryption and heavy miner network to safeguard data integrity and safeguard data tempering when access is delegated. However, the Blockchain based solution for DRM partiality meet overall performance challenges. Implementation of distributed system is difficult and Cloud computing is stack of technologies so more studies are needed to design lightweight Cloud DRM method.

Message authentication code (MAC), sometimes known as a tag, is method used to authenticate a message. The specific type of message authentication code (MAC) depend on cryptographic hash function and secret cryptographic key is called Hashed Message authentication code (HMAC). Macaroon (Birgisson et al., 2014) are HMAC based bearer token which were first presented in 2014. Their mechanism allows to create an immutable signature to help delegate Internet resources just like cookies used in Internet browsers.

However, Macaroon is more flexible and lightweight at the same time it's immutable or temper proof in nature as it builds chain of authorization proof of data and signatures. This chain of lightweight signature has been found suitable to implement lightweight and robust DRM for large distributed systems. These feature of Macaroon together with easily interoperable, makes it a good candidate for Cloud DRM in secure content sharing and controlled content authorization in collaboration scenarios. This will be explained further in Chapters 2 and 3.

1.3 Problem Statement

Cloud computing and distributed protocols are popular in storing critical data. The Cloud DRM needs to manage the access to data from not only the unauthorized but also from a licensed consumer as well as by attenuation. This is applied to limit the risk of further unauthorized data leakage, which is complex to mitigate - this is growing risk for distributed Cloud storage.

The safe and responsible use of data, over the Internet, consumed by ubiquitous devices required significant improvements in the protocol. Platforms that support social networks such as Facebook, LinkedIn, Instagram, and Twitter have millions of users across the world. Designing an efficient content authorization protocol for Cloud DRM is a challenge due to the geographically distributed nature of Cloud storage. The Use of Cloud for data storage is common for documents and useful information (H. Lee et al., 2016a, 2016b). For the content owner, the controlled sharing of copyright content is a significant challenge. The token based approach is popular these days but it creates overhead and not efficient for revocation. Recent studies have shown a trend to use cryptographic primitive for trusted, light-weight, and controlled sharing (Y. Zhang et al., 2017). However, the practical requirement of data trustworthiness, dynamic policies, and efficient revocation for distributed consumption is still a problem (Y. Zhang et al., 2017).

The access delegation in Cloud storage is with strong integrity protection is necessary for Cloud DRM.

Presently, the flexible solution for strong data integrity and authorization are lacking in Cloud DRM. As DRM in Cloud and its dependences are being discussed by few researchers (Alsaghier et al., 2017; J. Huang et al., 2014; H. Lee et al., 2016a; Yao et al., 2019; Zafar, Khan, Malik, et al., 2017) and recently Blockchain based DRM is also proposed as in build temper proof data integrity protection method (Ma, Jiang, et al., 2018; Savelyev, 2018; Zhaofeng et al., 2018). As the Cloud storages are growing with features like elasticity, pay-as-you-go, business continuity for long term retention and risk mitigation through data theft attacks. DRM solutions, with strong encryption, face challenges to satisfy the practical deployment and flexibility integration need, both within or across system. The effort to implement Blockchain based solutions are also not directly suitable for lightweight and flexible content delivery requirements. The robustness and high-level secure DRM based Blockhchain. To prevent copyright violations in Manufacturing and logistics researcher has proposed Bloackchain based solution (Holland et al., 2017). Another study (Millar et al., 2018) proposes to implement Macaroon to facilitate the use of storage to maximize the gain from stored data, including quality-of-service management, heterogeneous systems. This study presents an alternative approach for flexible authorization for Cloud DRM with an immutable license and easy attention. It is theoretically impossible to remove the access restriction impose but authorized users can add additional contextual access policies. This allows users to further specify the contextual condition to limit the authorization scope. The corresponding server face lightweight immutable resource authorization method, which is suitable for Cloud DRM. Contextual parameter appended to licenses and provide the feature to further limit the license as chain of integrity. This way the policy is traveling independently of data just as a bearer token and HMAC is governing its integrity. During literature review, the Macaroon approach to DRM is not yet explored in literature and this study aims to apply and evaluate the Macaroon approach to DRM in Cloud, for realizing lightweight, more practical, and flexible DRM benefits.

1.4 Research Objectives

Cloud computing adoption has been significant as remote, on demand, cost effective and revolutionary data storage. This adoption has overwhelmingly increased the volume of person and business critical data stored in these cloud storages which is often shared for collaboration. This data sharing required additional access control technologies supporting the cloud benefits. However, cloud DRM technologies lacks flexible and lightweight solutions. This is because the traditional authorization mechanisms lacks practical aspects. The multi layer Cloud DRM architecture with multi party interaction couldn’t be satisfied by the static token based authorization mechanism.

This research aims to address the need for flexible and temper proof licenses, by proposing an alternative approach for Cloud DRM. The proposed approach provide strong license integrity, flexible re-attenuation of license and, lightweight implementation for protecting and verifying data integrity in Cloud DRM.

As to achieve the aim stated, the main objectives of the research are:

- To review the state of the art DRM technologies proposed for protecting the intellectual property of online content in a distributed computing environment.
- To propose an alternate approach to DRM using Macaroon for flexible and temper proof integrity protection mechanisms in Cloud DRM.
- To evaluate Macaroon approach for Cloud DRM by comparison with other Cloud DRM approaches and analyze the optimal benchmarking of Macaroon libraries.

1.5 Research Gap and Significance

The literature review of salient DRM methods shows most of the existing DRM methods add an extra level of complexity and performance tradeoff. This study represents Macaroons as lightweight, flexible, and tamper-proof authorization token. Because of the salient attribute of Macaroon as it carry its own proof of authorization with integrity tracking by design. This can help in realizing immutable integrity protection methods and flexible policies for DRM in Cloud. The proposed method is analyzed and critically discuss how the Macaroon approach could achieve tamper-proof and flexible authorization in Cloud. Macaroon based solution is constructed using HMAC chain. The Macaroon feature with the flexibility to add unlimited caveats and its temper-proof nature of HMAC chain generate lightweight credentials. These credentials are better than the existing authorization techniques used in Cloud DRM. This will ease out efforts to make Cloud DRM flexible and efficient in resource constraints distributed environments.

1.6 Research Scope of the Study

This study is focused in assessing the Macaroon ability for DRM as an access delegation method, for next-generation temper proof authorization method in Cloud DRM. The thesis analyses Macaroon’s operation cost and flexibility and compared the computational cost with related cloud based integrity protection in Cloud DRM - for temper proof lightweight access delegation mechanism which better suites modern Cloud DRM scenarios. This study assumes Public Key Infrastructure (PKI) based underlying architecture is assumed to be secured. The PKI protocol stack security is excluded from this research such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS), etc.

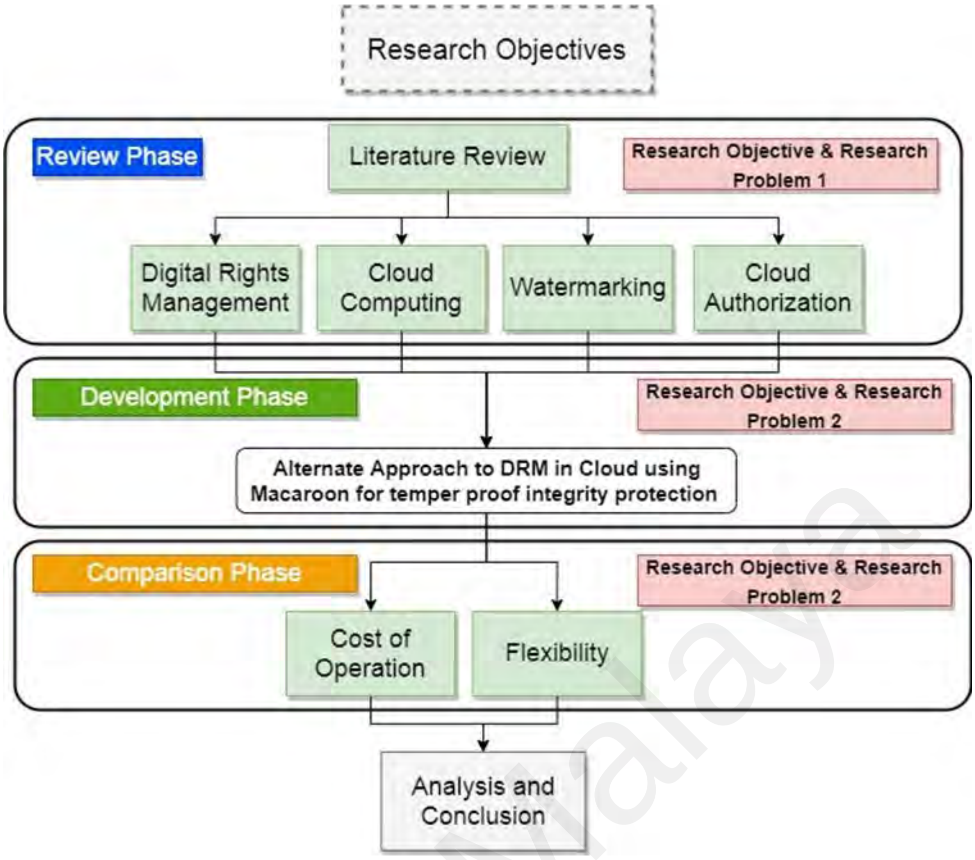

Research Objectives
Review Phase
Literature Review
Research Objective & Research Problem 1
Digital Rights Management
Cloud Computing
Watermarking
Cloud Authorization
Development Phase
Research Objective & Research Problem 2
Alternate Approach to DRM in Cloud using Macaroon for temper proof integrity protection
Comparison Phase
Research Objective & Research Problem 2
Cost of Operation
Flexibility
Analysis and Conclusion

Figure 1.1: Brief Summary of Proposed Research Methodology

1.7 Contribution of Research

The contribution of this research is to generate new knowledge in the area of DRM and introduce an alternative approach to controlled authorization in Digital Rights Management (DRM). The following steps were followed to achieve the objectives of this research.

- A comprehensive review of the recent applications of DRM for Cloud DRM was undertaken to identify the impact of DRM quality of service and usability. The articles for literature review were taken from prominent scholarly digital libraries and databases named; ScienceDirect, IEEE, Springer, Google Scholar, Wiley and ACM. The impact of the existing Cloud DRM authorization was also reviewed, and taxonomy for the Cloud DRM was also proposed.

Significant research gaps were discovered as a result of literature review along with the problems needed attention in order to address them.

- The problems were thoroughly investigated as per their corresponding significance was validated using empirical case study analysis. The performance was evaluated to verify the computation cost and significant potential of the methods against related studies.
- The performance of the proposed method was evaluated via a series of test case analysis. The cost of operation involved in authorization proof generation and verification was evaluated. The time to perform a DRM feature, degree of variety of dynamic policy support, and in-built features of Macaroon opted as performance metrics in this evaluation. The results of performance evaluation were validated using comparison with the results of other recent methods. The detailed research methodology will be presented in Chapter 3.

1.8 Research Contribution

The contribution of this research is to generate new knowledge in the area of DRM and introduce an alternative approach to solve the complex problem of flexible, lightweight, and immutable integrity protection mechanism in Cloud DRM. This study also highlights a different kind of DRM primitives that are suitable for practical and efficient and controlled authorization in distributed computing. As Macaroon approach is found to be a good invention and this study leverage the Macaroon benefits in implementing a flexible and temper poof DRM system. This study also explains the scenarios in which it can protect the content from unauthorized usage.

Many Internet users prefer to use the DRM content without paid licenses. Therefore, the DRM service offers a limited trial license in DRM free model, where one could have free access to limited content. In the current market, DRM service is costly regarding prices for users and the efforts of developers as device manufacturers and developers need to produce all the necessary components to support heterogeneous devices and services. Therefore, it is much needed to standardize DRM (Serrao et al., 2003). Standardization would help to reduce the development efforts and boost the DRM technology applications and usage. The Cloud storages are not the only prominent host of user's data over the Internet, but the online social network also accounts for growth in digital data (both static and dynamic content). Once the user's data entered the premises of the third party server, the data owner loses control over its data and there is limited integrity tracking support for users. There is need to increase the clarity of rights and visibility of personal data to the owner needs to be increased. Social media platforms do add the default content privacy-preserving feature of online social networking tools. With the hope to satisfy the user privacy and intellectual property requirements, but that has a very limited scope and features hence, no satisfactory for end users. The content owner needs to have extended control over its content after it is shared with a third party. Some DRM techniques rely on the trusted central platform. In this regard, a popular layered architecture based concept DRM in Cloud that provides some DRM functions in the Cloud environment (J. Huang et al., 2014; H. Lee et al., 2016a). Despite the large scale adoption of Cloud computing the industry and critical business documents are being stored in Cloud-based storage providers for safekeeping, reliability, and easy access to documents in collaborations. This make is vulnerable to content manipulation threats of further sharing the copyright data, without the consent of the actual document owner. Researchers are concerned about the content security, content intellectual property rights violation, content privacy, and integrity of data stored in the Cloud (Alsaghier et al., 2017; Yao et al., 2019). Content in Cloud based storage provider but still more research is needed in this area to address the content security as it leaves users premises. Moreover, how the content owner can have necessary control over its data stored in Cloud. Finally, a transparent data access policy when the data is being processed and shared with other services.

1.9 Thesis Structure

The further part of this thesis is organized into section and sub sections as represented in Figure 1.2. Chapter 2 reviews the research performed in the field of DRM and Cloud computing. This Chapter provides knowledge of DRM as well as reviews applications of Cloud and Fog DRM to highlight and present the state of the art of the research landscape and limitations.

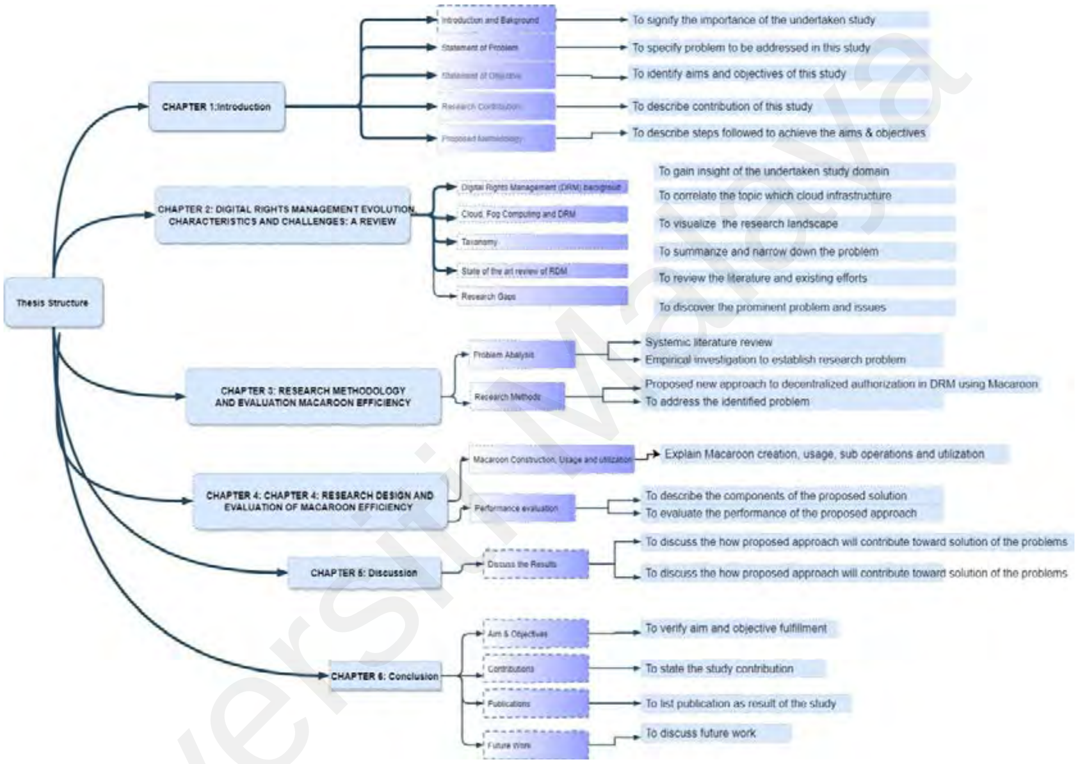

Thesis Structure
CHAPTER 1:Introduction
Introduction and Bakground
Statement of Problem
Statement of Objective
Research Contribution
Proposed Methodology
To signify the importance of the undertaken study
To specify problem to be addressed in this study
To identify aims and objectives of this study
To describe contribution of this study
To describe steps followed to achieve the aims & objectives
CHAPTER 2: DIGITAL RIGHTS MANAGEMENT EVOLUTION, CHARACTERISTICS AND CHALLENGES: A REVIEW
Digital Rights Management (DRM) backgroud
Cloud, Fog Computing and DRM
Taxonomy
State of the art review of RDM
Research Gaps
To gain insight of the undertaken study domain
To correlate the topic which cloud infrastructure
To visualize the research landscape
To summarize and narrow down the problem
To review the literature and existing efforts
To discover the prominent problem and issues
CHAPTER 3: RESEARCH METHODOLOGY AND EVALUATION MACAROON EFFICIENCY
Problem Abalysis
Research Methods
Systemic literature review
Empirical investigation to establish research problem
Proposed new approach to decentralized authorization in DRM using Macaroon
To address the identified problem
CHAPTER 4: CHAPTER 4: RESEARCH DESIGN AND EVALUATION OF MACAROON EFFICIENCY
Macaroon Construction, Usage and utilization
Performance evaluation
Explain Macaroon creation, usage, sub operations and utilization
To describe the components of the proposed solution
To evaluate the performance of the proposed approach
CHAPTER 5: Discussion
Discuss the Results
To discuss the how proposed approach will contribute toward solution of the problems
To discuss the how proposed approach will contribute toward solution of the problems
CHAPTER 6: Conclusion
Aim & Objectives
Contributions
Publications
Future Work
To verify aim and objective fulfillment
To state the study contribution
To list publication as result of the study
To discuss future work

Figure 1.2: Symbolic Presentation of The Thesis Outline

CHAPTER 2: DIGITAL RIGHTS MANAGEMENT EVOLUTION, CHARACTERISTICS AND CHALLENGES

This Chapter presents a thorough survey on Digital Rights Management (DRM) landscape its evolution, taxonomy, and state of the art DRM techniques used by researchers. This article also adds the stakeholder's knowledge by highlighting the DRM deployments in the Fog computing service. However, Fog computing is mostly tied to the IoTs, it is important to note that, its use is applicable in several other contexts, e.g., content package, license management, key management, and content encryption and audit functions. There are issues of real time multimedia content delivery in Cloud due to its geographically distributed nature, Fog Computing tried to reduce the latency problem. This Fog Computing is also useful for Cloud DRM. Many significant efforts and past studies have been performed on this domain in literature.

To achieve temper proof credentials in Cloud Blockchain based solutions are also proposed, However, after careful review Fog based approach is found to be efficient and flexible for DRM implementation in Cloud computing. A review paper has been published which proposes the use of Fog computing based DRM for efficient DRM service in distributed computing. Figure 2.1 presents the organization of this Chapter in details.

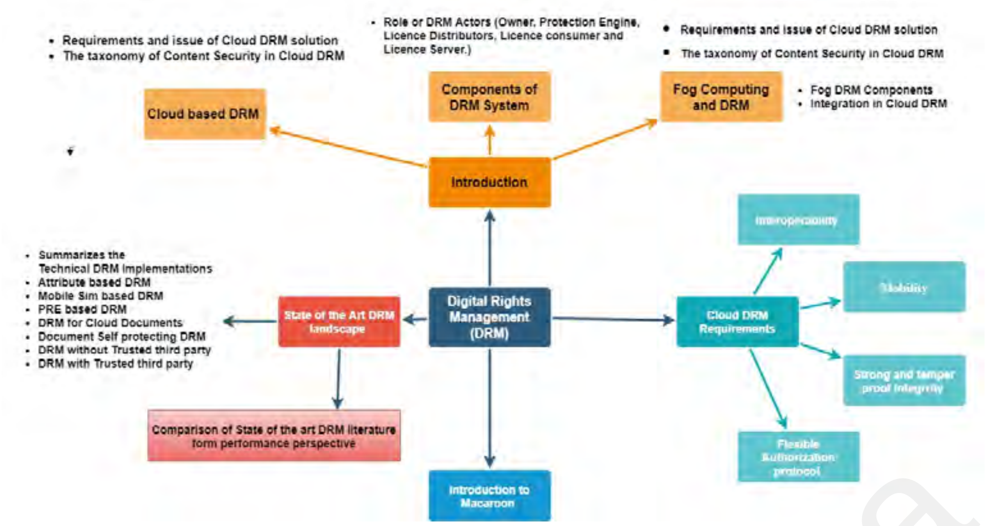

Requirements and issue of Cloud DRM solution
The taxonomy of Content Security in Cloud DRM
Role or DRM Actors (Owner, Protection Engine, Licence Distributors, Licence consumer and Licence Server.)
Requirements and issue of Cloud DRM solution
The taxonomy of Content Security in Cloud DRM
Cloud based DRM
Components of DRM System
Fog Computing and DRM
Fog DRM Components
Integration in Cloud DRM
Introduction
Interoperability
Mobility
Summarizes the Technical DRM implementations
Attribute based DRM
Mobile Sim based DRM
PRE based DRM
DRM for Cloud Documents
Document Self protecting DRM
DRM without Trusted third party
DRM with Trusted third party
State of the Art DRM landscape
Digital Rights Management (DRM)
Cloud DRM Requirements
Strong and tamper proof integrity
Comparison of State of the art DRM literature form performance perspective
Flexible Authorization protocol
Introduction to Macaroon

Figure 2.1: Semantic Presentation of Chapter 2

2.1 Introduction

With the growing use of information technology, online computing and storage systems, and applications are used in daily life. User's data from personal files to commercial and critical business and industry process documents are being stored in some Cloud hosting (D. Wang et al., 2018) and then they are shared with other entities for collaboration or any other purposes. Protecting the documents when it leaves the content owners premises is a significant area of research. Data integrity, confidentiality, security, and reliability control are the main challenges faced by Cloud DRM. In order to use DRM technology in protecting data, that may involve; authentication, authorization, licensing, payment, usage control, privacy protection, access violation detection, and access revocation. DRM involves content owner who owns the content and license server is used to generate a license, for the content. The license is generated for the authorized user to present and access the resource. The license or key distribution server transport the license. The content protection engine generates the license. The details of each are described in the following sections. In general DRM system consists of five main components as shown in Figure 2.2.

