

Blockchain Based Multimedia Content Protection Using Encryption in DRM (Digital Rights Management)

Ms. Shweta Sanjay Patil¹, Mrs. Pooja Sachin Dandge²

^{1,2}Assistant Professor, Changu Kana Thakur Arts Commerce and Science College, New Panvel (Autonomous), Maharashtra 410206, India

Abstract - A blockchain technology is being used in the multimedia content protection. There has been a rapid increasing incident related to multimedia copyrights in past few years. The number of successfully developed blockchain based systems are very less. In this project we have implemented Encryption using Digital Rights Management in blockchain technology . Blockchain Technology is used to store plain and cipher summary information of original and DRM protected digital content such as image, audio and video. It creates hash ID of the content. This project reveals blockchain based copyright protection applications. we propose a system in which we have implemented the blockchain based multimedia content protection systems for digital rights management, which supports the right content serves the right users in a right way, the DRMChain can provide trusted and high-level credible content protection. we proposed efficient and secure authentication for multimedia content.

Index Terms - blockchain; DRM; DRMChain; Encryption.

1. INTRODUCTION

Traditionally multimedia content was distributed through physical exchange of papers, compact disks or DVD's and no security is provided. Blockchain is the technology in which it is impossible to change the owners multimedia content. The blockchain based copyright protection application allow copyright owners to interact without costly intermediaries. These applications allow the content owners to upload copyrighted content, manage distribution, trace sources of piracy, and receive payments upon content usage. The success of such applications is however dependent on different factors related to the blockchain technology The blockchain technology is suffering from high latency, low throughput, high transaction cost, high energy and high computational power consumption. In this paper, we mainly focus on

removing or improving all these issues from the original blockchain system to make it suitable for our digital rights management system. This system allows only authorized user to use online contents and provide original multimedia contents. The DRM also take care of digital contents and keep track records of required content modification, copyright transfer or other transaction trails related to multimedia data. We Proposed a taxonomy that helps in encryption using DRM and copyright of multimedia content.

2. LITERATURE SURVEY

Blockchain technology has been studied by variety of researchers. Dhillon wrote an article (Dhillon, 2016) and with others a book section (Dhillon et al., 2017) about blockchain technology and open science. (Almenberg et al., 2009; Dreber et al., 2015; Dhillon et al., 2017). To create an incentive to participate, users get rewarded for the right prediction. Bartling manages an open living document about the usage of the BT for open science that contains many promising ideas, projects, and hypothesis (Bartling, 2018). In that sense, Chen et al. (2018) propose an architecture for blockchain based provenance sharing of scientific workflows to provide a secure and easy way for scientists to share their research data, for instance, to prevent the waste of resources. van Rossum (2017, 2018) also identifies blockchain as a technology that can foster especially open science in many aspects hence corresponding to most of the statements by Dhillon, Bartling, and Rachovitsa. Further literature and a web article by Bell et al. (2017), Brock (2018), and Opoku-Agyemang (2017) likewise describe the many possibilities of blockchain technology to improve science and all kind of research activities as statistical analyses, data evaluations, and medical trials. de La Rosa et al.

(2017) analyzed how blockchain-based protection of intellectual property in open innovation processes can work, such an approach is also critical for scientific environments. (Smith, 2006; Tennant et al., 2017). Most of the time, peer-review is a blackbox process and malicious behavior is difficult to detect. In a multi-disciplinary study of Tennant et al. (2017) about innovations in peer-review, they identified the blockchain technology as a potential future model with promising possibilities. Tenorio-Fornés et al. (2019) criticize the oligopolistic position of the publishers in academia regarding policies, embargo periods, and restrictions about the dissemination of data Janowicz et al. (2018) wrote a paper about blockchain-based open science and publishing.