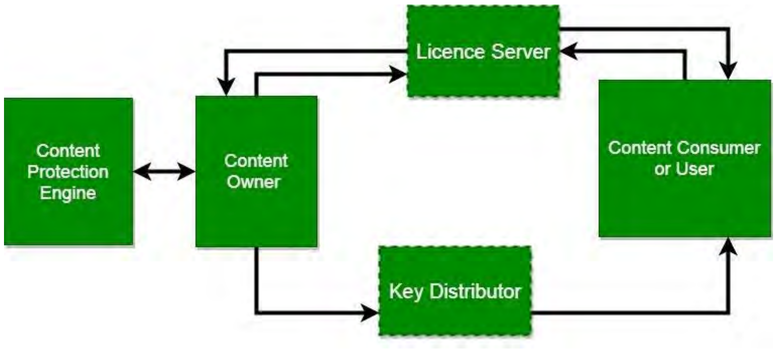


Figure 2.2: Components of DRM System

2.1.1 Content owner

The data owner with all the rights and intended to protect its content, using DRM technology. It also intends to share the data with the authorized user. The content owner provides its content to the protection component either in the encrypted or unencrypted format. After the content is protected, the usage license is returned to the content owner.

2.1.2 Protection Engine

This component encrypts the content and shares the content usage license and protected content with the content owner. This essentially applies encryption technique over content, to transform content into a format that can be subjected to licensing and user authentication eventually.

2.1.3 Key Distributor

After protecting the content, the owner needs to distribute its protected content an key, by using the key distribution component and usage licenses with the license server. The distribution could be through hardware drive or peer to peer software storage over the Internet.

2.1.4 License User

The user fetches the Protected Content from the distribution medium and extracts the information of the license server; usually from the metadata of protected content, that with information about the license server. After that, it contacts the license server to pay the license fee. Once the license fee is paid successfully, it receives the license key for the content.

2.1.5 License Server

The license server is used to issue the license to the user and also it provides the key to the content owner, updates the license usage, and executes the pricing usage policy. In case of fraud or security threat, it also responsible for user access revocation. Licenses generated during content protection are sent to the license server via the content owner. The license server is a trusted authority for authenticating the users and also capable of building user profiles and usage statistics.

As discussed in previous paragraphs, DRM technology regulates the use of digital content with the help of hierarchical components. The analysis report, authorizations, logging, and management of the tangible and intangible rights of corresponding company (Boucqueau, 2017; Munier et al., 2012). DRM includes relatively specialized technologies, such as encryption, proprietary encrypted file formats, Public Key Infrastructure (PKI), Advance attribute-based encryption, and watermarking. It also can be extended to business management in the process of licensing, data collaboration, documentation, and conditions for use. Using DRM technologies e-Book platforms are enforcing access policies that enable them to restrict unlawful use of copyrighted works publishers. Google, Amazon, and Microsoft also have their DRM services to protect the media content hosted in their storage.

2.2 Cloud Based DRM

Cloud based DRM is the application of DRM technology to safeguard data stored and access from Cloud. Cloud DRM manages the access control and authorization for its content and acts as a mechanism of enforcing the access policies. Cloud computing follows the N-services model in which the stored data could be consumed by diverse computational devices (e.g. Internet of Things devices, Desktop or Mobile, etc.) and thus provides easy and flexible access to the Cloud resources. Today is the era of Mobile technologies and with the use of high-speed internet, e.g. EDGE/3G/4G/5G, the mobile devices, though have limited memory, processor, and battery power are now trying to satisfy user performance expectations by offloading the processing to Cloud and thereby sharing their processing load to the Cloud. Consequently, there is an increase in depending on Cloud data storage providers to store the user's content. To effectively protect the contents by applying versatile DRM policies, many studies have been done by the researcher to propose efficient DRM in Cloud. We discussed those state of the art techniques in the following section.

The recent increase in the utilization of Cloud computing has tremendously increased the use of data sharing features for various applications. The decreased dependency on geographical distance would help in engaging bulk of users, in real time. Currently, both the private and public sector enjoying massive data hosting in Cloud, and it's sharing as a mechanism to enhance organizational efficiency. Cloud based DRM provides the Cloud consumers with content security services. Cloud based DRM is much needed in today's IT revolution (Patranabis et al., 2017). Cloud computing has changed the paradigm of data services being used in academics, medical science, economics, e-commerce, and online social networking. In addition to the benefits of Cloud DRM solutions, many users sitting in the different parts of the world could effectively collaborate, share, and exchange data with flexibility and convenience. The use of Cloud storage is currently increasing as individuals and organizations are relying on it for next generation storage and collaboration purposes. In the generic Cloud DRM, the consumers are the end user smart devices that utilize the protected content. And DRM Cloud developer builds API for DRM Cloud services. The content owner provides the content, and the user has to request for usage license from the license server in Cloud. These entities constitute the application layer of Cloud DRM.

In the service layer, the servers for license management, key management, domain management, and content packing modules are working together to build the functional service of Cloud DRM. All these components communicate with the application layer, using a central entity called DRM proxy (Chen et al., 2014). The core services of Cloud DRM developed by the developer are part of this layer. The platform layer contains the core entities performing encryption; decryption of content, license crating license updating, and so on. Finally, the storage layer contains the physical server and database for storing the licenses and user details.

Despite all its benefits, the data stored in Cloud storage is potentially vulnerable to data integrity breaking, privacy leaks, and other online security attacks. Due to ledagy methods it does not quite suitable for delay sensitive applications like screaming and quick-response scenarios. The main strength of Cloud based DRM is its flexible and easy data sharing and access from multiple devices. The Cloud DRM inherits the challenges of both Cloud computing as well as efficient DRM. It is important to highlight the key characteristics of Cloud DRM to identify the research gap and issue of strength of Cloud DRM

Generally, data stored in Cloud storage provider is considered secure, because of the distributed nature of Cloud architecture and the legacy network attacks are not effective. The user is always concerned about the security of their content and layers of protection technique. The service of Cloud based DRM needs to be efficient and licenses need to be temper proof, as it protects the critical document and highly confidential data of corporate and individuals. The Cloud based DRM service should have minimal latency and very responsive. Following are a few building blocks of generic DRM features.

- **Context Awareness:** Access rights are formalized as algorithms in the license, which need processing to determine a particular user have a valid right to consume content at a particular time and location. Cloud didn’t support the location aware services, so there is a need to revise the paradigms for Cloud DRM services (Cheng et al., 2016).
- **Users privacy:** Not only the security of data itself but the user’s personal information should also persevere, and there should be no possibilities to build the user’s profile.
- **Data Integrity and Confidentiality:** In real time, the content should not be consumed by unlicensed users as well as the Cloud service. Content privacy and integrity must remain intact when data is moving from Cloud to consumer and vice versa.
- **Key Distribution Overhead:** Fog computing could be used to deliver localized content and could help in reducing the key distribution overhead.
- **Efficient User Revocation:** The data owner must be able to prevent access to any malicious user’s access rights to data without affecting other legitimate users in the group. And this should support the quick action in real time. The taxonomy of the security aspect of DRM is presented in Figure 2.3.

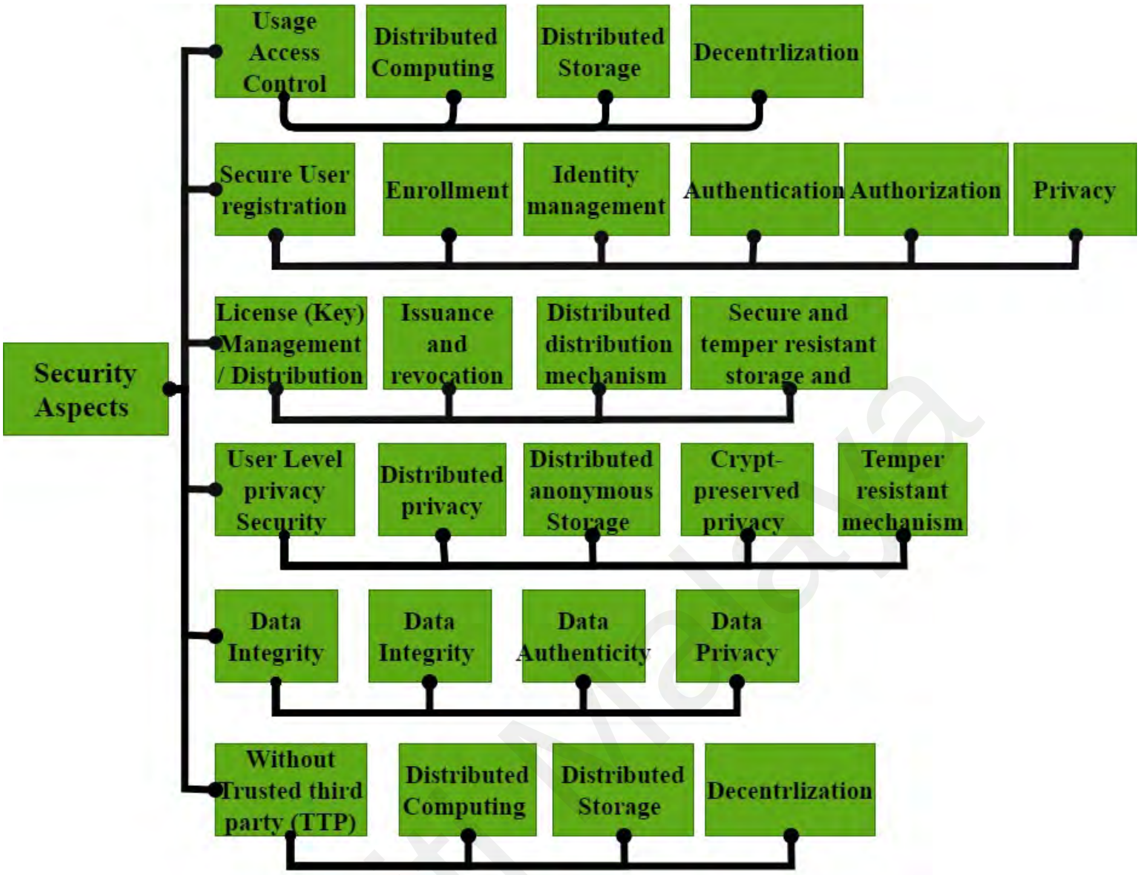


Figure 2.3: Taxonomy of Cloud DRM

2.3 Fog Computing and DRM

Fog computing concept is important in the heterogeneous computing environment when many devices sending data to the Cloud for processing. However, by the time data reaches the Cloud for processing it is too late to draw information out of it due to its real-time nature. It forms a new paradigm for delay sensitive applications is used and it is called Edge Computing or Fog computing. In the practical deployment of Cloud system Fog deployment architecture is mostly preferred for its suitability for latency sensitive application. Therefore, we discuss the DRM in Fog, its architecture, and components for DRM. Many future computing services will potentially use Fog Computing based Systems. This section provides provide new insights into the design and management of resilient Fog based DRM systems.

The basic principles of Fog computing are as following:

- Processing the real-time or streaming data at the edge of the network, physically close to where it originates, and facilitate transferring large amount of real-time data to the geographically distributed large Cloud.
- Process the data at the edge of the Cloud in no time depends on the policy
- Send relevant data to the Cloud storage for data intelligence and other statistics building.

Figure 2.4 graphically illustrates this Fog computing paradigm.

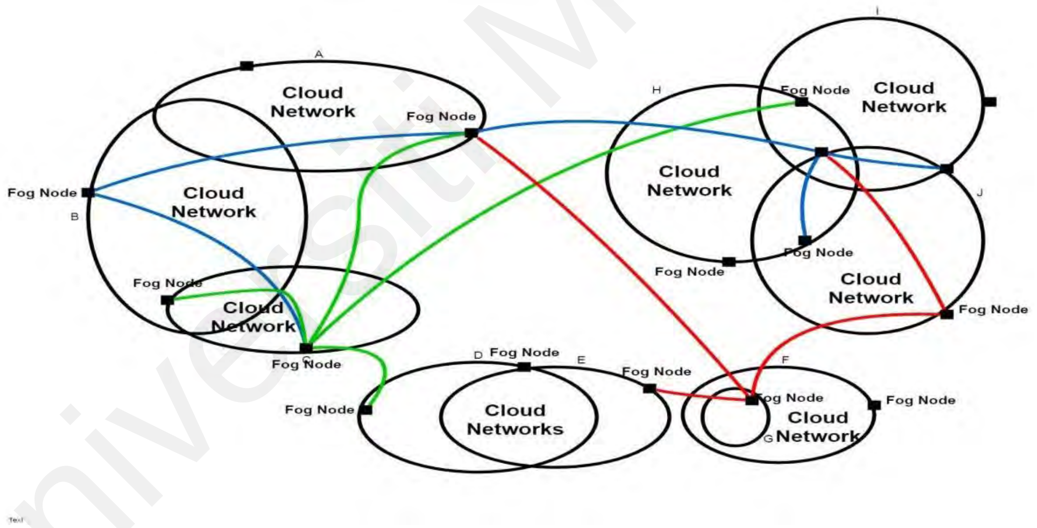


Figure 2.4: Fog Nodes in Cloud Computing Environment

Fog computing is modern paradigm that pertains to solves the limitations of Cloud computing and offers services to the Edge of the network whereas, in Cloud, a centralized processing approach is followed. Fog computing is suitable when more widely distributed context-aware that data is needed to be stored and accessed in real-time. Fog computing as a new paradigm is a good candidate for DRM in Cloud to fulfill the requirements, fast availability to the device, fast response to content producer and consumer, less processing overhead on Cloud, real-time analysis, and decision making with Cloud and so forth. Secure and efficiency is a problem to be addressed in the context of Cloud DRM (J. Huang et al., 2014).

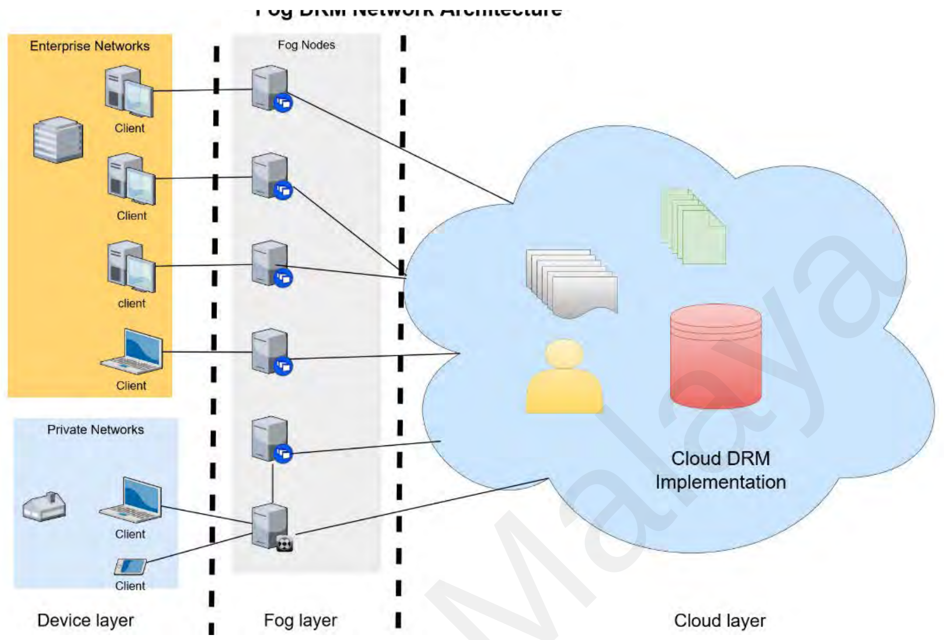


Figure 2.5: Fog DRM Layered Architecture in Cloud Computing

2.3.1 Fog DRM Architecture

Fog computing is a new paradigm, which extends the traditional Cloud computing and services to the edge of the network. It provides computational, communication, controllers, storage, and services capabilities at the edge of the network. The decentralized platform is different from other conventional computational models in architecture. In this section, we summarized the architecture and characteristics of Fog computing DRM, as compared to Cloud DRM, and what limitations of Cloud DRM could be solved by employing Fog DRM (A. Hussain et al., 2020).

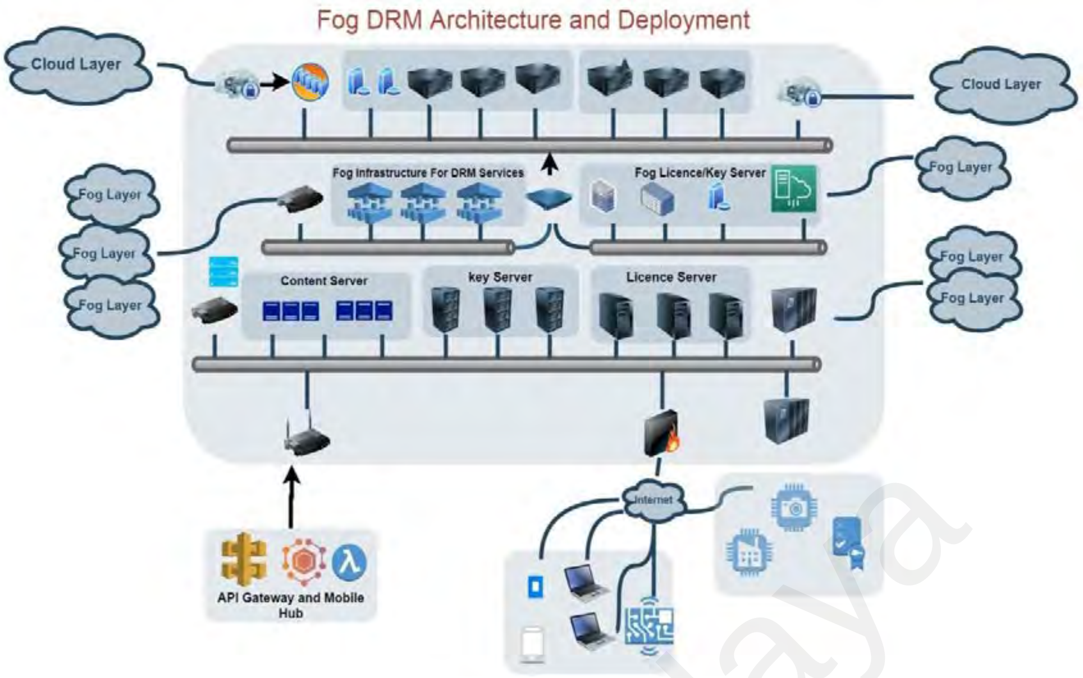


Figure 2.6: Fog DRM as Service and Deployment

- **Terminal Layer:** Contains end user devices that are connected directly with the Fog that uses the Internet
- **Fog Layer:** Contains all the Fog computing elements. Each node serves the request from the nearest locality and processes requests in a way that gives service better than the far distant Cloud.
- **Cloud Layer:** This is an actual Cloud network connected to Fog layer using the hierarchical architecture of Fog computing similar to as proposed by (P. F. Hu et al., 2017) is shown in Figure 2.6. Fog layer will offer its infrastructure as DRM service.

Recently, Fog computing has been proposed as a key shift in distributed computing and it was well endorsed by one of the big networking vendors called CISCO. All this successful adoption is due to its benefits of decreasing the time for a request to reach from device to service providers and vice versa. The idea of Fog computing has helped the development of protocols suitable for IoTs (P. F. Hu et al., 2017). Fog computing is being implemented in many IoT frameworks.

Fog computing is a standalone small-Cloud near the user geolocation. This small-Cloud has almost the same characteristics as that of public/private Cloud For computational offloading (Salim et al., 2010). The data volume is increasing, and hence the umber request per user to Fog layers will also increase. Predictably, the number of handoffs would increase. This high volume of handoff needs to be managed efficiently without the need for drastic network changes. The author (Yao et al., 2019) has presented three different handover scenarios, where mobile network is optimized with the help of Fog computing.

To satisfy the low latency, and location awareness requirements of DRM, Fog computing was introduced to be an intermediate layer between end users' consumer devices and Cloud. The scattered nature of data, changing network conditions, and the collaboration needs make it challenging to assure security and privacy. Therefore, the security and privacy issues cannot be fully resolved by employing the traditional public key or symmetric cryptosystem. To mitigate this risk, author (Sharma et al., 2018) proposed a registration based anonymous attribute credential, to control the network entities. They named their new approach as an attribute credential based public key cryptography (AC-PKC). In AC-PKC flexible key management is realized using certificate-less public key cryptography and the tracking feature of elliptic curve cryptography. Their study shows the basic operation of DRM e.g. Encryption, authentication, and access control with privacy preserving could be easily implemented by using AC-PKC. The features could better satisfy the security challenges of Fog computing based content hosting platform.

Unfortunately, the geographically distant and wide scale deployment, interaction, and varying characteristics of Cloud computing expose it to a new era of security and privacy challenges. The internet was developed to facilitate the wider audience and increase the impact of internet connectivity benefits towards end user and industry. The Cloud computing also leverages the reachability of benefits of the internet. The Internet penetration is increasing quite well in the past decade. However, the free natures of Internet content served through Cloud make strange nodes interact with each other. This could lead to data or privacy leakage, intellectual property rights violations, and content exploitation as well (Puliafito et al., 2019). On the other hand, the distributed and dynamic environment and resource constraint nodes introduce limitations on security mechanisms in Cloud computing.

Consequently, the existing public-key infrastructure based cryptography (PKI-PKC), identity-based public key cryptography (IB-PKC), and symmetric cryptography are unable to satisfy the security and privacy requirements of Fog computing based digital manufacturing. The presented Fog computing architecture for DRM could be useful in further defining efficient DRM for distributed computing scenarios.

2.4 State of the Art

Many future innovations in Cloud computing services will use Cloud DRM, integrated with third party access management services. These new services, built on many different technologies, need to provide low latency functions, and also provide flexible integration with their environment, to constitute secure and safe data storage, computation, communications, and control. Some prominent problems to be solved before these systems can be considered appropriate for this purpose. The high heterogeneity, complexity, and dynamics of these Cloud systems highlights emerging challenges to their robust and flexible operation, which shows the importance for resilience management strategies. This section surveys the state of the art in the Cloud DRM and discusses the prominent research issues and emerging future research directions. This study emphasis on the future applications that have very stringent requirements, notably high-precision latency and synchronization between a large set of flows.

The DRM technical implementation landscape has been reviewed from literature and a state of the art technologies proposed in DRM are summarized in the following sections:

2.4.1 Literature Sources

The first formal effort to define and standardize DRM started in 2001, W3C formed the first digital rights management (DRM). Later ACM SIGSAC, IEEE promoted attention to (Hao & Su, 2012; Keoh, 2011; Marques & Serrao, 2014; Munier et al., 2012; Serrao et al., 2003; Zou et al., 2010) critical problems for DRM, since 2001 the researchers are discovered actively contribution in the DRM topic. We have included utility articles from science direct, IEEE Explore, and Web of Science, with the keyword (("Abstract": Cloud) AND "Abstract": digital rights), from 2008 till 20th April 2021.

After carefully filtering, the articles it was discovered that the trend in DRM was more towards the encryption technologies which is more suitable in client server mode. However, the complex encryption doesn’t give optimal performance for the application of Cloud DRM authorization. Narrowing down the scope, closely related Conference papers, Journal articles as well as surveys were included in the study.

2.4.2 DRM for E-books Scenarios

The author (Chen et al., 2014) presents secure DRM to protect E-books stored in public Cloud storage and access by using mobile devices. User’s requests are subjected to session based authentication and, Cloud server aims to produce the session key between user and Cloud. The session key is generated such that, it adds the last viewed page number to the mechanism itself has the capability to identify the last viewed page number, even if the user accesses the E-book from different devices. They propose less complex algorithms like a hash function, exclusive-OR, and lightweight operations in the communication. The Cloud authenticates the user identity, generating symmetric encryption message. An object communication model is used, when a user request is being processed. At this point, request does not need not be worried about the internal processing of Cloud, therefore, allows users to apply to other Cloud services, shown in Figure 2.7. However, more research is needed to make this approach applicable in the interconnected federated Cloud. The motivation behind the use of low complex encryption was to improve performance and accessibility in mobile devices. But low complexity hashing algorithms increases security risk.

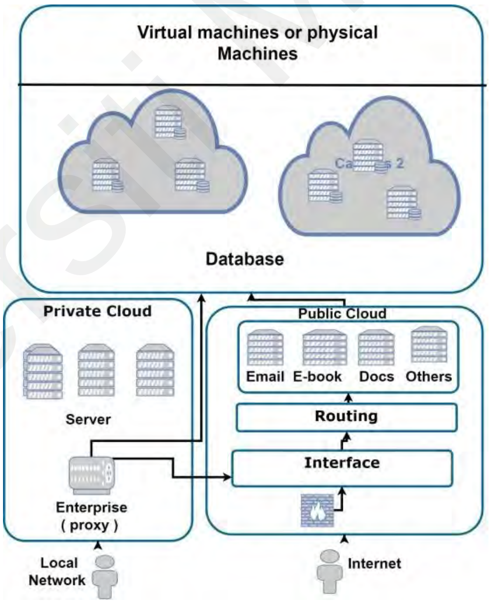


Figure 2.7: DRM to Protect E-books

2.4.3 DRM for Cloud Documents

In the software as a service (SaaS) model, the trustworthiness of devices part of data processing units in the Cloud is a big matter of concerts as a data provider or data source organization losses direct control of their provided data. These leave data owners at risk of data security. Data source organization is not responsible for third-party managing and using their data, so it also raised legal and data confidentiality concerns. It is possible to estimate the integrity of third-party data processing components in service-oriented architecture and Cloud computing scenarios (Salim et al., 2010). The author proposed a model to preserve confidentiality and protect the integrity of data and access the trustworthiness of data processing components with the four major entities; data owner, license issuer, data processing component, an integration component. The model employs multilayer licensing. Each layer could be expected to be up-to-date with the security principals at the next level, and each license issuer could be certified for the trustworthiness of the security principals following it. They have implemented their proposed schemes by using eXtensible Rights Markup Language ("XrML"), a configuration file; they access the integrity of computing service or device and with the help of security rules, and pass on a machine-enforceable usage policy to collaboration components in the Cloud. XrML is a type of Rights Expression Languages (REL), which is the policy or set of rules that govern the interaction among DRM attributes entities like rule, data, conditional checks, and consumer. The XrML, first data is encrypted by using unique random data encryption key followed data usage license issue by the original data owner and the valid encryption key and then the access right delegation is performed by root delegation and distribution. Their model lacks task delegation and they don't protect the data created within collation itself. Also, there is no revocation mechanism to stop access in real time.

2.4.4 DRM Without Trusted Third Party

Traditional Public key Certificates (PKC) being used as authentication mechanisms that are linked with attribute keys, so the identity of the content consumer is at risk. This paper (H. Gourkhede & Theng, 2014) presents a novel DRM scheme that doesn't depend on the trusted third party to protect the privacy and also has accountability. The proposed scheme is based on blind decryption and hash chain. The proposed scheme also uses the revocation mechanism to protect the privacy, which makes sure the authentication is by assigning authenticating with the true identity of a user. User’s real credentials are stored at the time of registration. This scheme proposed a tree hierarchy of content distribution which comprises N (number of) Distributor (depth of the tree) and L (number of) levels. Contents consumers are served by level L. Consumer client first validates PKC by the Owner, and generate a blindly decrypted token and attribute keys. At this time of license generation, the consumer client submits the blind token to the Content Provider for authentication and didn't send PKC or attribute keys. This way, the scheme restricts the prediction and leakage of personal user information and there is no connection between attribute keys, the user id, and hence the purchased content. This way the proposed scheme solves the problem of reliance on the trusted third entity (TTE) and protecting the privacy of the user. Evaluation results not available to validate the performance and efficiency of their approach.

2.4.5 DRM with Trusted Third Party

A privacy-preserving DRM scheme for executing purchased software at maximum n-times in a Cloud provider was proposed (Joshi & Petrlic, 2013). Their approach was focusing to prevent user's profile building. This scheme uses a combination of ring signatures and anonymous recipient techniques. ElGamal cryptosystem based on unidirectional proxy-re-encryption technique is employed, to protect the privacy of the user, which allows entity A to assign to B without requiring B to assign to A. Proxy couldn’t see the content in plain text, as shown in Figure 2.8. To protect the secrecy, they used an arbitrarily large number of shares, and users need at least a certain number of shares to decrypt the secret. Anonymous recipient encryption is used to create more than one public key for a message and can be encrypted at the same time the message can be decoded using single private key. Those public keys are not connected. This way the anonymous receipts could be assured. Ring signatures allow data to be attested in a way that, it possibly verified that's it’s signed by a member of a specific group. The signing entity remains hidden and not reviled. Using an anonymous payment scheme a user anonymously fetches digital coins from a bank. Any entity, even the bank, cannot map the coins to the user who paid for the coins, afterward. The bank anonymously attaches the RSA encrypted digital coins and charge the amount from the user’s account. They used CHAUM’S scheme, which is based on blind signatures. Their scheme relies on the trusted third entity (TTE) to issue licenses. The user first anonymously purchases a license for the software from the software provider. To execute the software, the user receives software execution token from TTE. This issue a certified token after verifying the license. On sharing the token with the computing center, the computing center verifies the token and entertains the software execution request. While purchasing licenses anonymously pays service providers fee using the anonymous payment scheme. This approach doesn’t take into account the performance parameters and may result in the poor quality of service.

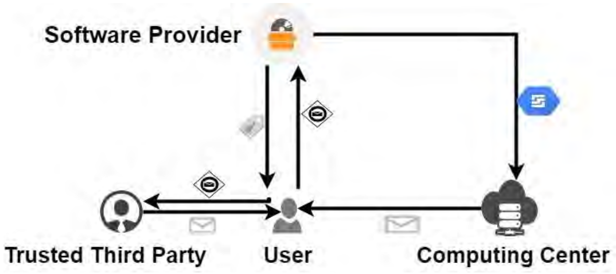


Figure 2.8: DRM which involves Trusted Third Party

2.4.6 Attribute Based DRM

Authors (Q. Huang et al., 2013) presented an attribute-based DRM scheme was proposed which combined the cipher text-policy attribute-based encryption (ABE) and proxy re-encryption and addressed the problem of the heavy overhead of key distribution on the content provider. In ABE, content is encrypted based on user attributes and only user with the specific attribute can decrypt the content. Their technique allows the user to stay anonymous and hence protect its privacy. They divided the key between two; first is called master and second assistance key. The access policy is reflected in the master key. The master key is then shared with the users together with the license, whereas the assistant key is cryptographically saved on the key server. The only user with a valid access policy can reconstruct the content master key and then fetch an assistant key from the key server and decipher the content and consume it. In revocation operation, attributes authority delegate revocation tasks to the key server without revealing the assistant key. A key server can deny sharing the assistant key for those users or attributes which as no longer authorized. The user remains anonymous to the Cloud service provider and key server in the Cloud as it is in the process of obtaining the attribute secret keys and license, as shown in Figure 2.9. They have demonstrated good efficiency but key distribution is still overhead when dealing with large data set. Their scheme does not support dynamic usage control in distributed computing.

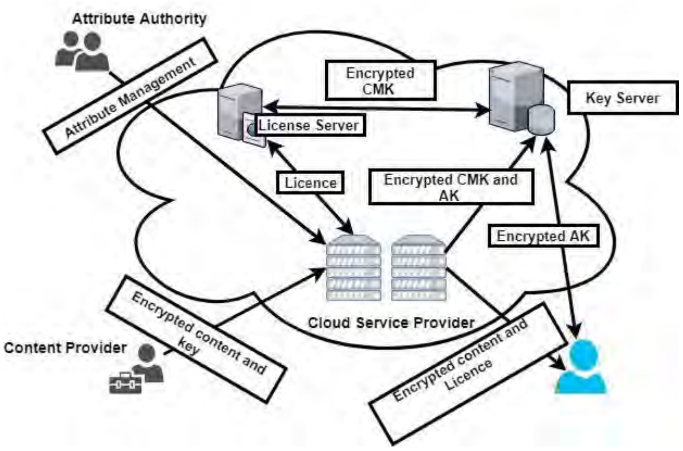


Figure 2.9: Attribute-Based DRM

The privacy preserving, secure and digital rights management (DRM) scheme using holomorphic encryption for Cloud computing was presented in (Chiang et al., 2013). Proxy re-encryption can be subjected to man in the middle attack. The technique presented in this study use proxy re-encryption and holomorphic probabilistic public key encryption. In the DRM process, key generation server sends the homogeneous key via license to the client besides proxy re-encryption key this was to make sure high security and reliability, as shown in Figure 2.10. The proposed scheme is different from other homogenous based context protection scheme that it protects the content and privacy. This takes place without the need to re-encrypting the content repetidely. Efficient license models are used and have low computational complexity to support massive users. This approach can be subjected to man in the middle attack.

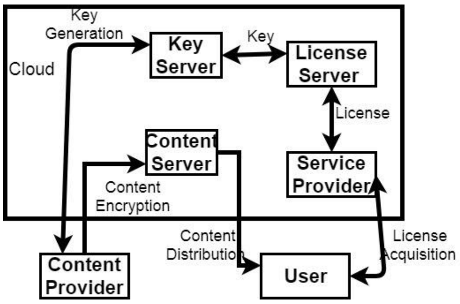


Figure 2.10: PRE and Holomorphic Probabilistic Public Key Encryption

2.4.7 Mobile Sim Card Based DRM

Pirated software and copyright material is a tremendous impact on the trustworthiness and reputation of digital content providers and the mobile industry. Authors in (Zou et al., 2010) presented a solution to unstructured data and for its efficient digital rights management (DRM) services used Sim card. They call their system “Phosphor”, and it has two main features one is lower cost and improved system security. Many of the present mobile DRM schemes have limitations to compatibility with a large model of devices, poor support to extend and development, costly and prone to security loopholes. The author relied on Cloud security and implemented backend in the Cloud. Their proposed DRM algorithm is based on Cloud backend to protect uses unstructured content and license. It protects, user’s integrity, misuse of protected content, and unauthorized user access but it cannot revoke user access. GSM technology is dependent on signal strength so the reliability and usability of the proposed system will not be good in a remote location and low GSM signal strength areas. The approach is show graphically in Figure 2.11.

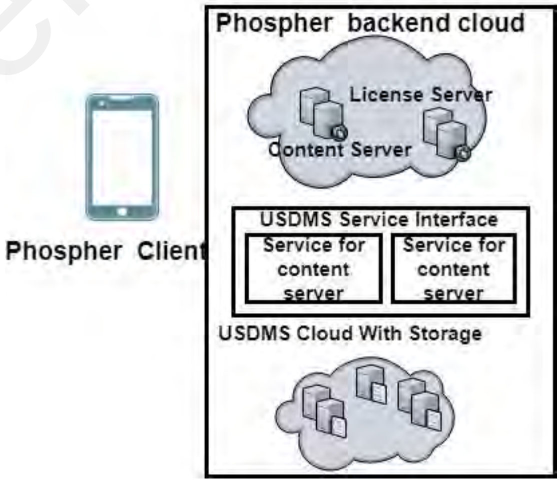


Figure 2.11: Phosphor a Mobile Sim card based DRM

2.4.8 Document Self Protecting DRM in Cloud

The author presented privacy-preserving Cloud DRM in (Petrlic & Sorge, 2014). They have proposed the packing of applications into virtual machines (VMs) by software (Cloud) providers and the VMs can be executed at any site in the Cloud. All the necessary components to preserve the content integrity, privacy, security, and access rights management reside inside the VM preventing the content provider not to be able to build usage patterns of the user's computations in the Cloud.

Their approach cryptographically signs both the VM and hardware and allow user to enjoy the execution of software’s at most n-time and content provider cannot interfere with the data while user’s data is in processing. This prevents the user's profile building. Their scheme also supports a flexible pricing model with software execution of n-time. In case of a security breach, there is the possibility of users’ data leakage so this scheme needs improvement in terms of the security of user’s data.

A lightweight, platform independent, secure, and easy document protecting and editing solution for Cloud storage providers was demonstrated in (Arora et al., 2016). They encrypt the user's file before saving it to Cloud storage such as Google Drive and then save the encrypted version in Google Drive on user behave. And decrypt the file and display it to user acting as a trusted third party extension. They have demonstrated improvement in performance and easiness from a user point of view. Their solution does not work in all Cloud based storage providers as it dependents on storage providers’ private API. Additionally, it is not completely privacy preserving as users’ profile building is still possible. Their solution does not have a mechanism to protect the document in collaboration. Their solution is not completely privacy preserving as users’ profile building is still possible and their web application is vulnerable to traditional web attacks like session hijacking and man in the middle attack. The approach is show graphically in Figure 2.12.

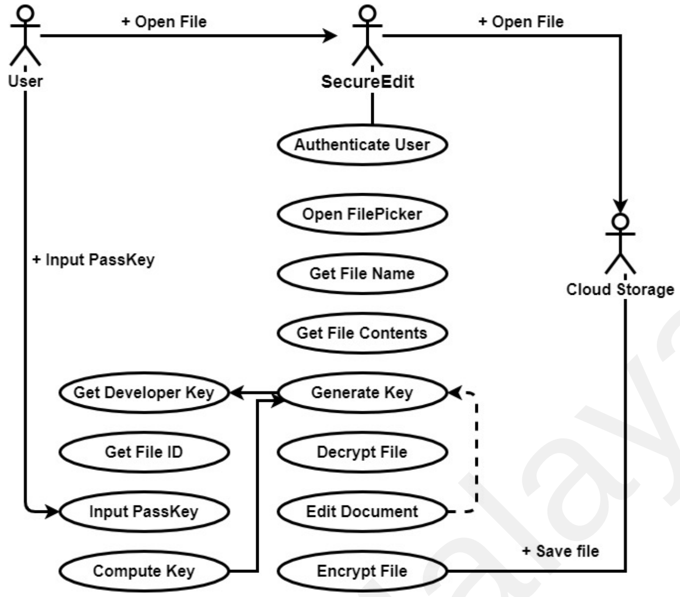


Figure 2.12: Protecting Document of Existing Cloud Storage

A framework to protect documents outside the source enterprise network has been presented in (Doncel et al., 2011). They make the document programmable and intelligent to determine its position in a network and document itself takes part in the DRM process. This way document behaves as a self-guard for its integrity and avoids content modification for a basic operation like reading or copy, and modify. Therefore, safeguarding document integrity and preventing illegal access became characteristic of document itself. They transform the static document into an active document to control the operations performed on the document e.g. copy, print, using. They store the active properties of a document in the meta-data, User sitting outside the network. A Temper-Proof document framework acts as an intermediate between the underlying operating system and software that open documents. Framework encrypts the document, enumerates the machine and user details and enforces the access policy, and is capable of identifying each machine and user inside. A client utility enables to access the active documents produced by the framework. One of the consumer side documents precedes the validation and access only if the Temper-Proof framework is installed. This framework may not be easy to integrate with propriety document viewing software also they don’t take into account if the user machine is compromised. Also, every user has to install framework and client viewer utility which may not be favorable in every scenario.

Authors in (Munier et al., 2012) partially presented the concept of the document itself protecting its integrity, availability, and confidentiality after it is being shared with an external entity (either Cloud or USB). Data and security mechanisms (access control, usage control) are embedded in the document and results in an autonomic document administrates itself security. They have a database that stores the data of a document including meta-data, security kernel which talks to OS and enforces access kernel, embedded applications for opening the document in document views applications, and license to define the access policy. Autorun file is used to invoke the embedded application after that security kernel takes control of the document. This approach is a unique feature that client-side encryption/Decryption is not used and dedicated module of security kernel is used for this purpose. Hence the user can update the document and republish overhead avoided. This approach doesn't satisfy the Cloud and multi-user collaborative data storage use cases. They are still in the prototyping stage and security improvements need as encrypted data and policy can be subjected to brute force attacks. The approach is show graphically in Figure 2.13.

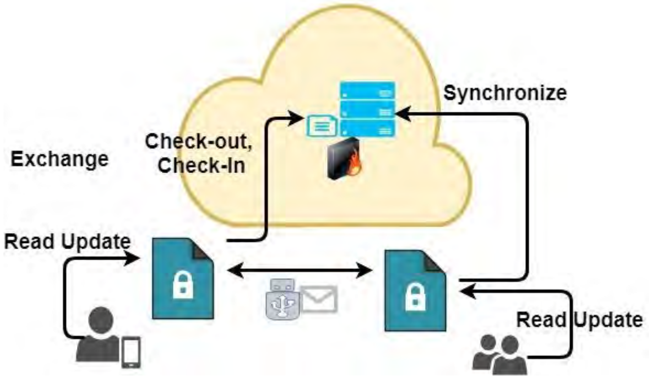


Figure 2.13: Self Protecting Document System

A small-scale and low-cost DRM system for Cloud storage providers is presented in (Kumar & Goyal, 2019; Sriborrirux et al., 2014). The content is encrypted when it travels from user to Cloud storage but encrypted data stored inside Cloud storage provider's end. And the user can stream the book using proprietary verified viewer application. The key management system distributes a unique encoded portion of the secret key to different VM-based servers, so it a very difficult to hijack or recovers the key. OAuth 2.0 protocol is used for user authorization in login and authentication for the user. The user can purchase the license to e-book then user's social account (Facebook, Google plus, or Twitter) details are shared with DRM server to authorize the user. After successful user authorization users can request e-books to DRM system. User's privacy is not preserved. Instead of unicast or multicast key distribution authors (Cheng et al., 2016) proposed a novel user role and service type key based distribution is proposed for the video streaming application deployed on Cloud. Their approach can deal with users with various rights and various communication bandwidths. But in the Cloud as video streaming data volume increase it a tough challenge to deliver the appropriate quality of service.

Simple, frequent, and flowing access to data and content has become more and more important for example online media purchases. Authors in (Llewellyn-Jones et al., 2009) analyzed the trust of the community to protect the existing peer-to-peer file-sharing network using DRM. They have implemented an assurance algorithm based on the

Gnutella network and used cellular automaton trust mechanism, every node in the network is treated as a cell of the cellular automaton. The algorithm requires a note to update at the same time and changing network delay makes it hard to achieve in a real network and they-they have to implement a caching mechanism. They have identified synchronization as a problem that hinders the effective working of the trust mechanism. The easy and frequent movement of content is also identified as an important parameter for protecting the rights holders.

Watermarking is still popular in online TV video broadcasting. Authors (Jiang et al., 2016) have proposed a more robust and secure watermarking method based on H.264 compressed domain enforcing DRM in video content. Their proposed method doesn't fully decode and re-encoding in both embedding and extracting processes. Their mechanism cannot be applied to non-video content.

To address the limitation of providing dynamic usage rights, authors (Qinlong et al., 2014) proposed a secure attribute based DRM scheme in Cloud computing. In ABE cipher-text is linked with a set of user’s attributes and user’s decryption key is dependent on the access structure. The author proposed additive homomorphic encryption, which makes the license server, in the Cloud, change the user's usage rights dynamically without disclosing the unencrypted data. The paper focuses on the key management is performed using cipher text policy attribute-based encryption (CP-ABE) and proxy re-engineering (PRE). Providers encrypt their contents with the content encryption key (CEK) which has two parts, content master key (CMK) and assistant key (AK). The CMK is protected using CP-ABE and shared in the encrypted content. However, the AK is protected using PRE and shared along with the licensed content. The content providers selectively provide their contents among a targeted authorized users after encrypting the CMK under the access policy. The framework delegates the license server in the Cloud to revoke the attributes and users immediately.

Most of the DRM solution involves trusted third entity (TTE) entity to issue the licenses, if that trusted entity is compromised then it can break the privacy protection of users' critical data and user privacy. An author of (Subramanyam et al., 2012) presents a DRM scheme that doesn't involve TTE their scheme also preserve the privacy distributes the content securely. They used blind decryption and hash chain in their architecture and user stay anonymous. The user creates anonymous tokens, completes registration. Assume, Alice has a command encrypted with public key of Bob. Using blind decryption, Alice can reconstruct the command decrypted by Bob, even Bob not familiar with the message, and Alice not familiar with the private key of the Bob. This whole process involves RSA cryptosystem. Hash chain is created by many-times applying a one-way and collision-free hash function. On the distributor side, content provides take care of the content purchase and transactions with the users. But User revocation is costly operation. The approach is show graphically in Figure 2.14.

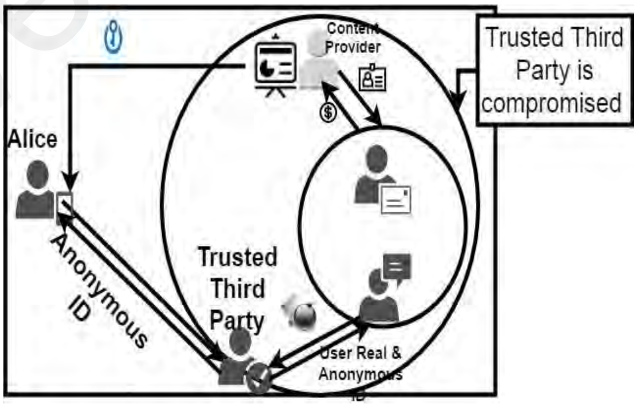


Figure 2.14: DRM Scheme Without Trusted Third Entity (TTE)

Authors (He et al., 2014) presented attribute-based encryption (ABE) for P2P Cloud storage. Their scheme has low computation overhead as compared to other ABE schemes. Content creator delegates the task of re-encryption of file to Cloud servers and also assigns user secret key to trusted cluster of peers registered with trustworthy P2P system. The central trusted server makes sure that it didn’t leak the contents and legitimate user secret keys to an unauthorized user. This way it achieves low computation burden onto the data owner and Cloud servers for user revocation.

In Cloud DRM, key management and distribution is an overhead. Recently, (Petrlic & Sorge, 2014) proposed a cryptography based approach to increase the efficacy in Cloud based data sharing and collaboration applications. The core of their technique is to decrypt multiple varieties of data using a fixed size single key and that too can be used by many users. Key aggregate cryptosystem (KAC) can produce fix-size ciphertexts which allow to effectively delegating the decryption power for a set of cipher texts. So, it can aggregate a set of secret keys and make generate one key representing all the feature keys aggregated. They used composing of a secure key aggregate cryptosystem (KAC) that is efficiently implementable using elliptic curves.

DRM service used for protecting the corporate data is also called Enterprise Digital rights management (E-DRM). Author (He et al., 2014) also suggests storage efficiency, especially for enterprise digital right management. They have proposed to store encrypted digital content in more than one server and efficient data retrieval algorithm for robust and low complex retrieval of data from the storage component. Improving the performance of DRM content server is the main focus of this paper.

The efficiency of DRM system is the need of today's as mobile users are also consuming DRM. Authors in (J. Huang et al., 2014) proposed DRM scheme focused on efficient authentication, low processing hungry encryption, consume less storage space, and also recover the user’s key if the mobile device is lost.

Survey of Cloud DRM focused on Interoperability issues of DRM Cloud solution. Their proposed solution allows multiple DRM protection mechanisms within a Cloud DRM and supports the consumption of diverse end-user devices regardless of DRM technique involved. An enterprise can have its protection mechanism and also can interact with the protected content of another enterprise. A unique DRM agent is managing each type of protection mechanism. The interaction between different Cloud DRM is still a challenge to be solved.

A scalable DRM solution is a requirement of the market. The author's (Bellini et al., 2014) proposed low cost and low complex DRM solution by using distributed hash table (DHT) Peer to peer (P2P) technology for efficient rights authorization, user's authentication, and rights validation. Their approach utilizes the efficient load balancing feature of peer to peer network for group licensing (flexible), short-term licenses, interdependent licenses and can integrate with other DRM solutions. They have tested their approach on AXMEDIS DRM for MPEG-21 file format. But the P2p protocol lacks in optimal performance when it comes to real time and delay sensitive service.

2.4.9 Use of Rights Expression Language in DRM

The Syntax based Explicit rights specification like rights expression language (REL) are not enough complex unforeseen access rights so machine understandable semantic based are proposed by author (García et al., 2007). REL mostly depends on the set of dictionary keyword and lake scalability, difficult to automate the access rights, performance bottleneck which it comes to process a large amount of data over the internet. To solve the limitations an interoperability and automation friendly DRM system which depends on meta data web semantic approach. They transform the REL terms into a machine understandable terms. They define web ontology which is accessible as URIs and make it easy to adapt and interoperable. Generic copyright ontology is defined to support the legal needs.

2.4.10 Watermarking for DRM

If protected content is fully decrypted by users device, then there is a risk that users can manage to access the unencrypted content and redistribute it to the unauthorized user. To solve this problem an advance watermarking DRM techniques have been proposed by (Thanh & Iwakiri, 2016) which use incomplete decryption and fragile watermarking (watermarking which detects if the content is modified). The quality of trial constant to willingly degrade and level of degrading depends on the key of watermarking using the incomplete decoding mechanism and information of the consumer is encapsulated into decrypted content. The Watermarking decoding key is dependent on the user's personal information. A malicious user is detected using fragile watermarking; it will match with user information if the user is authorized. In case authenticated users try to convert the image using image processing then fragile watermarking information will vanish. A similar approach that uses Huffman code as incomplete decryption is proposed by (Iwakiri & Thanh, 2012). These approaches are limited to image DRM purposes and when the image is distributed via the internet.

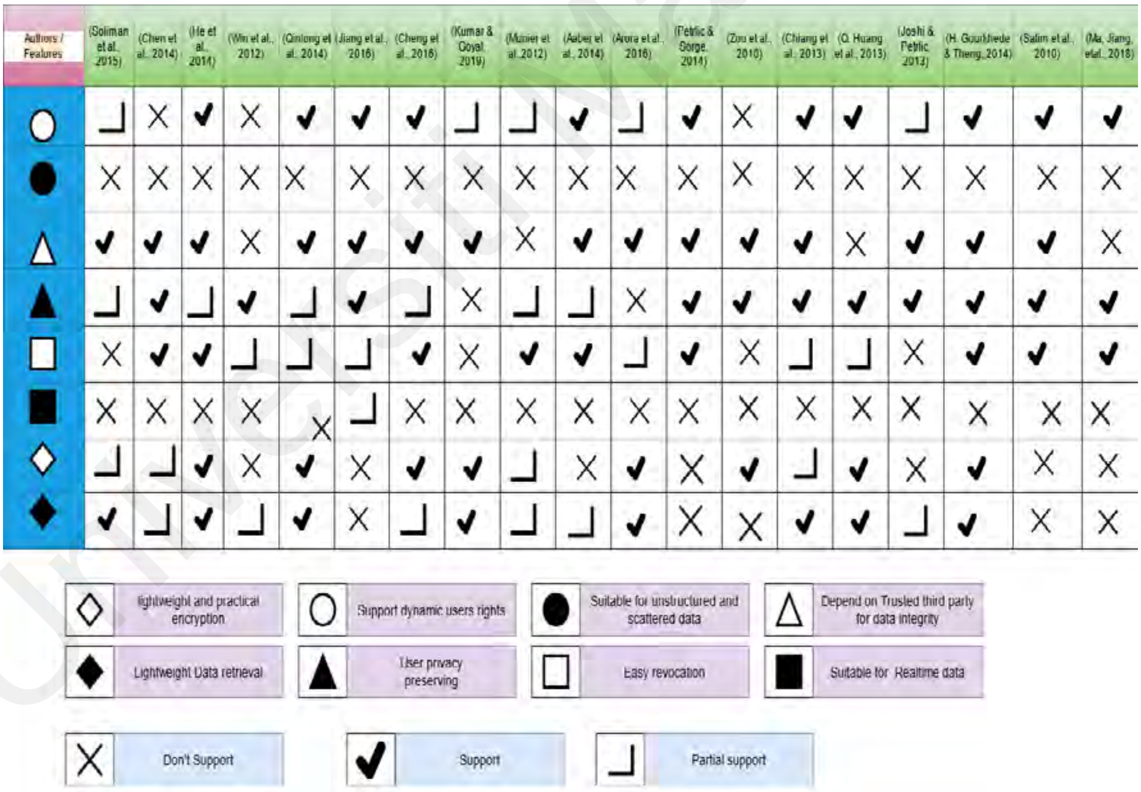
The author has improved the work of (H.-W. Yang et al., 2013) and prosed security improvements like prevention of stolen smart card attack, improved password update mechanism by optimizing the resource usage, and forward secrecy property (completely unlinking the server's private key and each session key so that long-term keys is not containing the past session keys) is proposed to secure the session key involved in components of DRM system. Their improvements are from increasing security but this may be at the cost of efficiency.

2.4.11 DRM Standardization Effort

Moving Picture Experts Group (MPEG) is a working group that aims to formalize the standards for compression, decompression of image, and video content. MPEG Multimedia Services Platform Technologies (MPEGH-M) is the standard developed by MPEG for easily handling the interoperable flow of media among various devices and it also defines a standard for interoperable DRM mechanism. Due to the middle-ware nature of the proposed system, it is capable of supporting heterogeneous devices and a variety of services. The picture shows the architecture. Author (Doncel et al., 2011) illustrates the concept of MPEGH-M interoperable standard which supports single and aggregated service. These standards are only applicable to MPEG technologies.

Currently millions of users use social media to share pictures, videos, and other daily life documents. This Sharing is a very common and useful way of sharing personal contacts and information. But the user has very limited control over its data after the data is available in social networking platforms whereas the platform and user can tamper with the data and easily republish it. Author of (Rodriguez et al., 2009) presented a DRM system that addresses this privacy issue though by empowering the user’s to have enjoyed more control over its data shared on the social network. They used Open and Secure DRM (OpenSDRM) which is the European IST FP5 MOSES RTD project. OpenSDRM is open and molder in nature so can be easily adapted to any business requirement. Author (Rodriguez et al., 2009) also developed a browser extension as a client-end application, for the user to get registered on OpenSDRM, uploads data to OpenSDRM which they want to share, writes the access policy over data, and permission to render the content on social media. Every time user wants to share anything it has to use the browser extension which acts as middleware between the user and social media platform. This approach blindly trusts the OpenSDRM framework and didn't evaluate the trustworthiness of data processing components involved in protecting.

The output of the state of the art review has been summarized as a comparison of major techniques from a performance lightweight and flexibility perspective in Table 2.1. As evident from Figure 2.15 the proposed method better meet the dynamic user’s rights, which is suitable for unstructured and scattered data, also depend on trusted third party for data integrity. The approach also better in term of depending on the trusted third party for data integrity, user privacy preserving, easy revocation, suitable for real time data, lightweight and practical encryption. Lightweight data retrieval is the important feature for flexible DRM in Cloud. The flexible and efficient license distribution for Cloud DRM is also important. However, the lightweight approach to data integrity for distributed computing is still lacking in the literature.



Authors / Features	(Soliman et al. 2015)	(Chen et al. 2014)	(He et al. 2014)	(Win et al., 2012)	(Qinlong et al. 2014)	(Jiang et al., 2016)	(Cheng et al. 2016)	(Kumar & Goyal 2019)	(Munier et al. 2012)	(Aaber et al., 2014)	(Arora et al., 2016)	(Petric & Sorge, 2014)	(Zou et al., 2010)	(Chiang et al. 2013)	(Q. Huang et al., 2013)	(Joshi & Petric 2013)	(H. Gourkhede & Theng, 2014)	(Salim et al., 2010)	(Ma, Jiang, et al. 2018)
○	⌟	✗	✓	✗	✓	✓	✓	⌟	⌟	✓	⌟	✓	✗	✓	✓	⌟	✓	✓	✓
●	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
△	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗
▲	⌟	✓	⌟	✓	⌟	✓	⌟	✗	⌟	⌟	✗	✓	✓	✓	✓	✓	✓	✓	✓
□	✗	✓	✓	⌟	⌟	⌟	✓	✗	✓	✓	⌟	✓	✗	⌟	⌟	✗	✓	✓	✓
■	✗	✗	✗	✗	✗	⌟	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
◇	⌟	⌟	✓	✗	✓	✗	✓	✓	⌟	✗	✓	✗	✓	⌟	✓	✗	✓	✗	✗
◆	✓	⌟	✓	⌟	✓	✗	⌟	✓	⌟	⌟	✓	✗	✗	✓	✓	⌟	✓	✗	✗

◇	lightweight and practical encryption	○	Support dynamic users rights	●	Suitable for unstructured and scattered data	△	Depend on Trusted third party for data integrity
◆	Lightweight Data retrieval	▲	User privacy preserving	□	Easy revocation	■	Suitable for Realtime data
✗	Don't Support	✓	Support	⌟	Partial support		

Figure 2.15: Comparison of State of The Art DRM Literature Form Performance Perspective

2.5 Cloud DRM Authorization

Another study (Xie et al., 2021) attempts to address the content security or DRM in Cloud computing whereby focusing on attribute-based encryption (ABE). It uses attribute of user's involved in encryption to actually apply DRM encryption. Also, it attempts to address the challenging requirement of multiple devices, for optimal handling in modern deployment scenarios. The author proposed hybrid cloud multi-authority ciphertext-policy attribute-based encryption (HCMACP-ABE). The proposed method utilizes Linear Secret-Sharing Schemes (LSSS) data structure for access implement secure access method, which is independent of the private Cloud. The private Cloud is responsible for maintaining the overhead of the user’s authorization list and verifying the user. Their approach targets the hybrid Cloud environment.

The aforementioned scheme empowers the content processing users and enforces the security of datahi by regulating the access for mobile devices in hybrid Cloud scenarios. In involved proxy layers and Cloud user assistance involve screening the request as proxy layer as well as a component with apply encryption and decryption. The aforementioned scheme applied Canetti’s transformation as a reference for security and performance. The study aims to reduce the computation overheads, also attempt to improve the efficiency, of the mobile Cloud environment. However, an extra layer of Cloud user assistance (CUA) can bring additional cost and overhead in latency-sensitive scenarios. With the advent of Cloud computing in the public Cloud environment to facilitate the keywords of interest or search in protected content shared over public Cloud. A similar study (Cui et al., 2018) revolves around multi user delegation and group search operation. They proposed an attribute-based keyword search with an efficient revocation scheme (AKSER). Their design improved efficiency of user revocation and fine grained authorization of the search and group authorized entities. Their method achieves semantic security, unlikability of keywords, and resilience to the collision.

In AKSER, content authors use personal or custom access policies to encrypt the file indices. That increase mapping over the role or category of the user authorized to query the index. Aforementioned approach focuses scalable multi-certificate authority access control mechanism capable of searching many keywords and many data owners. The resultant system relies upon the central server to implement efficient revocation operations per user basis. This approach aims to improve the accuracy of Cloud access control server in releasing the search use cases. Keeping the recent trend of using users attribute to the context of request as identity in the process of authorization, the authors (X.-J. Lin, Wang, et al., 2021) presents identity-based encryption with an equality test (IBEET). The author proposed a primitive, called identity-based encryption with equality test and datestamp-based authorization mechanism (IBEET-DBA). In aforementioned approach, the content owner has the authority to control as well as validate data. The author addresses the limitation of ciphertext-specified authorization and user-specified authorization. the formal definition of the approach primitive along with security notion. Moreover, author propose the first IBEET-DBA scheme and demonstrates its security. Authors (Voundi Koe & Lin, 2019) redesigned proxy re-encryption to unlink users personal data from the Cloud store thereby moving the identified masked from Cloud storage. Thereby leveraging the control of Cloud storage for improved user privacy by enhanced authentication and authorization mechanism. This study also attempts to improve the flexibility of user authentication and authorization mechanism, and it saves the user from being online all the time to protect their data in the cloud. Another study by (Pareek & Purushothama, 2020) focuses on increasing the efficiency of Proxy Re-encryption (PRE) by requirements and also discusses its potential in the solid versatile access control facilities. The study demonstrates the controlled sharing can be achieved efficiently with PRE for versatile delegation scenarios.

The author (Deng et al., 2017) proposed Multi-user searchable encryption (MSE) which uses encryption and applies DRM to facilitate authorized user in searching of protected content. The proposed solution targets the use case involving Cloud storage where content is reshared for collaboration and the risk of unauthorized consumption but can leverage the search feature over the encrypted data. The study aims to address the practical limitations of Cloud authorization. The study highlights the gap that no existing scheme to achieve all these properties at the same time. The proposed schedule addresses the needs by applying attribute based complex encryption operations which authorize other users to lookup subset of keywords in encrypted form. The proposed schedule uses an asymmetric bilinear map along with keyword auth organization binary tree (KABtree) to craft new way to achieve performance benefits.

Another study (Antonolpoulos et al., 2018) focus on user privacy and automated Physical Access Control System (PACS). They propose to enhance private Cloud capable of applying access control safely by encrypting sensitive information at the same time preserving user privacy. The cloud service tracks the overall system activities in physical infrastructure and inbound alerts for a data breach or access violation. The approach involves processing of logs in the public Cloud. The authors (Chadwick & Fatema, 2012) proposed cloud authorization using XACML applied to web service in Cloud. The author discusses the importance of simple policy implementation to handle the authorization and the design complexity. The authorization protocol needs to be application developer friendly and as simple as possible, especially in the Infrastructure as a Service (IAAS) deployment. And the study proposes that the complexity needs to be under the web service interface, leaving less responsive on infrastructure and simplicity. The proposed OASIS SAML-XACML as a solution to increase access control, in Cloud with less complexity toward Cloud layer.

Authors (Parmar & Bhavsar, 2020) propose a new terminology RoT as an alternate terminology to address the unified need for Authentication, Access Control, Confidentiality, Scalability, Encryption, Integrity, and Authorization. The Author

(Esposito, 2018) presents a model which aims to address the multistakeholder authorization among the organizations. The study emphasizes on the solution to interoperable problem of authorization. The study also highlights the deficiency of effective support to enable the coexistence of multiple access control in a context. The study also advocates the need for dynamic approaches with greater support for seamless interaction of multi role with the cloud over time and resist unauthorized data leak attacks. Aforementioned approach is based on ontology-based access control given the trust among entities of a process and also use pseudonyms for privacy needs. The approach proposes as second-level defense for data going the public cloud. That critical data is marked with the severity of access using tags that associate the trust. The research also highlights the access control beyond identity access scope by facilitating unlinkability of personal data or data which can facilitate the unauthorized consumption of data to predict user habits and profiling which is necessary for improved trust and transparency of digital systems.

Another study (Shen et al., 2017) addresses the computation overhead for data integrity in Cloud for resource-constrained environments. Authors present auditing mechanisms for Cloud storage auditing schemes suitable for cluster users and aiming to optimize the computation overhead from end user devices. They named their proposed method as Third Party Medium (TPM). The TPM is in charge of generating authenticators for users and verifying data integrity on behalf of users. TPM is also specialized to enable end user to make sure data is not modified by Cloud storage, this adds a significant contribution toward big problems of data integrity verification in the Cloud. TPM does time exhaustive operations which user need to do thereby reducing the overhead and verifying data on end user devices. This saves users from heavy decryption operations when interacting with its data saved in the Cloud. This results in user operation taken care of by the Cloud. The privacy is proposed to extend by applying data blinding operation as users upload data. The authorization method is time bound, making it easy for an authorized user to enjoy data integrity with time as additional parameters for Cloud data auditing needs. The secure attached comprised of content security areas such as content privacy infringing, data hacking, and unauthorized data access involved in the cloud layers. The study discovered that the attack gets more damaging as lower Cloud layers which directly community to OSI model and basic network service are directly affected (S. A. Hussain et al., 2017).

An effort focused on integrity protection features of Cloud DRM was made by the researcher (Lu et al., 2020) and their study emphasized the greater data integrity in shared data storage cloud servers. They attempt to address the integrity protection mechanism over the content by applying access control in mobile cloud computing. Their approach to integrity protection applies encryption over the plain text data and aiming to implement a second wall of protection to safeguard data privacy and integrity defense in case of data leaks. The approach attempts to optimize the secure and lightweight integrity verification scheme for Internet of Things (IoT) mobile terminal devices. They designed data sharing method for data owners to share cloud data with authorized users. Finally, the study proposed Merkle Hash Tree as a Version Based Merkle Hash Tree (VB_MHT) that present solution to preserve the information of block node fresh for improved security and integrity verification of the shared data. Their approach focuses on achieves lightweight operations of data owners. They also have defined mechanics data collaboration, among authorized users, and sharing among users for downloading and consumption from shared cloud data. The author also presents the performance of computation and communication costs.

As the real world deployment of IoT and Cloud will bring a high volume of data which will be hard to manage. In case of the scattered data spread over a distant geographic area. This challenge will give birth to mechanisms involving end user devices and data owners in playing role in the infrastructure as a whole. The author (Tapas et al., 2020) presents IoT-Cloud based model for authorization and access delegation which also utilized Blockchain technology. Although the study focuses on smart city requirements and presents smart contracts driven methods for smart features and assessed access need of control and delegation in IoT. Three real-world scenarios for access control and delegation in IoT use Blockchain technologies. The study presents a theoretical analysis of time and space complexity targeting create delegation, delete delegation, and check access. Their model implemented onto the Etheruem testnet Ganache and public testnet Rinkeby. The study also presents the performance evaluation. Researchers (Bernal Bernabe et al., 2014) focused on the greater availability of the access control feature in cloud computing. The study focuses on increasing the adoption of the modern authorization model in practical cloud deployment scenarios. The author represents Role based access control (RBAC), hierarchical objects (HO), conditional RBAC (cRBAC), and hierarchical RBAC (hRBAC) for cloud storage. The proposed model has support for multi agent and federated access control features as well. The federated authorization together with semantic mapping of access is discussed. Resultant model address the fine grained trust for administering a trusted federated central server in cloud computing. The author has also presented the validation of the prototype by developing it using OpenStack with python and Java programming languages. The authors (Sun et al., 2020) presents searchable encryption scheme which makes up defense of per user personalized linkable search. Their approach is using server assisted searchable encryption. Multiple users are facilitated by selective authorization. The data owners only need to know the public key of an administration server to generate the searchable ciphertext. The study comparison with the related word in the parameters of search privacy, ease of use case, computational burden, and communication latency.

Another study (Sultan et al., 2018) highlights the future perspective of a secure inter-cloud authorization scheme called ICAuth. ICAuth uses ciphertext-policy attribute-based encryption (CP-ABE) for authorization of user access token. Their approach target to meet low latency, low communication overhead, and less storage consumption for lightweight computation costs. IAuth generates a single decryption key in a standalone manner independent of other entities. The one key can be used to access many resources. The revocation mechanism involved a re-encryption algorithm which has overhead in itself. ICAuth also aims to be more flexible and scalable for inter-cloud shared access scenarios. The author also presents security analysis and demonstrates it is immune toward Chosen Plaintext Attack (CPA). The performance analysis is presented keeping in view the use cases, network and file system overhead, latency, practical applicability, usability, and computation costs.

2.6 Cloud DRM Requirements

In Cloud DRM, the technology stack is important to design for optimal flexible content delivery and with the focus on Cloud infrastructure security. Based on the literature review, we identify the key issue of Cloud DRM. These issues include robust revocation, depending on central third party, temper proof, flexible license and access policies, and lightweight approach for authorization. The actual requirement of Cloud DRM depends on the business model it applies so, we presented an abstract view of the necessary features and their trade-off. Following are the requirements of Cloud DRM requirement in Cloud are important to identify.

Hardware and software implementations: PlayReady is a Microsoft platform for protection and distribution of entertainment content and used in major Hollywood studios e.g. UltraViolet™, and HbbTV (Ghiglieri & Waidner, 2016). They support pay as peruse for download, rental, and streaming. Google has Videvine and apple has FairPlay DRM service. But all of these three can protect video content only.

Interoperability & Mobility: The Internet provides a chance to visualize the global community of its users as one identity and provide open and free access via any type of internet gadget. The Internet makes it possible to access it with several diverse computing devices without any restriction of device type. It is according to the basic spirit of accessibility and open principle of the Internet. DRM technology application domain is accessible using heterogeneous devices. Whereas the majority of proposed DRM systems are closed source and high relying. The proprietary file formats and custom encoding/decoding and customized software or hardware requirements. Therefore, the protected content of one DRM system is not accessible to other DRM systems and limits the users to enjoy the benefits of interoperability in DRM.

Nowadays, users prefer to use multiple devices and systems to access protected content from various DRM services. Users can use mobile apps, web version, or desktop applications for any operating system. Therefore, DRM service providers should support multi-device compatibility model and allow users to use DRM across a broad range of mobile devices. Few examples of existing DRM implementations aiming to address multi-device include Apple iPod (Cihal et al., 2013) and Sony Open Magic Gate (Awano & Tanabe, 2018).

Security: Security is the prime motivation and requirement of the DRM. Any DRM systems needs to provide content confidentiality and its integrity and should be able to provide robust revocation mechanisms towards unauthorized access users to access users data even in case of Security attacks.

2.7 Macaroon

Macaroon in English is a noun for delight but Macaroon word in computer science literature was first used in a research paper by authors (Birgisson et al., 2014). The author presented a new scheme for authorization credentials. This scheme is particularly targeting decentralized Cloud environments. The authors presented Macaroon as bearer credentials that, provide the functionality of access delegation and access control. Macaroon creates temper resistant access control mechanism and work in similar manner as of Bearer token (Khan & Sakamura, 2017), to address the claim the access to an internet resource. The bearer token is then presented as proof of authorization and after verification of token, you will be given access to resources (Khan & Sakamura, 2017). These bearer token are mostly stored in cookies, in the web application scenario. These Macaroons based tokens are different from bearer tokens as it has attributes attached to them in a stateless manner. They can generate new credentials, impose further permission control to limit its context and all the conditions, once added, cannot be removed from HMAC chain. These features provided the foundation for fine grained access control mechanism for Cloud DRM (Birgisson et al., 2014). This property of Macaroons makes it a suitable for Cloud DRM architectures. Adding conditions to Macaroon is a one-way process and access restrictions (conditions) cannot be removed. These contextual; conditions are also called predicates. This immutable property of caveats is due to the HMAC based Macaroon. Hence, the integrity of access control can be easily verified using the verifier of that Macaroon.

Macaroons can better perform the job of authorization of access to services with restrictions to their access scope in varying context parameters. Which means a user or component with context specific access rights can also generate new Macaroon (bearer token) from their Macaroon(credentials) that reduces the access permission and allow attenuated access (Birgisson et al., 2014). This way the Macaroon’s utilization as DRM in Cloud provides a foundation for flexible and fine-grained access policy which can be useful in any distributed computing deployment scenario. The HMAC encryption is lightweight, and its temper proof property of caveats makes it the best candidate for temper resistant digital resource protection system. Whereas otherwise such a property possible with the complex systems and strong encryptions.

The advantages of Macaroons be leveraged effectively to make a DRM solution for flexible and temper proof Cloud DRM methods. This makes it address the distributed authorization problem in Cloud DRM for more flexible and temper proof credentials. The Macaroon approach to authorization is not significantly explored in literature. In Chapter 3 the study will present detailed research methodology.

2.8 Chapter Summary

In this Chapter, we have proposed presented comprehensive literature review performed to explore the problem statement. We discussed Cloud and Fog DRM and their requirement. State of the art DRM techniques is also presented along with their comparison and open issues. The Cloud DRM authorization issues were highlighted as well. This Chapter also briefly introduces Macaroon and its features toward lightweight and flexible temper proof DRM system.

Chapter 3 will present the detailed research design, methodology, and steps taken to perform the research.

CHAPTER 3: RESEARCH METHODOLOGY

The Chapter 2 presents research landscape ad proposed solutions. It also related studies and gives through background of the methods and their weaknesses and strengths. Additionally, summaries of various techniques used to implement a flexible Cloud DRM system. It also introduced the Macaroon and its approach to authorization in Cloud DRM. This Chapter presents the methodology used in this study and discusses how this study was carried out. This Chapter is organized into four sections. Section 3.1 introduces the methodology and presents the research design. Section 3.2 explains the experimental steps and steps taken to fulfill the objectives. Section 3.3 discusses the software requirements of Cloud DRM.

3.1 Introduction

A comprehensive review and synthesis of the recent applications of DRM for Cloud were undertaken to identify the issues of Cloud DRM and challenges referring to scholarly digital libraries, particularly IEEE, ScienceDirect, Wiley, Springer, Google Scholar, and ACM. The state of the art methods used for DRM and DRM in Cloud were reviewed, and taxonomy of the open issues of DRM was also presented. Many research gaps were discovered via literature review as well as the problems to be addressed in this thesis, details of which is presented in Chapter 2. The identified problem helps to shape the research design.

Research design is divided into several types, for example, qualitative and quantitative research. This study used a quantitative research method. The study obtain and analyzing data from different scholarly databases followed by quantitative analysis using mathematical tools to deduce results. The study attempts to elaborate the significance of the problem, proposed solution and measure the effectiveness of the proposed method in solving the problem.

Apart from the quantitative research method this research also uses historical design, as it collects verifies, and synthesizes evidence from past studies to establish facts that defend or refine its hypothesis. In the context of social schemes, this method can be considered when the primary source of evidence comes from the collection of data from journals and articles which researchers have established as the main way of collecting data in the study as opposed to interviewing and questioners.

To fulfill the first objective the study investigates and analyses a vast amount of literature from past studies on the topic of Digital Rights Management (DRM) and Cloud computing. From those shortlisted studies, the study laid out all the significant methods for DRM in Cloud and figure out that the literature gap of lightweight, immutable and flexible Cloud DRM method. The gap was addressed by identifying an alternative approach to fulfill the research objectives.

The second research objective we fulfilled by highlight and critically discussion the implication and application of Macaroon paradigm into Cloud DRM. An evaluation prototype was then created to evaluate the method and later compared with other related studies. Furthermore, performance benchmarks testing was also performed to identify the optimal technology stack of Macaroon as library itself.

The contribution of this research is to generate new knowledge in the area of DRM, introduce an alternative approach to controlled authorization in Digital Rights Management (DRM) along with its evaluation and comparison.

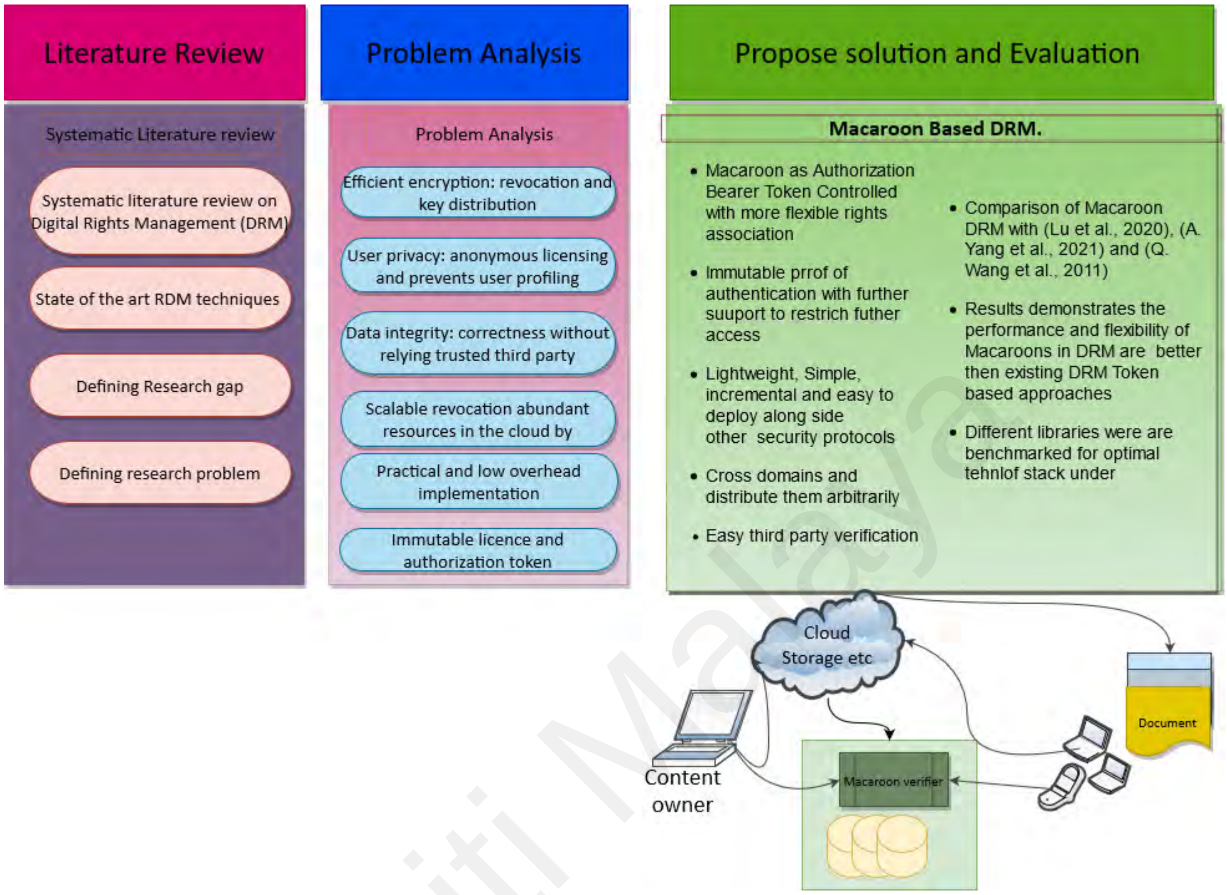

Literature Review
Problem Analysis
Propose solution and Evaluation
Systematic Literature review
Systematic literature review on Digital Rights Management (DRM)
State of the art RDM techniques
Defining Research gap
Defining research problem
Problem Analysis
Efficient encryption: revocation and key distribution
User privacy: anonymous licensing and prevents user profiling
Data integrity: correctness without relying trusted third party
Scalable revocation abundant resources in the cloud by
Practical and low overhead implementation
Immutable licence and authorization token
Macaroon Based DRM.
• Macaroon as Authorization Bearer Token Controlled with more flexible rights association
• Immutable prrof of authentication with further suuport to restrict futher access
• Lightweight, Simple, incremental and easy to deploy along side other security protocols
• Cross domains and distribute them arbitrarily
• Easy third party verification
• Comparison of Macaroon DRM with (Lu et al., 2020), (A. Yang et al., 2021) and (Q. Wang et al., 2011)
• Results demonstrates the performance and flexibility of Macaroons in DRM are better then existing DRM Token based approaches
• Different libraries were are benchmarked for optimal tehnlof stack under
Cloud
Storage etc
Content
owner
Macaroon verifier
Document

Figure 3.1: Research Methodology

3.2 Experimental Steps

The research Methodology was carried out in incremental stages. As shown in Figure 3.1, the research was conducted following the research question and objectives that were set at the beginning of this study.

It was practically impossible to review all the available literature that were related to DRM and Cloud in content authorization. Consequently, the study reviewed articles after carefully shortlisting. The literature review was carried out after selecting over more then One Hundred and Ten (128) research and review articles and figured out several models adopted in their solutions. Reviewed articles were shortlisted to the current number based on the similar models followed by few researchers.

The study particularly review the articles by investigating and accessing the strengths of each of the proposed method in finding solutions to the flexible authorization challenge in the Cloud DRM. The study also summarized the state of the art methods and finally proposed the way forward for Cloud DRM flexible and temper proof integrity protection mechanism for large and heterogeneous DRM applications.

Bearer tokens are widely used as access delegation license. They are issued and handed over to the authorized users. Users receive these tokens and exchange them to gain access to the system or resources. Most of the existing token or rights expression based DRM provides two functions, create the token and verify. We anticipate a Cloud DRM system that will support flexible caveats addition and temper proof licenses for protecting and verifying data integrity. These features will offer more flexible and transparent content protection in a secure and decentralized way.

Immutable proof of authentication with further support to restrict further access Lightweight, Simple, incremental, and easy to deploy alongside other security protocols cross domains and distribute them arbitrarily. Easy third party verification with a time sensitive tradeoff of complexity and flexibility.

The identified problems were critically analyzed and their importance was verified through empirical case study analysis. The performance was evaluated the cost and flexibility of the existing methods to discover research gap. The performance of the proposed method was evaluated via a series of test case benchmark analysis. The cost of operation involved in various portions of the operation was evaluated. The time to perform an overall DRM operation of generating the authorization token and its verification opted as performance metrics in the evaluation. The testing was performed on Ubuntu 14.04 LTE x64 on Intel Core i5 1.80 GHz processor and 2 G RAM. A careful comparison was made with the performance of related methods. Furthermore, benchmarked the performance of different Macaroon libraries for discovering optimal performance optimization among Macaroon implementations. The benchmarking comparison of Macaroon libraries over the Windows 10 platform. The results of performance evaluation were compared with the results of related study.

3.3 Software Requirements

For any DRM application to be very efficient and reliable, strong, and lightweight integrity protection mechanisms might be applied. This will mitigate the risk of infringing intellectual property rights such as tampering, reputation damage, spamming as well as any unauthorized access delegation. The Public Key Encryption (PKE) is widely being used for many security requirements such as anonymity collusion, and content encryption. However, with the extensive and prevalent adoption of PKE infrastructure in Cloud DRM, the need to improve and enhance the capabilities and efficiencies of PKE are becoming more relevant. Therefore, the need of fine grained method to enable lightweight integrity, confidentiality, reliability as well as the authenticity of the Cloud DRM content.

Another prominent method used in DRM is Attribute Based Encryption (ABE). This DRM model satisfies some of the practical security and privacy requirements. ABE has also been found to partially provide finegrained and human-centric access to electronic data (Gjerdrum et al., 2016). The approaches discussed is being used to achieve accountability, transparency, and audits of health data need to be enhanced and supported. Adopting any of the three approaches mentioned will assist to provide security and privacy (Garg et al., 2013). They will also assist in identifying how the authorized entities are making use of critical data.

Efficient revocation of granted access entity is yet important issue. The user dependet access policies and various content of users from different domains is complex to relaise in Cloud environment. The study attempt to reduce to the time of apply the DRM on the data ("A High Secure Medical Image Storing and Sharing in Cloud Environment Using Hex Code Cryptography MethodSecure Genius," 2019).

Watermarking tends to improve content security by embedding the trademark directly into the data, which implements the inseparability of data and security measures. The author proposes a new watermarking technique that combines Reversible, Zero, and RONI. Their method gives high values of Peak Signal to Noise Ratio, and Structural Similarity index. Author (Roček et al., 2016) of the article make use of RONI watermarking for better difficulty level in an attempt to forge the document. The reversible watermarking creates the original image at the receiver side after removing the watermark. As proof of this method, we can mention the possibility of securing the whole image by robust watermarking methods and higher capacity than RONI watermarking. The major disadvantage is the need to create another channel for secure transport to find differential information. Recently proposed watermarking based joining the Blockchain. Their approach demonstrates the robustness and high-level security. These approaches used image Arnold transform to enhance the security and use image DCT coefficients of middle frequency to embed watermark for robustness. Their approach is suitable for large un-tampered ledgers for decentralized rights confirmation. However, this is not a practical constrains of efficient Cloud DRM service. Yet another recent study blind medical image watermarking scheme based on Fast Discrete Curvelet Transform and Discrete Cosine. Transform (DCT) is proposed watermark data is performed by correlation of White Gaussian Noise (WGN) sequences (Rana & Sur, 2016). This approach output the mandatory noise in the recovered image. Also, this method cannot embed text data as watermark only binary data is possible.

Authors (Anjum et al., 2018; Easley et al., 2012) proposed an efficient file protecting DRM that enables the user in a non-interactive way to search the files in their encrypted form and consume the files. The proposed approach is targeting only a file that contains certain private keywords. It is a kind of group decryption that the user downloads and decrypts all the materials he is authorized.

Another study (Ahmed et al., 2019) presented a model to data provenance suitable to the decentralized environment and which doesn't rely on trusted third-party. They archive secure provenance becomes provenance records are chained through an aggregated signature approach. Furthermore, the proposed scheme is capable of detecting attacks introduced by multiple consecutive colluding users. The proposed scheme is suitable to save computational and storage cost. However, it involves string encryption and the latency of encryption operation is not as good as the Macaroon approach. The detailed analysis and results is presented in the next Chapter 4.

3.4 Chapter Summary

This Chapter presents the research methodology and how the research was conducted in finding the answer to the research questions. The next Chapter 4 will present the prototype and evaluation of the proposed solution. The next Chapter will leverage the Macaroon property, its sub-operation, and further performance analysis of Macaroon libraries and comparison.

CHAPTER 4: RESEARCH DESIGN AND EVALUATION OF MACAROON

4.1 Introduction

This Chapter presents the design, engineering and evaluation of the proposed method which involves the use of Macaroon, aims at a more flexible DRM approach, suitable for decentralized authorization. Multiple figures and table have been used to explain the series of experience and results to justify the flexible and lightweight Macaroon approach to Cloud DRM.

Establishing a Transport Layer Security (TLS) based secure online connection that makes sure data confidentiality, request authenticity, and payload integrity is a requirement for service and infrastructure identity and legitimacy. But in the service delivery model authentication of each request is not a suitable approach to validate the legitimacy of the request. The concept of authorization is applied to delegate access to an already authenticated service. Strong and secure authorization schema make an additional wall of defense against content abuse by, temper resistant, prevent masquerading the identity, and controlled delegation of digital access. Yet, authentication only is insufficient to toughly make sire content security as a trusted and authenticated service, or users could also be malicious may elevate access to cause privilege escalation. In order to mitigate this risk, a new methods for robust and context-aware authorization are needed. In DRM license service need flexible authorization technology to manage the licenses. This is where Macaroon can be used to form an efficient and flexible approach to license authorization.

Figure 4.1 explains authentication and authorization scenarios. In basic authentication schemes, users need to provide the username and password to log in but after the user is login it gives a token. The token is used as a substitute for a valid username and password. Users with a valid token can access the service.

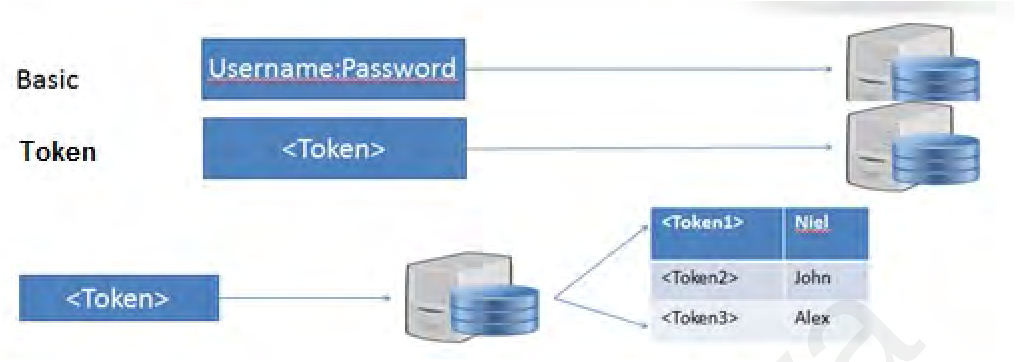


Figure 4.1: Basic and Token Based Authentication

The most basic solution that involves explicit trusted an authenticated DRM service which processes its requests. In the DRM trust, the accessibly is managed by an authentication service. The service should make data available to authorized users. The authorization security control has to limit the scope of the license to only the authorized user as well as the user's context in which a particular request is being serviced. The efficient revocation of licenses is an important aspect as well. Thus, importance of find grained access control schemes to protect the content from unauthenticated client resources legitimate authorisation. If we consider a traditional file sharing scenario, the HTTP is mostly used with its build its authentication to block all connections except the legitimate ones. Whereas this PKE based secure connection and login security approach prevents the malicious request. But after login, the authorization mechanism acts as an additional layer of security. Still, the implementation of authorization does not remove the problem of a compromised service. If a legitimate service is compromised, it could request access to the target service until the compromise is monitored and acted upon. But it does limit the effect of content compromise (Suomalainen, 2019).

4.2 Macaroon Construction and Usage

Creating the Macaroon is also called minting the Macaroon. Figure 4.2 mentions the formula of HMAC used to generate a Macaroon.

$$\mathrm{HMAC}(K, m) = \mathrm{H}\Big((K' \oplus opad) \parallel \mathrm{H}\big((K' \oplus ipad) \parallel m\big)\Big)$$

Figure 4.2: HMAC Formula (Birgisson et al., 2014)

Where

- *H* is a cryptographic hash function
- *m* is the message to be authenticated
- *K* is the secret key
- *K'* is a block-sized key derived from the secret key, K; either by padding to the right with 0s up to the block size or by hashing down to less than the block size first and then padding to the right with zeros
- *//* denotes concatenation
- *⊕* denotes bitwise exclusive or (XOR)
- *opad* is the block-sized outer padding, ipad is the block-sized inner padding,

This Macaroon definition is defined in RFC 2104 (H. Krawczyk; M. Bellare; R. Canetti, 1997).

Macaroon consists of a public and private part. The private part is the HMAC generated with a symmetric key and the public part consist of random nonce along with a set of conditions a.k.a called caveats. The caveats enable complex assertions like - "trust this as long as it satisfies these caveats"(Anantharaman et al., 2016). These caveats form the public part of the Macaroon. Macaroons can chain together, e.g., a service *S1* with public Macaroon *m1* and secret *k1* can use *k1* to generate a Macaroon *m2*, *k2* for service *S2,* and so on. Generally speaking, Macaroons are created by producing an HMAC tag of the content to provide content integrity and authenticity (Birgisson et al., 2014; Suomalainen, 2019). Due to the nature of HMAC, Macaroons can be created in layers by adding more and more caveats, each time producing a new signature of the token content. Figures 4.3 and 4.4 show a simplified view of Macaroon which is acting as key to identify the users in the table.

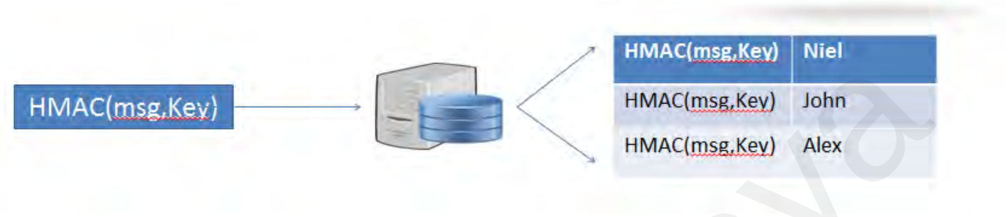


Figure 4.3: Simple Illustration of Macaroon as Bearer Token

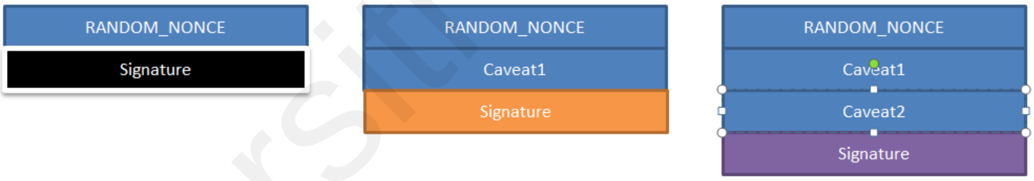


Figure 4.4: Macaroon Layers as Chaining

The caveats are then verified by reconstructing the chain of HMACs and comparing the resulting keyed digests. First, a nonce is needed, which is an arbitrary cryptographically secure random or pseudo-random number (Anantharaman et al., 2016). Figure 4.5 illustrates how a basic Macaroon looks like after appending the read-only permission as a caveat.

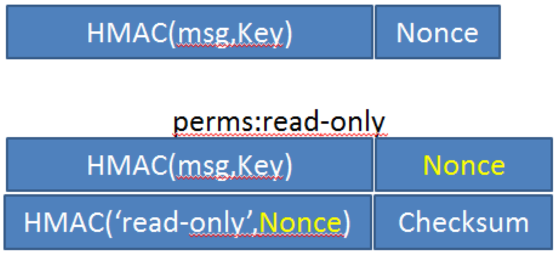
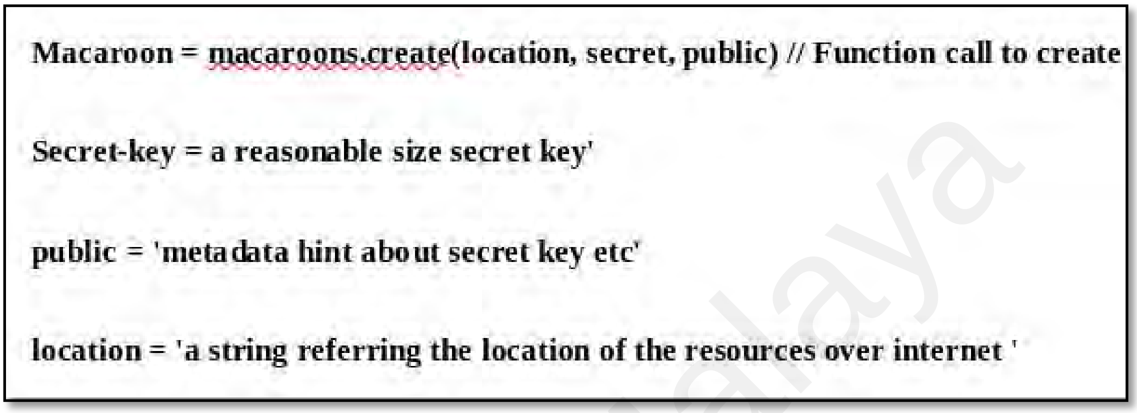


Figure 4.5: Basic Macaroon with One Caveats

Macaroons can be created with a validity caveat in them. These validity caveats along with other caveats can generate the validity of Macaroon by racking it life span. As we add caveats Macaroon is signed with the validity caveat and custom value lifespan can be set. This Macaroon is then being shared to any entity we want to delegate the access. Once the validity caveat is expired, it expires the Macaroon as well, making the Macaroon is invalid.

The caveats mentioned so far as first party caveats as they do not require any additional verification or authentication from an external entity. Macaroon's security is based on the security properties of the used HMAC algorithm (Birgisson et al., 2014). This means security is dependent on the one-way hash function and the nature of the key (H. Krawczyk; M. Bellare; R. Canetti, 1997). As Macaroons use HMAC as a black box, a Macaroon solution can be made more secure by choosing an HMAC algorithm with stronger security properties, such as a SHA512 instead of SHA256. This will increase the size of the signature which affects for example the amount of bandwidth used and storage requirements. This means that the key we need to use security algorithm proven secure as per the recommendations of the National Institute of Standards and Technology (*NIST*, 2020).

More specifically, the creation of Macaroon involves location, secret-key, and public as described below. These three parameters need to be passed to create a Macaroon as shown in Figure 4.6.

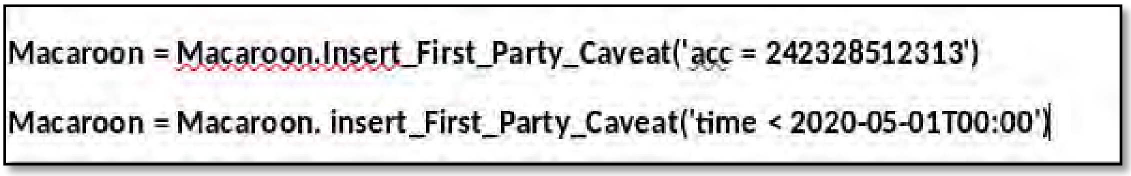


```
Macaroon = macaroons.create(location, secret, public) // Function call to create

Secret-key = a reasonable size secret key'

public = 'metadata hint about secret key etc'

location = 'a string referring the location of the resources over internet '
```

Figure 4.6: Basic Building Blocks of Macaroon

And after successfully creating the Macaroon the value *Macaroon.identifier* refers to public value, Macaroon.location to location and Macaroon.signature to the HMAC value assigned to this Macaroon.

We can call the add caveats to function passing caveats as parameters. Each time we add new caveat the signature vale of Macaroon is changing or in other work Macaroon is refresh with a new HMAC signature. As shown in Figure 4.7, two caveats are attached to Macaroon. In first the condition is the value of *acc* must match with number *242328512313* while in the second condition, *time* is matched with value *2020-05-01T00:00,* and for successful verification of Macaroon time must be less than this value. This time value can control the validity of the Macaroon as both caveats need to satisfy for the successful verification of Macaroon.



```
Macaroon = Macaroon.Insert_First_Party_Caveat('acc = 242328512313')
Macaroon = Macaroon. insert_First_Party_Caveat('time < 2020-05-01T00:00')
```

Figure 4.7: Adding First Party Caveat to Macaroon

Macaroon can be shared with other entity, after applying an encoding process called serializing. Serializing usually involved base64 encoding, and safety serialized form token is made sure by transporting over HTTPS protocol. Macaroon serialization operation looks like this command *Macaroon.serialize(format=1)*.

Similarly, the deserializing in the opposite operations then the serializing and it takes encoded Macaroon and decode it to plaintext and can be accessed using following representation:

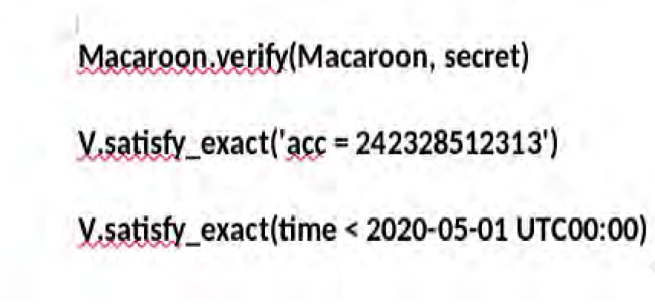
Macaroon = macaroons.deserialize_function(encodedMacaroon).

The verification process will need the Macaroon and its secret key. One can get the secret using deserialized, Macaroon and its identifiers from Macaroon can be accessed like following statement:

Macaroon.identifier.

First party caveats are the conditions to be verified by one service. If one service needs further verification form another service, it’s called third party verification and uses third party caveat. In the case of first party caveats, we need to inform the verifier by providing the values. e.g. *acc* value of *242328512313* and *time* must be less than *2020-05-01 UTC 00:00*. This is shown graphically in Figure 4.8. The verifier has two caveats to check, *acc* value must match *242328512313* and the current *time* should be less than the value *2020-05-01 UTC 00:00*. This way we can add as many contextual caveats to restrict the scope.

Only the authorized user with *acc* value is *242328512313* can further add immutable caveats to this Macaroon but cannot remove any caveats.



```
Macaroon.verify(Macaroon, secret)

V.satisfy_exact('acc = 242328512313')

V.satisfy_exact(time < 2020-05-01 UTC00:00)
```

Figure 4.8: Macaroon with two first part caveats

Macaroons allow conditions (a.k.a. caveats) to specify access parameters (called predicates) that are co-enforced by external entities or third parties. A Macaroon with a third-party caveat required the successful grant of access from third party entities as well. This constitutes less coupled distributed systems in the job of processing authorize requests and provide ground for separating data from the policy. For example, Cloud storage can provide Macaroons that are validated if and only if the client application's authentication service verifies the authenticity of the user. The user get proof of its authentication from the authentication service. It can be presented as proof alongside the original Macaroon, to the Cloud service. The Cloud storage service can validate ad verify that the user is actually authenticated, without knowing anything about the authentication service's of third party entity and its implementation. In a possible standard implementation, the storage service can authorize the request without even communicating with the third party authentication service. The user’s is responsible to present the proof of authorization from the third party entity and present to verifier for verification purpose.

As discussed in the previous section, the Macaroons approach intrinsically segregates data form the access policy attached to it. The policy of your application (What, who, and when can access), from the enforcing algorithm (the code that enforces this policy). It is due to the way the verifier is designed; it hides the access policies it is implementing. It just analyzes the policy (as appended evidence) and validates that the provided evidence is correct. The policy defined at the time of the construction of Macaroons and distributed. A third party application can easily make sure within the application, and make sure that its policy is followed, as Macaroon travels.

Macaroons carry their proof of authorization, which is cryptographically secured, this is the core reason they are efficient. A Macaroon's caveats are composed using chained HMAC functions. The HMAC chain allows it to add a caveat, but impossible to delete a caveat. When a service adds caveats, it attenuates the access level of Macaroon and passes to another application. The cryptographically protected conditions (caveats) that cannot be removed from the Macaroon. Only the entity that is creating a Macaroon can verify it when presented with the embedded proof of authorization.

Macaroons can be used to implement a single, unified model integrated with existing authorization mechanisms. It can also be used as new types of authorization for Cloud DRM applications. It can also be used to improve the trust among Cloud entities as well by strengthening the authorization of data flow among entities. They are useful for many existing end-user Cloud application scenarios. For example, a Macaroon can be minted for sharing an image on Google Docs or Dropbox, with third-party caveats limiting its use to a particular set of users.

A related study purely on Macaroon as bearer token was performed by (Suomalainen, 2019) and their performance benchmark the different encryption algorithms. 256 bit (ECDSA), 2048 bit RSA, and 4096 bit RSA were used in the comparison. Their results show signing and signature verification using the NIST Curve P-256 and RSA signing and verification operations with the key length of 2048 and 4096 bits. ECDSA was found to be efficient in signing, while the 2048 bit RSA was better in verification operations. The performance difference is meaningful enough to impact the choice of algorithm depends on the size of the requests the tokens are passed along and through that how much of computational overhead the verification operation represents.

4.3 Macaroon Utilization in DRM

A study propose to use proxy re-encryption (Wood & Uzun, 2014) based on access delegation across entities. Their approach was extended by appended users attribute to the key, making it efficient and it's called Attribute based proxy re-encryption (RBPRE) (Abe et al., 2013; Garg et al., 2013; Q. Huang et al., 2013; Qinlong et al., 2014; Yao et al., 2019). Maintaining Access Control Lists (ACL) is also used to regulate access control. Another method, uses a matrix representation of licenses per column per resource. This approach is helpful in data-oriented environments, however, in service-oriented communication context it binds the access rights to object which make it less suitable for authorization operations. Subsequent efforts were still struggling with fine-grained access control in Cloud computing with efficient revocation and license immutability (De Angelis & Di Marzo Serugendo, 2017; Ma, Jiang, et al., 2018). In service oriented software model, the context with TLS, the authorization decision can be based on information embedded in certificates received from an internal certificate authority, as the client certificate is evaluated during the TLS handshake only. Therefore, it is important to increase the authorization security for service-oriented model.

The tokenization approach to authorization is being used in past few years. The most popular approach uses JSON Web Token (JWT). It use an encoded object which carries authorization proof, cryptographically signed or protected with a Message Authentication Code (MAC) algorithm. Its compactness requirement is based on the way they are transferred, which is via HTTP Authorization headers. Few of know variant implications are JSON Web Signature (JWS) or JSON Web Encryption (JWE). JWT has three parts, header, payload, and signature. The header of a JWT describes the type of the object and what algorithm was used in signing or encrypting it. The payload includes the actual claims, the biggest edge of Macaroons over JWTs lies in the third-party caveats it make possible. For example, Macaroon could augment it with a third-party caveat and present a valid token from the authorization service X, which the target service verifying the Macaroon would then be able to verify from the external authorization service X.

Macaroon can be used for efficient first party and third authorization in DRM service. This will help robust license integrity validation which is not possible with traditional approaches. The level of flexibility Macaroon caveats offers helps in easily decoupling the policy with data and its best suites the DRM Cloud service authorization.

Figure 4.9 describes the mechanism, how DRM could work with Macaroon. Lets consider the scenario of request authorization. The user requests an access token from DRM service gateway B, to access the DRM protected data D, of service X. DRM gateway B will get the public key of service X, as they are partners to implement the Macaroon DRM model. This key will be exchanged over a secure medium. Then the service gateway will mint a Macaroon (similar to bearer token) and append the third part verification caveat for service X. User will receive the Macaroon with third party caveat and eventually it will contact service X for a discharge (permission) Macaroon, to consume the data D via DRM gateway. After receiving a valid discharge Macaroon form

X the gateway will then verify the discharge and grant access to resources. This Macaroon will essentially act as a token however its immutable nature, platform independence, and unlimited caveats will make its suite lightweight and flexible authorization even with the third party. The ease of built-in third party integration can serve the foundation for future federated DRM service and solve interoperable issues as well.

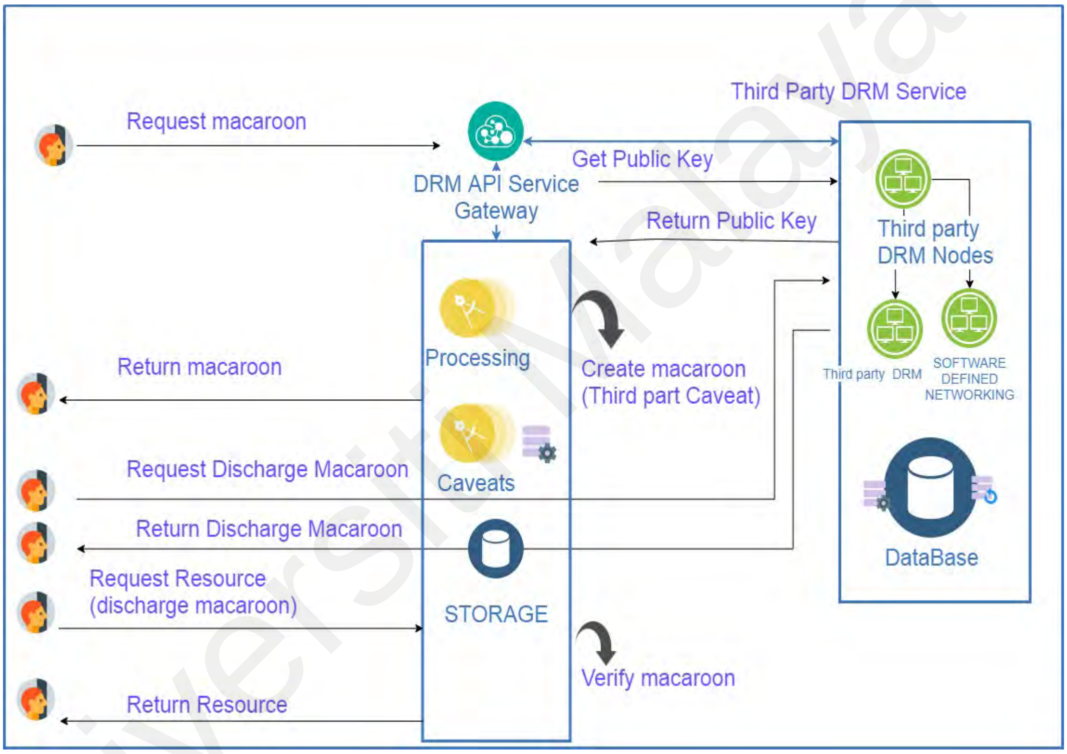


Figure 4.9: Macaroon Use case and Interaction as DRM

4.4 Macaroon DRM comparison with closely related solutions

In Macaroon DRM scheme, the main communication cost generates between verifying the Macaroon from central verifier or in case of multi-party authorization involved discharge Macaroon. The Cloud hosting send minted Macaroon for DRM request to request. Verifier will be notified of the Macaroon consumer that it has authorization proof for the access. Verifier will check the authenticity of Macaroon and then will be able to decode the give component for access to the Cloud DRM resource. The overall communication cost and verifying cost has been compared among three closely related studies by (Lu et al., 2020), (A. Yang et al., 2021) and (Q. Wang et al., 2011) in Figure 4.10 and 4.11 respectively. The aforementioned related studies used a tree-like data structure which is closely related to HMAC chain based Macaroon DRM approach. The tests were performed in Linux Ubuntu 14.04 LTE x64 on Intel Core i5 1.80 GHz processor and 2 G RAM.

The content was divided into blocks and fix number of blocks of data were used. The time was the calculation for the overall request authorization token generation and its verification. Fix the number of the block were used to repeat the iteration from 100, 200, 300, and 400 to compare the efficiency of the proposed method.

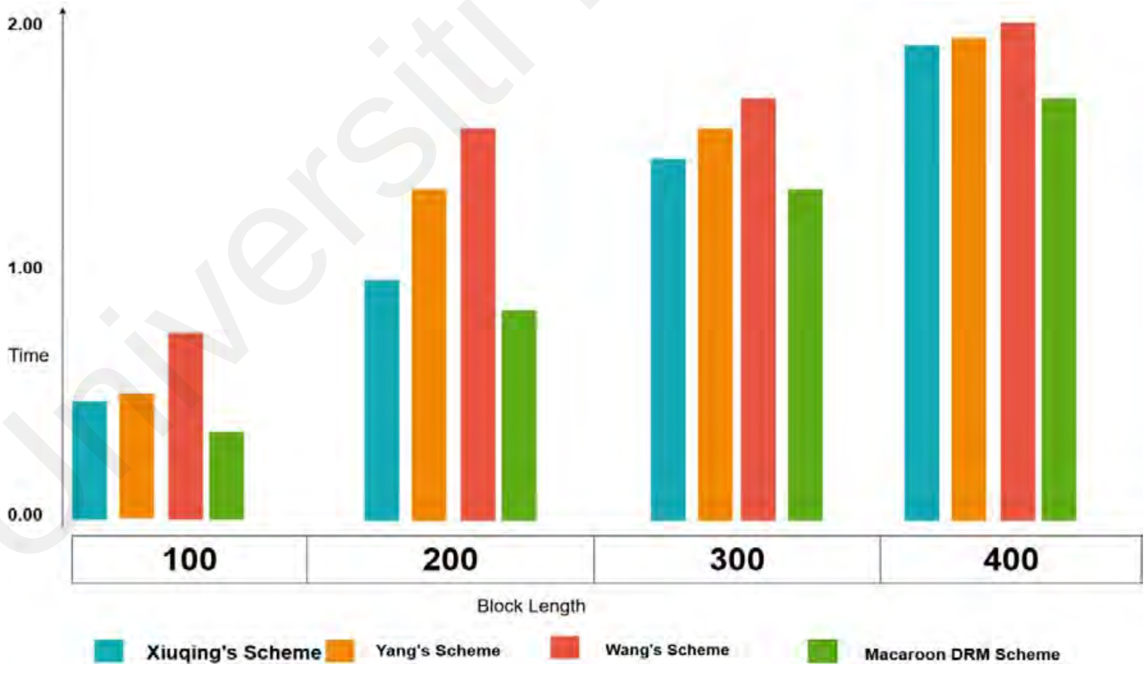


Figure 4.10: Comparison of overall delay in the mechanism

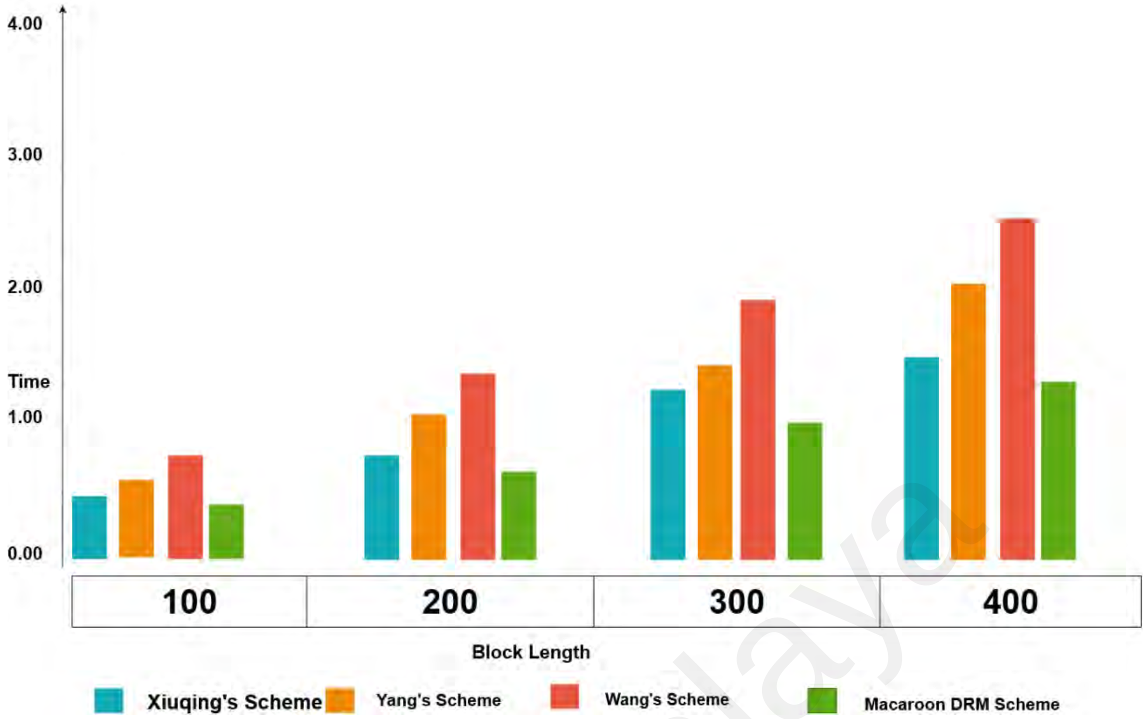


Figure 4.11: Comparison of verification time

Figure 4.10 and 4.11 shows that Macaroon based DRM method is giving better performance than the other three and it's more flexible and immutable by design to better suits Cloud DRM as well as immutable policy requirements.

4.5 Benchmarking of Macaroon Libraries and Evaluation

There are many Macaroon implementations of standalone Macaroon available as libraries. Python (Evan Cordell, 2017), Java (Martin W. Kirst, 2019), JavaScript (Roger Peppe, 2018), PHP (Mickaël, 2014; Networks, 2014) and c++ (Konrad Zemek, 2015).

This study also evaluated the benchmark among various operations of Macaroon construction, serialization and deserialization, and verification. We generate the data by implementing the tests and running the benchmark for JavaScript (Roger Peppe, 2018) and PHP (Mickaël, 2014) implementation. The simulation results are compared with the Java benchmark results by (Martin W. Kirst, 2019).

The following Table 4.1 list the benchmarking result for various configurations. The first column of table list the Macaroon operation and the results of latency in different programming languages are mentions in subsequent columns.

Table 4.1: Performance benchmarking among libraries of Macaroon

Function	Java	JavaScript	PHP
Serialize_with_key_string	252302	19,836	15,231
Serialize_with_key_bytes	424008	19,537	22,202
Serialize_with_key_bytes_and_1_caveat	242060	15,015	14,554
Serialize_with_key_bytes_and_2_caveats	166017	12,126	10,112
Serialize_with_key_bytes_and_3_caveats	127712	10,257	6,267
Deserialize_and_Verify_key_bytes	457262	45,504	26,398
Deserialize_and_Verify_key_string	262689	43,859	12,007

The benchmarking test is performed in windows 10 x64 Intel core i7 JavaScript. Java is a more popular technology and popular because of its speed of expectation. Java executes the byte code in its special Java virtual directly. JavaScript based nodejs is emerging as a popular technology for its asynchronous coding design where everything is executing in one thread and this achieves less throughput then synchronous programming PHP. However, the Java library is performing the lowest among JavaScript and PHP. The PHP based library gives maximum throughput as it can be seen from Table 4.1 that PHP based Macaroon library is giving lower latency then JavaScript and Java. This is because the PHP implementation is closer to the operating system and is simpler and takes less time to compute arithmetic operations.

Overall, we can see the verification of Macaroon is lightweight which makes it suitable for Cloud DRM. Java, JavaScript (nodejs), and PHP are three popular backend technologies therefore the analysis and results will be useful to evaluate the Macaroon performance in the individual implementations. The results will be useful in selecting technology stack for DRM implementations and set directions for further enhancement of the Macaroon library, its standardization, and increase adoptability for enhanced use. The choice of the technology stack and design pattern is important in delivering optimal Cloud services. Therefore, it is useful to estimate the cost of operation. The lightweight verifying capability is also useful for third party caveats verification and the performance of Cloud DRM.

4.6 Chapter Summary

This Chapter elaborates the Macaroon construction, utilization as part of the DRM system. This Chapter also describes Macaroon library evaluation and comparison of different implementation. Next Chapter 5 will discuss the thesis objectives and contribution.

CHAPTER 5: ENGINEERING MACAROON FOR DRM

This Chapter discusses the findings of this study by pointing out its achievements. It also discusses the findings of the study and analyses its limitations.

5.1 Research Contribution

This study represents Macaroons as an alternative method for lightweight, flexible, and tamper-proof for integrity in releasing immutable integrity protection methods and flexible policies for DRM in Cloud. The proposed method is analyzed and critically discussed, how the Macaroon approach could achieve tamper-proof and flexible authorization in Cloud. And also, how the aforementioned method can build an efficient DRM solution. Macaroon based solution is constructed using HMAC chain. This feature along with the flexibility to add unlimited caveats and its temper-proof nature of HMAC chain generate lightweight credentials. This way the aforementioned method is better than the existing authorization techniques used in Cloud DRM for flexible and efficient access control management and practical constraints. This study also analyzes the operation cost of Macaroon by benchmarking its libraries. The benchmarks result correlates the implementation technology with the performance of sub-operations.

This thesis aims to improve content security at the application layer by proposing Macaroon as a method for Cloud DRM solutions. This study archives the objective outlined in section 1.4 by reviewing the problems of Cloud DRM and identified the state of the art constraints. Moreover, challenges in designing DRM technologies better and a flexible way of protecting the intellectual property of online content in a distributed computing environment.

5.2 Implication of Research

Macaroon with its chain of temper proof authorization with lightweight verification is found to be suitable for flexible authorization of content in Cloud DRM. Protecting and verifying the integrity of content in Cloud DRM is an important issue to address. In order to address this for improved flexible and lightweight method, Macaroon in Cloud DRM is found to be lightweight solution as copared to closely related studies. The prominent difference is to achieve similar benefits with Authorization Bearer Token having less room for flexibility and complex distributed scenarios of rights association. Therefore, it is important to bearer tokens that tamper proof to some considerable degree. In this study, we propose temper resistant integrity protection solution for Cloud DRM leveraging Macaroon. The tamper resistant nature of Macaroon caveats makes it satisfy an important feature of secure DRM system which resist against various attacks. Hence, focusing on the solution perspective, we have demonstrated the Macaroon DRM method involving a digital token from its generation and storage to circulation between different players, and final redemption.

We have analyzed the benefit of lightweight, flexibility, and immutability from DRM perspective. The sub-operation of the Macaroon creation, verification, etc are giving benefits of immutability proof of access with much flexibility to further limit the access in a standalone manner. The evaluation of Macaroon approach for Cloud DRM and estimate the cost of Macaroon sub-operations and comparison with the implementation of different programming language. Macaroons applicability to large and open distributed systems for content protection and performance comparison of various related studies prove its flexibility.

5.3 Comprehensive Analysis of The Most Related and Salient Works

The study started with a systematic literature review of the DRM technologies being proposed in the DRM. The generic DRM system have been taken as a reference and aim on supporting flexible applications with Cloud DRM features. The systematic literature review to understand the useful methods to solve the said problem. The literature was mainly gathered by applying search queries in academic journal and conference databases with the relevant keywords, such as digital rights management, Cloud DRM, Cloud authentication, and decentralized authorization. The downloaded literature was studied in depth in summarizing the approach and future challenges.

In the beginning, this study established some standards for a new DRM Cloud system for better performance and security. This study also discusses Fog Computing in DRM to solve the latency problems in Cloud DRM in section 2.3. The taxonomy of Cloud DRM elaborates the problem of Cloud solution including need of flexible and lightweight integrity protection method in Cloud DRM.

5.4 Research Gap and Analysis

As millions of users use social media to share pictures, videos, and other daily life documents. This sharing is a very common and useful way of exchanging personal content and information. What makes these social services so unique and attractive to users is not the fact that they allow them to know other persons, but the fact that they allow the users to expose their network of friends to others and share their content. But the user has very limited control over its data after the data is available on social networking or Cloud storage platforms whereas the platform and authorized user can tamper with the data and easily republish it.

The feature of online social networking platforms allow users to share their social network with others, and user can also see the social network of others. The targeted audience to see the shared content can be the direct connection or the further links of our direct connected users or anyone on the same platform with a valid account (regardless of the weather it's your connection or not). These social network sharing functionalities are very important and inviting further social interaction. However, they are at the same time, the cause of serious privacy and security concerns. Currently, the sharing control is not on the end-user side, but on the social platform side with a limited set of features for users to protect its privacy and intellectual property. Ideally, users should be able to handle their content and define the boundaries and rules of access to it. This is something that does not yet happen in most current social networks.

Most of the online social networking platform uses Cloud computing paradigm to store and serve data. After user transfer the data in any Cloud-based storage provider, the data itself is managed by the Cloud provider and the data owner have little control over its data in rest or when the user shares the data with another user or with the online social media platforms. DRM in Cloud refers to the technology which enables content publishers to access control on its contents for the content consuming devices. DRM in the Cloud is necessary, to preserve intellectual property, to manage data confidentiality, data integrity, and data security, especially after content, is shared with the third party. This third party verification feature is an emerging topic of research an optimal access technology can help to solve the problem in Cloud DRM.

In the literature the prominent DRM paradigms are: Attribute-based Encryption, Advance Watermarking (Ma et al., 2016), DRM relying on Trusted third party (TTP) (Birrell & Schneider, 2013), DRM Without relying on TTP (Win et al., 2012), and Blockchain (Public verified)(Ma, Jiang, et al., 2018) based DRM were proposed. However, the Message authentication code approach to DRM is not significantly explored. As Macaroon approach can provide easy and practical authorization therefore this study analyzed the Macaroon approach to DRM for flexible and temper proof solution for data integrity in distributed computing.

Macaroons DRM could provide a better solution, as it provide better delegation of authorization, autonomous attenuation, and scalable cross-domain, storage providers are now exploring how to use Macaroons (Birgisson et al., 2014). Example of storage systems which are also known to be exploring Macaroons and its benefits to their storage system (SurfSARA, MinE, dCache, and SWESTORE) (Millar et al., 2018). Fast revocation, carry its cryptographic signature as proof for access are among the attractive features. Table 5.1 presents the comparison of Macaroon DRM with closely related Cloud DRM approaches.

Table 5.1: Macaroon Cloud DRM Comparison With Traditions Approaches

DRM Feature	Related Studies	Macaroon based DRM in Cloud Computing
Multi-user searchable encryption (MSE)	(Deng et al., 2017)	The multi-user search is not supported
Focus of ABE	(Xie et al., 2021), (Cui et al., 2018; X.-J. Lin, Wang, et al., 2021; Pareek & Purushothama, 2020; Sultan et al., 2018; Voundi Koe & Lin, 2019)	Unlimited distinct contextual attribute could be added and supported
hybrid cloud environment	(Esposito, 2018; S. A. Hussain et al., 2017; Sultan et al., 2018; Tapas et al., 2020; Xie et al., 2021)	Better in term of complexity
aims to reduce the computation overheads	(Cui et al., 2018; Deng et al., 2017; Lu et al., 2020; Shen et al., 2017; Sultan et al., 2018; Tapas et al., 2020; Xie et al., 2021)	Better in terms of Lightweight and chain of HMAC make it more suitable for resource constrained environments.
improve the efficiency	(Bernal Bernabe et al., 2014; Esposito, 2018; X.-J. Lin, Sun, et al., 2021; X.-J. Lin, Wang, et al., 2021; Lu et al., 2020;	The method is more flexible and brings more

	Shen et al., 2017; Sultan et al., 2018; Tapas et al., 2020; Xie et al., 2021)	performance and implementation efficiency
Physical Access Control System (PACS).	(Antonolpoulos et al., 2018)	Not supported
Simple and flexible approach	(Chadwick & Fatema, 2012; Cui et al., 2018; Voundi Koe & Lin, 2019)	Unlimited attenuation makes it a far more flexible method
Integrity protection	(Lu et al., 2020; Shen et al., 2017)	Bring immutability by design into cloud DRM

5.5 Evaluating the Macaroon's Operation Used in DRM

Macaroon carries its proof of authorization as a chain of delegations. In this way, the delegated authority enjoys the same level of access and without involving too much process complexity. Each Macaroon is to grant permission, thereby appending more caveats (conditions) to which result in further squeeze the permissions. The attenuation is possible not only by original creator of Macaroon but any intermediate authorized entity, which can reduce scope of Macaroon by appending caveats. To use the delegated permissions, the attenuated Macaroon can be presented to the service provider. The service provider can verify whether the nonce of the caveats in the Macaroon is modified or not as from originally issued by the service provider. The performance comparison of the aforementioned approach shows its giving better performance. Moreover, the benchmarking results aim to evaluate the Macaroon operations cost (time) in various libraries to quantify the optimal deployment scenario of Macaroon in Cloud DRM. The Macaroon system model and benchmarking results will be useful in selecting technology stack. DRM implementations and set of directions for further enhancement of the Macaroon library its standardization and interoperability for enhanced use.

5.6 Challenges of Macaroons

Macaroon are developed based on the assumption that the service wish to give access permissions to another service and both are already communicating with each other.

Macaroon also are disjoint from the security of underlying channel and assume it to be secure. It is only dealing with the delegation of the existing permissions of a service. These features of Macaroon make it work as a standalone and flexible discovery mechanism. The minting and reconstruction of a Macaroon require the root secret key. This implies, either the minting or verifying is done solely by that one service or the secret needs to be shared. This in turn requires methods for secure distribution and management of secrets. Macaroons are designed for short time permissions and the order of access permission is not significant. Macaroons heavily depend on service providers using it. The Macaroon works in the same context as the service Cloud provider gave at the beginning of granting access and the level of access is attenuated as its delegate. Every time a Macaroon is attenuated it transforms into another Macaroon. Only the initial service provider can verify these delegated accesses Macaroon. In both of these systems, only the service provider can verify permissions. Macaroons constitute a simpler system and have performance benefits. This study summaries the discovered pros and cons of Macaroon in Table 5.2.

Table 5.2: Advantage and Disadvantages of Macaroon as Authorization Token

Pros	Cons
Possible for secure HMAC option only	Formalization of the logic needed
Unique feature of Third-party caveats for authentication and authorization.	Lack of interoperability and platform dependency.
Simple one-way hash function acting as standalone encryption.	Minting and verification using symmetric cryptography creates secrets management challenges.
Unlimited combination to attenuation and delegation of access bring flexibility.	Lack of standard implementation more burden over developer.
Enables granular resource-level access control based on the set authorization policy.	The addition of more features, the more logic needs to be implemented on the application level.

5.7 Chapter Summary

This Chapter discusses the findings of the proposed Macaroon DRM approach and its evaluation and limitations. This Chapter also highlights potential areas for future improvement.

CHAPTER 6: CONCLUSION AND FUTURE WORK

This Chapter is to conclude the study by highlighting its achievements and to provide direction for future work.

The content abuse and intellectual property rights violation is a growing challenge in online space. More and more personal and critical business information is moving among parties for collaboration and sharing purposes. Over the past decade, many DRM approaches attempt to achieve optimal authentication and authorization. The traditional authorization mechanisms are not directly suitable in Cloud paradigm as most of the proposed DRM methods add an extra level of complexity and performance tradeoff when it comes to scope attenuation. This study proposed and analyzed the temper proof and flexible authorization method in Cloud for an efficient DRM solution with easy access attenuation.

6.1 Research Contributions and Achievement of Objectives

The main objective of this research was to explore and propose a flexible and temper proof authorization mechanism to be used in Cloud DRM services. This approach to authorization will easy out fine-grained access control implementation in Cloud DRM. The objectives were successfully met with the proposed Macaroon based solution which is constructed using HMAC chain. The Macaroon feature with the flexibility to add unlimited caveats and its temper proof nature of HMAC chain generate lightweight credentials that are better than the existing authorization techniques proposed in Cloud DRM.

The contributions of this research are as follows:

- A thorough analysis of various existing Cloud DRM techniques was conducted in this research to assess the limitation and area of improvement. The challenges and limitations discovered in the state of the art DRM technologies. The closely related techniques in literature which also aims to protect the integrity and the intellectual property of online content in a distributed computing environment are presented by authors (He et al., 2014; Khan & Sakamura, 2017; Ma, Jiang, et al., 2018). An improvised technique subsequently was proposed based on temper proof and flexible credentials suitable for distributed deployment. The immutable feature of Macaroon based DRM will provide data integrity along with context dependent flexible licenses policies for fine-grained access control in Cloud DRM.

- The proposed alternate approach to authorization in Cloud DRM using Macaroon enabled flexible and lightweight temper proof credentials in Cloud DRM. Macaroon with the flexibility to add unlimited caveats and its temper proof nature of HMAC chain generates lightweight credentials that are easy to transport similar to Bearer token in web applications stored in a cookie in browsers. Macaroon are platform independent technology so their strong feature of temper proof credentials and seamless support to apply in Cloud DRM make it a good candidate for Cloud DRM in service oriented environment.

- The evaluation of Macaroon DRM was performed by comparing the computation cost of overall latency of proof generation and verification process. The results show Macaroon DRM approach is lightweight and flexible then the other approaches. The performance benchmarking of various Mcaroon libraries show the PHP based library is giving better performance them JavaScript and the Java based library.

6.2 Analysis of The Related Works

The achievements of the research objective in this study are further elaborated in the following sections:

1. To study the current Cloud DRM techniques.
    - A comparative study of existing Cloud DRM techniques is thoroughly conducted in this research. The details of existing techniques were presented in Chapter 2. It can be concluded that the Cloud DRM techniques were mainly focusing on strong encryption and complex implementation for the immutable license. To the best of our knowledge, none of the techniques was proven flexible and immutable licenses to track the integrity of license when applied to DRM in the Cloud. With this finding, the first objective of this research was successfully achieved.
2. To propose a suitable technique for Cloud DRM targeting on a flexible authorization mechanism.
    - Macaroon based new method for authorization in Cloud DRM has been proposed in this research. The objectives were successfully met with the proposed technique, as Macaroon which is based on HMAC chain generates a bearer token that carries its proof of authorization. The cryptographically protected proof of authorization carries the access control policy and the conditions in policy can be further attenuated by any other authorized service. This gives flexibility to any authorized service to further reduce the scope of access by utilizing unlimited contextual parameters.
3. To evaluate the proposed technique in terms of its performance.

- The performance of the proposed technique was analyzed and compared against closely related Cloud content authorization techniques. Results show that the proposed technique performs better flexibility in authorization in Cloud DRM. The proposed technique also provided a lightweight approach to protect and validates data integrity in distributed computing. The benchmarking of various Macaroon sub-operations shows Hence all the three objectives of this research were successfully achieved.

6.3 Suggestions for Future Work

Although this study achieved its objectives and many suggestions for future studies have been identified. This section presents suggestions for future works based on the identified limitations.

Digital content is always at risk of being manipulated and misused. Finding new and robust and tamper proof authentication and authorization methods are important for safer and secure Internet. Although, this work experimented based on several real world Cloud content abuse scenarios; especially the social media content which potentially vulnerable to data theft, intellectual property right violation, etc.

The development of an advanced version of the DRM System suitable for Cloud computing would enable researchers to protect online content more effectively, with greater content security. The integrity of online content lacks some features compared to the real adoption and deployment challenges, such as interoperability, internationalization, Internet policy, etc. Further research on these issues would benefit the DRM research community in the future (Xie et al., 2021).

REFERENCES

A High Secure Medical Image Storing and Sharing in Cloud Environment Using Hex Code Cryptography MethodSecure Genius. (2019). *Journal of Medical Imaging and Health Informatics*, *9*(7).

Abe, M., Camenisch, J., Dubovitskaya, M., & Nishimaki, R. (2013). Universally Composable Adaptive Oblivious Transfer (with Access Control) from Standard Assumptions. *Proceedings of the 2013 ACM Workshop on Digital Identity Management*, 1–12. https://doi.org/10.1145/2517881.2517883

Ahmed, I., Khan, A., Ahmed, M., & Rehman, S. ur. (2019). Order preserving secure provenance scheme for distributed networks. *Computers & Security*, *82*, 99–117. https://doi.org/https://doi.org/10.1016/j.cose.2018.12.008

Alsaghier, H. M., Ahamad, S. S., Udgata, S. K., & Reddy, L. S. S. (2017). A Secure and Lightweight Protocol for Mobile DRM Based on DRM Community Cloud (DCC). *Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications, Ficta 2016, Vol 1*, *515*, 475–483. https://doi.org/10.1007/978-981-10-3153-3_47

Anantharaman, P., Palani, K., Nicol, D., & Smith, S. W. (2016). I Am Joe’s Fridge: Scalable Identity in the Internet of Things. *2016 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 129–135. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.47

Anjum, A., Malik, S. ur R., Choo, K.-K. R., Khan, A., Haroon, A., Khan, S., Khan, S. U., Ahmad, N., & Raza, B. (2018). An efficient privacy mechanism for electronic health records. *Computers & Security*, *72*, 196–211. https://doi.org/https://doi.org/10.1016/j.cose.2017.09.014

Antonolpoulos, F., Petrakis, E. G. M., Sotiriadis, S., & Bessis, N. (2018). A physical access control system on the cloud. *Procedia Computer Science, 130,* 318–325. https://doi.org/https://doi.org/10.1016/j.procs.2018.04.045

Arora, S., Varshney, G., Atrey, P. K., & Mishra, M. (2016). SecureCEdit: An approach for secure cloud-based document editing. *2016 IEEE Conference on Communications and Network Security (CNS),* 561–564. https://doi.org/10.1109/CNS.2016.7860548

Awano, H., & Tanabe, K. (2018). The strategy of repeated "open" and "narrow" approaches for standardised media. *International Journal of Technology Management*, *78*(4), 261–279.

Bedi, R. K., Singh, J., & Gupta, S. K. (2018). MWC: an efficient and secure multi-cloud storage approach to leverage augmentation of multi-cloud storage services on mobile devices using fog computing. *The Journal of Supercomputing*. https://doi.org/10.1007/s11227-018-2304-y

Bellini, P., Nesi, P., & Pazzaglia, F. (2014). Exploiting P2P scalability for grant authorization in digital rights management solutions. *Multimedia Tools and Applications*, *72*(2), 1611–1637. https://doi.org/10.1007/s11042-013-1468-y

Bernal Bernabe, J., Marin Perez, J. M., Alcaraz Calero, J. M., Garcia Clemente, F. J., Martinez Perez, G., & Gomez Skarmeta, A. F. (2014). Semantic-aware multi-tenancy authorization system for cloud architectures. *Future Generation Computer*

Systems, 32, 154–167. https://doi.org/https://doi.org/10.1016/j.future.2012.05.011

Birgisson, A., Gibbs Politz, J., Erlingsson, Ú., Taly, A., Vrable, M., & Lentczner, M. (2014). *Macaroons: Cookies with Contextual Caveats for Decentralized Authorization in the Cloud*. https://doi.org/10.14722/ndss.2014.23212

Birrell, E., & Schneider, F. B. (2013). Federated Identity Management Systems: A Privacy-Based Characterization. *Ieee Security & Privacy*, *11*(5), 36–48. https://doi.org/Doi 10.1109/Msp.2013.114

Boucqueau, J. M. (2017). Digital Rights Management. *IEEE Emerging Technology Portal, 2006–201*. https://slidex.tips/download/digital-rights-management-10#

Chadwick, D. W., & Fatema, K. (2012). A privacy preserving authorisation system for the cloud. *Journal of Computer and System Sciences*, *78*(5), 1359–1373. https://doi.org/https://doi.org/10.1016/j.jcss.2011.12.019

Chen, C.-L., Tsaur, W.-J., Chen, Y.-Y., & Chang, Y.-C. (2014). *A Secure Mobile DRM System Based on Cloud Architecture* (Vol. 11). https://doi.org/10.2298/CSIS130919057C

Cheng, Y. Y., Li, H., & Zhang, N. (2016). Character-Based Online Key Management in Cloud Computing Environment. *Proceedings of 2016 Ieee Advanced Information Management, Communicates, Electronic and Automation Control Conference (Imcec 2016)*, 738–741.

Chiang, J. K., Yen, E. H.-W., & Chen, Y.-H. (2013). Authentication, Authorization and File Synchronization in Hybrid Cloud: On Case of Google Docs, Hadoop and Linux Local Hosts. In *Proceedings of the 2013 International Symposium on Biometrics and Security Technologies* (pp. 116–123). IEEE Computer Society.

https://doi.org/10.1109/isbast.2013.22

Chokngamwong, R., & Jirabutr, N. (2015). Mobile Digital Right Management with Enhanced Security using Limited-Use Session Keys. *2015 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (Ecti-Con)*.

Cihal, A. L., Terry, C., Kallie, L., Nicole, M., & Bin, H. (2013). Validation of a novel GaitReminder (TM) Apple iPod application to measure real-time stride data and control music play in a gait rehabilitation program for people with Parkinson’s disease. *Movement Disorders*, *28*, S164–S164.

Cook, A., Robinson, M., Ferrag, M. A., Maglaras, L., He, Y., Jones, K., & Janicke, H. (2017). *Internet of Cloud: Security and Privacy issues*.

Cui, J., Zhou, H., Zhong, H., & Xu, Y. (2018). AKSER: Attribute-based keyword search with efficient revocation in cloud computing. *Information Sciences*, *423*, 343–352. https://doi.org/https://doi.org/10.1016/j.ins.2017.09.029

Das, A. K., Mishra, D., & Mukhopadhyay, S. (2015). An anonymous and secure biometric-based enterprise digital rights management system for mobile environment. *Security and Communication Networks*, *8*(18), 3383–3404. https://doi.org/10.1002/sec.1266

De Angelis, F. L., & Di Marzo Serugendo, G. (2017). SmartContent—Self-Protected Context-Aware Active Documents for Mobile Environments. *Electronics*, *6*(1). https://doi.org/10.3390/electronics6010017

Deng, Z., Li, K., Li, K., & Zhou, J. (2017). A multi-user searchable encryption scheme with keyword authorization in a cloud storage. *Future Generation Computer*

Systems, *72*, 208–218. https://doi.org/https://doi.org/10.1016/j.future.2016.05.017

Doncel, V. R., Delgado, J., Chiariglione, F., Preda, M., & Timmerer, C. (2011). Interoperable digital rights management based on the MPEG Extensible Middleware. *Multimedia Tools and Applications*, *53*(1), 303–318. https://doi.org/10.1007/s11042-010-0513-3

Easley, R., Kim, B. C., & Sun, D. (2012). Optimal Digital Rights Management with Uncertain Piracy. *2012 45th Hawaii International Conference on System Sciences*, 4525–4534. https://doi.org/10.1109/HICSS.2012.460

Esposito, C. (2018). Interoperable, dynamic and privacy-preserving access control for cloud data storage when integrating heterogeneous organizations. *Journal of Network and Computer Applications*, *108*, 124–136. https://doi.org/https://doi.org/10.1016/j.jnca.2018.01.017

Evan Cordell. (2017). *A Python Macaroon Library*. https://github.com/ecordell/pymacaroons

García, R., Gil, R., & Delgado, J. (2007). *A web ontologies framework for digital rights management* (Vol. 15). https://doi.org/10.1007/s10506-007-9032-6

Garg, R., Veerubhotla, R. S., & Saxena, A. (2013). AtDRM: A DRM Architecture with Rights Transfer and Revocation Capability. *Proceedings of the 6th ACM India Computing Convention*, 2:1--2:6. https://doi.org/10.1145/2522548.2522599

Ghiglieri, M., & Waidner, M. (2016). *HbbTV Security and Privacy: Issues and Challenges* (Vol. 14). https://doi.org/10.1109/MSP.2016.54

Gjerdrum, A. T., Johansen, H. D., & Johansen, D. (2016). Implementing Informed

Consent as Information-Flow Policies for Secure Analytics on eHealth Data: Principles and Practices. *2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, 107–112. https://doi.org/10.1109/CHASE.2016.39

H. Gourkhede, M., & Theng, D. (2014). *Analysing Security and Privacy Management for Cloud Computing Environment*. https://doi.org/10.1109/CSNT.2014.142

H. Krawczyk; M. Bellare; R. Canetti. (1997). *HMAC: Keyed-Hashing for Message Authentication Status*. https://doi.org/https://tools.ietf.org/html/rfc2104

Hao, H., & Su, S. (2012). Digital Copyright Protection Scheme Based on JUNA Lightweight Digital Signatures. *2012 Eighth International Conference on Computational Intelligence and Security*, 582–586.

He, H., Li, R., Dong, X., & Zhang, Z. (2014). *Secure, Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud* (Vol. 2). https://doi.org/10.1109/TCC.2014.2378788

Holland, M., Nigischer, C., & Stjepandic, J. (2017). Copyright protection in additive manufacturing with blockchain approach. *Advances in Transdisciplinary Engineering*, *5*, 914–921. https://doi.org/10.3233/978-1-61499-779-5-914

Hou, J. U., Kim, D., Ahn, W. H., & Lee, H. K. (2018). Copyright Protections of Digital Content in the Age of 3D Printer: Emerging Issues and Survey. *Ieee Access*, *6*, 44082–44093. https://doi.org/10.1109/Access.2018.2864331

Hu, P., Dhelim, S., Ning, H., & Qiu, T. (2017). Survey on fog computing: architecture, key technologies, applications and open issues. In *Journal of Network and Computer Applications*. https://doi.org/10.1016/j.jnca.2017.09.002

Hu, P. F., Dhelim, S., Ning, H. S., & Qiu, T. (2017). Survey on fog computing: architecture, key technologies, applications and open issues. *Journal of Network and Computer Applications*, *98*, 27–42. https://doi.org/10.1016/j.jnca.2017.09.002

Huang, J., Lu, P., Juang, W., Fan, C., Lin, Z., & Lin, C. (2014). Secure and efficient digital rights management mechanisms with privacy protection. *Journal of Shanghai Jiaotong University (Science)*, *19*(4), 443–447. https://doi.org/10.1007/s12204-014-1523-5

HUANG, Q., FU, J., MA, Z., YANG, Y., & NIU, X. (2014). Encrypted data sharing with multi-owner based on digital rights management in online social networks. *The Journal of China Universities of Posts and Telecommunications*, *21*(1), 86–93. https://doi.org/10.1016/S1005-8885(14)60273-9

Huang, Q., Ma, Z., Fu, J., Niu, X., & Yang, Y. (2013). *Attribute Based DRM Scheme with Efficient Revocation in Cloud Computing* (Vol. 8). https://doi.org/10.4304/jcp.8.11.2776-2781

Hussain, A., Kiah, M. L. M., Anuar, N. B., Md Noor, R., & Ahmad, M. (2020). Performance and Security Challenges Digital Rights Management (DRM) Approaches Using Fog Computing for Data Provenance: A Survey. *Journal of Medical Imaging and Health Informatics*, *10*(10), 2404–2420. https://doi.org/10.1166/jmihi.2020.3178

Hussain, S. A., Fatima, M., Saeed, A., Raza, I., & Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing. *Applied Computing and Informatics*, *13*(1), 57–65. https://doi.org/https://doi.org/10.1016/j.aci.2016.03.001

Iftikhar, S., Kamran, M., Munir, E. U., & Khan, S. U. (2017). A Reversible Watermarking

Technique for Social Network Data Sets for Enabling Data Trust in Cyber, Physical, and Social Computing. *Ieee Systems Journal*, *11*(1), 197–206. https://doi.org/10.1109/Jsyst.2015.2416131

Iwakiri, M., & Thanh, T. (2012). *Incomplete Cryptography Method Using Invariant Huffman Code Length to Digital Rights Management*. https://doi.org/10.1109/AINA.2012.112

Jiang, M., Ma, Z., Niu, X., & Huang, J. (2016). *A Video Watermarking DRM Method Based on H.264 Compressed Domain with Low Bit-Rate Increasement* (Vol. 25). https://doi.org/10.1049/cje.2016.07.010

Joshi, N., & Petrlic, R. (2013). Towards practical privacy-preserving digital rights management for cloud computing. *2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, 265–270. https://doi.org/10.1109/CCNC.2013.6488456

Keoh, S. L. (2011). Marlin: Toward Seamless Content Sharing and Rights Management. *Ieee Communications Magazine*, *49*(11), 174–180.

Khan, M. F. F., & Sakamura, K. (2017). A tamper-resistant digital token-based rights management system. *2017 International Carnahan Conference on Security Technology (ICCST)*, 1–6. https://doi.org/10.1109/CCST.2017.8167837

Kishigami, J., Fujimura, S., Watanabe, H., Nakadaira, A., & Akutsu, A. (2015). The Blockchain-based Digital Content Distribution System. *Proceedings 2015 Ieee Fifth International Conference on Big Data and Cloud Computing Bdcloud 2015*, 187–190.

Konrad Zemek. (2015). *A C++11 Macaroons library - wrapper for libmacaroons*.

https://github.com/kzemek/libmacaroons-cpp

Koulouzis, S., Mousa, R., Karakannas, A., de Laat, C., & Zhao, Z. (2018). Information Centric Networking for Sharing and Accessing Digital Objects with Persistent Identifiers on Data Infrastructures. *Proceedings of the 18th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 661–668. https://doi.org/10.1109/CCGRID.2018.00098

Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, *33*, 1–48. https://doi.org/10.1016/J.COSREV.2019.05.002

Kwon, G. R., Lama, R. K., Pyun, J. Y., & Park, C. S. (2016). Multimedia digital rights management based on selective encryption for flexible business model. *Multimedia Tools and Applications*, *75*(12), 6697–6715. https://doi.org/10.1007/s11042-015-2563-z

Lankton, N. K., McKnight, D. H., & Tripp, J. F. (2017). Facebook privacy management strategies: A cluster analysis of user privacy behaviors. *Computers in Human Behavior*, *76*, 149–163. https://doi.org/10.1016/J.CHB.2017.07.015

Lee, C. C., Li, C. T., Chen, Z. W., Lai, Y. M., & Shieh, J. C. (2018). An improved E-DRM scheme for mobile environments. *Journal of Information Security and Applications*, *39*, 19–30.

Lee, H., Park, S., Seo, C., & Shin, S. U. (2016a). DRM cloud framework to support heterogeneous digital rights management systems. *Multimedia Tools and Applications*, *75*(22), 14089–14109. https://doi.org/10.1007/s11042-015-2662-x

Lee, H., Park, S., Seo, C., & Shin, S. U. (2016b). *DRM cloud framework to support* *heterogeneous digital rights management systems %J Multimedia Tools Appl. 75*(22), 14089–14109. https://doi.org/10.1007/s11042-015-2662-x

Lin, X.-J., Sun, L., Qu, H., & Zhang, X. (2021). Public key encryption supporting equality test and flexible authorization without bilinear pairings. *Computer Communications*, *170*, 190–199. https://doi.org/https://doi.org/10.1016/j.comcom.2021.02.006

Lin, X.-J., Wang, Q., Sun, L., & Qu, H. (2021). Identity-based encryption with equality test and datestamp-based authorization mechanism. *Theoretical Computer Science*, *861*, 117–132. https://doi.org/https://doi.org/10.1016/j.tcs.2021.02.015

Llewellyn-Jones, D., Merabti, M., Shi, Q., & Askwith, B. (2009). *Trusted Digital Rights Management in Peer-to-Peer Communities*. https://doi.org/10.1109/DeSE.2009.54

Lu, X., Pan, Z., & Xian, H. (2020). An integrity verification scheme of cloud storage for internet-of-things mobile terminal devices. *Computers & Security*, *92*, 101686. https://doi.org/https://doi.org/10.1016/j.cose.2019.101686

Ma, Z. F., Huang, J. Q., Jiang, M., & Niu, X. X. (2016). A Novel Image Digital Rights Management Scheme with High-Level Security, Usage Control and Traceability. *Chinese Journal of Electronics*, *25*(3), 481–494.

Ma, Z. F., Huang, W. H., Bi, W., Gao, H. M., & Wang, Z. (2018). A Master-Slave Blockchain Paradigm and Application in Digital Rights Management. *China Communications*, *15*(8), 174–188.

Ma, Z. F., Jiang, M., Gao, H. M., & Wang, Z. (2018). Blockchain for digital rights management. *Future Generation Computer Systems-the International Journal of Escience*, *89*, 746–764. https://doi.org/10.1016/j.future.2018.07.029

Marques, J., & Serrao, C. (2014). Improving user content privacy on social networks using rights management systems. *Annals of Telecommunications-Annales Des Telecommunications*, *69*(1–2), 37–45. https://doi.org/10.1007/s12243-013-0388-1

Martin W. Kirst. (2019). *Pure Java implementation of Macaroons*. https://github.com/nitram509/jmacaroons

Mickaël. (2014). *A php implementation of Macaroons: Cookies with Contextual Caveats for Decentralized Authorization*. https://github.com/mickaelvieira/macaroons

Millar, A. P., Adeyemi, O., Behrmann, G., Fuhrmann, P., Garonne, V., Litvinsev, D., Mkrtchyan, T., Rossi, A., Sahakyan, M., & Starek, J. (2018). Storage for Advanced Scientific Use-Cases and Beyond. *2018 26th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*, 651–657. https://doi.org/10.1109/PDP2018.2018.00109

Mtech, R. K. (2015). *The Non-Tangible Masking of Confidential Information using Video Steganography*.

Munier, M., Lalanne, V., & Ricarde, M. (2012). Self-Protecting Documents for Cloud Storage Security. *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, 1231–1238. https://doi.org/10.1109/TrustCom.2012.261

Networks, I. (2014). *PHP implementation of Macaroons*. https://github.com/immense/php-macaroons

NIST. (2020). https://www.nist.gov

Nuñez, D., Agudo, I., & Lopez, J. (2017). Proxy Re-Encryption: Analysis of constructions and its application to secure access delegation. *Journal of Network and Computer Applications, 87*, 193–209. https://doi.org/10.1016/J.JNCA.2017.03.005

Pareek, G., & Purushothama, B. R. (2020). Proxy re-encryption for fine-grained access control: Its applicability, security under stronger notions and performance. *Journal of Information Security and Applications, 54*, 102543. https://doi.org/https://doi.org/10.1016/j.jisa.2020.102543

Parmar, P., & Bhavsar, M. (2020). Achieving Trust using RoT in IaaS Cloud. *Procedia Computer Science, 167*, 487–495. https://doi.org/https://doi.org/10.1016/j.procs.2020.03.264

Patranabis, S., Shrivastava, Y., & Mukhopadhyay, D. (2017). Provably Secure Key-Aggregate Cryptosystems with Broadcast Aggregate Keys for Online Data Sharing on the Cloud. *Ieee Transactions on Computers, 66*(5), 891–904. https://doi.org/10.1109/Tc.2016.2629510

Petrlic, R., & Sorge, C. (2014). *Privacy-Preserving Digital Rights Management based on Attribute-based Encryption*. https://doi.org/10.1109/NTMS.2014.6814044

Puliafito, C., Mingozzi, E., Longo, F., Puliafito, A., & Rana, O. (2019). Fog Computing for the Internet of Things: A Survey. *ACM Trans. Internet Technol.*, *19*(2), 18:1--18:41. https://doi.org/10.1145/3301443

Qinlong, H., Zhaofeng, M., Yixian, Y., Xinxin, N., & Jingyi, F. %J C. C. (2014). *Attribute based DRM scheme with dynamic usage control in cloud computing*. *11*, 50–63.

Rana, S., & Sur, A. (2016). Depth-Based View-Invariant Blind 3D Image Watermarking. *Acm Transactions on Multimedia Computing Communications and Applications, 12*(4). https://doi.org/Artn 4810.1145/2957751

Roček, A., Slavíček, K., Dostál, O., & Javorník, M. (2016). A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters. *Biomedical Signal Processing and Control*, *29*, 44–52. https://doi.org/https://doi.org/10.1016/j.bspc.2016.05.005

Rodriguez, E., Rodríguez-Doncel, V., Carreras, A., & Delgado, J. (2009). *A Digital Rights Management approach to privacy in online social networks*.

Roger Peppe. (2018). *Javascript implementation of macaroons*. https://github.com/go-macaroon/js-macaroon

Sachan, A., Emmanuel, S., & Kankanhalli, M. S. (2012). Aggregate Licenses Validation for Digital Rights Violation Detection. *ACM Trans. Multimedia Comput. Commun. Appl.*, *8*(2S), 37:1--37:21. https://doi.org/10.1145/2344436.2344443

Salim, F., Sheppard, N., & Safavi-Naini, R. (2010). *A Rights Management Approach to Securing Data Distribution in Coalitions*. https://doi.org/10.1109/NSS.2010.94

Salman, O., Elhajj, I., Chehab, A., & Kayssi, A. (2018). IoT survey: An SDN and fog computing perspective. *Computer Networks*, *143*, 221–246. https://doi.org/10.1016/j.comnet.2018.07.020

Savelyev, A. (2018). Copyright in the blockchain era: Promises and challenges. *Computer Law & Security Review*, *34*(3), 550–561.

Serrao, C., Marques, J., Dias, M., & Delgado, J. (2018). *OPEN-SOURCE SOFTWARE AS A DRIVER FOR DIGITAL CONTENT E-COMMERCE AND DRM INTEROPERABILITY*.

Serrao, C., Neves, D., Barker, T., Balestri, M., & Kudumakis, P. (2003). *OpenSDRM -*

An open and secure digital rights management solution.

Sharma, V., Kim, J., Kwon, S., You, I., & Leu, F.-Y. (2018). An Overview of 802.21a-2012 and Its Incorporation into IoT-Fog Networks Using Osmotic Framework. In Y.-B. Lin, D.-J. Deng, I. You, & C.-C. Lin (Eds.), *IoT as a Service* (pp. 64–72). Springer International Publishing.

Shen, W., Yu, J., Xia, H., Zhang, H., Lu, X., & Hao, R. (2017). Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium. *Journal of Network and Computer Applications*, *82*, 56–64. https://doi.org/https://doi.org/10.1016/j.jnca.2017.01.015

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/J.COMNET.2014.11.008

Singh, A. K., Nag, A., Karforma, S., & Mukhopadhyay, S. (2019). Implementation of multi-agent based Digital Rights Management System for Distance Education (DRMSDE) using JADE. *International Journal of Advanced Computer Science and Applications*, *10*(3), 343–352. https://doi.org/10.14569/IJACSA.2019.0100345

Sriborrirux, W., Promsiri, P., & Limmanee, A. (2014). Multiple Secret Key Sharing based on the Network Coding Technique for an Open Cloud DRM Service Provider. *2014 IEEE 17th International Conference on Computational Science and Engineering (CSE)*, 953–959. https://doi.org/10.1109/Cse.2014.191

Subramanyam, A. V, Emmanuel, S., & Kankanhalli, M. S. (2012). Robust Watermarking of Compressed and Encrypted JPEG2000 Images. *IEEE Transactions on Multimedia*, *14*(3), 703–716. https://doi.org/10.1109/TMM.2011.2181342

Sultan, N. H., Barbhuiya, F. A., & Laurent, M. (2018). ICAuth: A secure and scalable owner delegated inter-cloud authorization. *Future Generation Computer Systems*, *88*, 319–332. https://doi.org/https://doi.org/10.1016/j.future.2018.05.066

Sun, L., Xu, C., Li, C., & Li, Y. (2020). Server-aided searchable encryption in multi-user setting. *Computer Communications*, *164*, 25–30. https://doi.org/https://doi.org/10.1016/j.comcom.2020.09.018

Suomalainen, J. (2019). *Defense-in-Depth Methods in Microservices Access Control*. https://trepo.tuni.fi/handle/123456789/27172

Tapas, N., Longo, F., Merlino, G., & Puliafito, A. (2020). Experimenting with smart contracts for access control and delegation in IoT. *Future Generation Computer Systems*, *111*, 324–338. https://doi.org/https://doi.org/10.1016/j.future.2020.04.020

Thanh, T. M., & Iwakiri, M. (2016). Fragile watermarking with permutation code for content-leakage in digital rights management system. *Multimedia Systems*, *22*(5), 603–615. https://doi.org/10.1007/s00530-015-0472-7

Torres, V., Serrao, C., Dias, M. S., & Delgado, J. (2008). Open DRM and the future of media. *Ieee Multimedia*, *15*(2), 28–36.

Verma, G. K., & Singh, B. B. (2018). Efficient identity-based blind message recovery signature scheme from pairings. *Iet Information Security*, *12*(2), 150–156. https://doi.org/10.1049/iet-ifs.2017.0342

Voundi Koe, A. S., & Lin, Y. (2019). Offline privacy preserving proxy re-encryption in mobile cloud computing. *Pervasive and Mobile Computing*, *59*, 101081. https://doi.org/https://doi.org/10.1016/j.pmcj.2019.101081

Wang, D., Gao, J., Yu, H., Li, X., Li, F., Takagi, T., Xu, C., & Zhang, X. (2018). *A Novel Digital Rights Management in P2P Networks Based on Bitcoin System*. 227–240.

Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2011). Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. *IEEE Transactions on Parallel and Distributed Systems*, *22*(5), 847–859. https://doi.org/10.1109/TPDS.2010.183

Win, L. L., Thomas, T., & Emmanuel, S. (2012). Privacy Enabled Digital Rights Management Without Trusted Third Party Assumption. *IEEE Trans. Multimedia*, *14*(3–1), 546–554. https://doi.org/10.1109/TMM.2012.2189983

Wood, C. A., & Uzun, E. (2014). Flexible End-to-End Content Security in CCN. *2014 Ieee 11th Consumer Communications and Networking Conference (Ccnc)*.

Xie, M., Ruan, Y., Hong, H., & Shao, J. (2021). A CP-ABE scheme based on multi-authority in hybrid clouds for mobile devices. *Future Generation Computer Systems*, *121*, 114–122. https://doi.org/https://doi.org/10.1016/j.future.2021.03.021

Xu, R. Z., Zhang, L., Zhao, H. W., & Peng, Y. (2017). Design of Network Media's Digital Rights Management Scheme Based on Blockchain Technology. *2017 Ieee 13th International Symposium on Autonomous Decentralized Systems (Isads 2017)*, 128–133. https://doi.org/10.1109/Isads.2017.21

Yang, A., Xu, J., Weng, J., Zhou, J., & Wong, D. S. (2021). Lightweight and Privacy-Preserving Delegatable Proofs of Storage with Data Dynamics in Cloud Storage. *IEEE Transactions on Cloud Computing*, *9*(1), 212–225. https://doi.org/10.1109/TCC.2018.2851256

Yang, H.-W., Yang, C.-C., & Lin, W. (2013). *Enhanced digital rights management* *authentication scheme based on smart card* (Vol. 7). https://doi.org/10.1049/iet-ifs.2012.0191

Yao, X., Kong, H., Liu, H., Qiu, T., & Ning, H. (2019). An Attribute Credential Based Public Key Scheme for Fog Computing in Digital Manufacturing. *IEEE Transactions on Industrial Informatics*, *15*(4), 2297–2307. https://doi.org/10.1109/TII.2019.2891079

Zafar, F., Khan, A., Malik, S. U. R., Ahmed, M., Anjum, A., Khan, M. I., Javed, N., Alam, M., & Jamil, F. (2017). A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends. *Computers and Security*, *65*, 29–49. https://doi.org/10.1016/j.cose.2016.10.006

Zafar, F., Khan, A., Suhail, S., Ahmed, I., Hameed, K., Khan, H. M., Jabeen, F., & Anjum, A. (2017). Trustworthy data: A survey, taxonomy and future trends of secure provenance schemes. *Journal of Network and Computer Applications*, *94*, 50–68. https://doi.org/10.1016/J.JNCA.2017.06.003

Zhang, Y., Xu, C., Liang, X., Li, H., Mu, Y., & Zhang, X. (2017). Efficient Public Verification of Data Integrity for Cloud Storage Systems from Indistinguishability Obfuscation. *IEEE Transactions on Information Forensics and Security*, *12*(3), 676–688. https://doi.org/10.1109/TIFS.2016.2631951

Zhang, Z. Y., Wang, Z., & Niu, D. M. (2015). A novel approach to rights sharing-enabling digital rights management for mobile multimedia. *Multimedia Tools and Applications*, *74*(16), 6255–6271. https://doi.org/10.1007/s11042-014-2135-7

Zhaofeng, M., Weihua, H., & Hongmin, G. (2018). A new blockchain-based trusted DRM scheme for built-in content protection. *Eurasip Journal on Image and Video*

Processing, *2018*(1). https://doi.org/10.1186/s13640-018-0327-1

Zou, P., Wang, C., Liu, Z., & Bao, D. (2010). Phosphor: A Cloud Based DRM Scheme with Sim Card. *2010 12th International Asia-Pacific Web Conference*, 459–463. https://doi.org/10.1109/APWeb.2010.43