In recent years, the blockchain technology is used in various applications such as finance, health care, supply chain management and intrusion detection system. Now it is observed in the copyright protection system. The main fundamental attributes are security, hash id, transparency, reliable database, digital cryptocurrency for protecting digital content. Currently rapid development in blockchain technology is observed but combination of blockchain technology and Digital Right Management using encryption has not given more attention by researchers in the literature. So recently we investigated the use of blockchain technology in multimedia applications such as images, audio and videos. Though this research we have analyzed that how multimedia data should be protected and copyright infringement related problem can be solved using blockchain technology.

3. OBJECTIVE

- To maintain high security when transferring the multimedia data.
- To encrypt the multimedia data.
- To protect the copyrights of electronic media.
- To allow digital information to be recorded and distributed but not editable.
- To secure encrypted data using blockchain in digital rights management.

4. METHODOLOGY

The proposed system in which publishers, authors and other content creators use an application that encrypts

multimedia data. Only authorized user allows access to multimedia content. The core technologies used by DRM which include encryption. Encryption technologies are used to control who has access to the content and how it is being used. DRM is to ensure that the digital rights of the copyright holders are not violated. DRM systems have been proposed to support encryption of data. First admin upload the video in global environment after that file has been encrypted using secure hash algorithm that is designed using Hypertext Preprocessor (PHP) programming and which is applied on multimedia content. After this process unique hash ID is generated and content is being secured and protected.

4.1. Multimedia Encryption

The process of encoding plaintext messages into ciphertext messages is called encryption, and the reverse process of transforming ciphertext back to plaintext is called decryption. This technique is expected to provide one or more of the following properties:

- Confidentiality: It refers to limiting data access or disclosure to authorized users and preventing access or disclosure to unauthorized ones.
- Integrity: It refers to protection of data or modification of data.
- Authenticity: It refers to enabling the receiver of data to ascertain its origin. In this research approach, the entire multimedia content is encrypted using standard Secure Hash Algorithm (SHA-1).
- PHP: PHP is hypertext preprocessor. It is server scripting language and powerful tool for making dynamic and interactive web pages. PHP code executed on server and result is returned to the browser as plain html. In this project we have implemented encryption using PHP language in blockchain technology.

4.2. Digital Rights Management(DRM)

DRM have been implemented to provide the secure delivery of digital content. DRM provides the secure protecting content. It is designed for following requirements:

- Unauthorized copying: It prevent unauthorized usage that is achieved by encryption.

- Secure distribution: It distribute content securely with authorized user.
- Conditional access: It provide access license specified by the owners.

4.3. Algorithm

In this research we have implemented sha1() algorithm that calculates the SHA-1 hash of a string. The sha1() function uses the Secure Hash Algorithm 1. SHA-1 produces a 160-bit output called a message digest. for example, be input to a signature algorithm which generates or verifies the signature for the message. using the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature.

5. RESULT & DISCUSSION

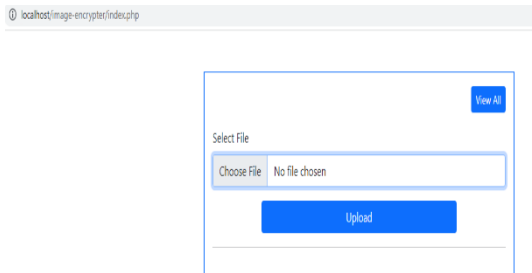


Fig.5.1

The Fig.5.1 shows that blockchain based system have to select the multimedia file (i.e. Images, Audio, Video, Files) from computer library and upload it.

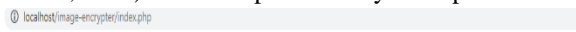


Fig.5.2

Fig.5.2 shows that any multimedia file is selected for encryption using blockchain technology

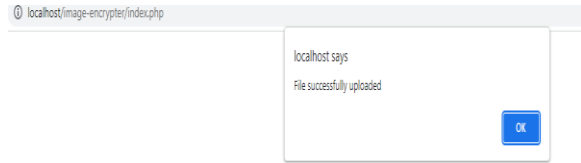


Fig.5.3

Fig.5.3 shows that the file has been successfully uploaded in the blockchain based system and Unique hash ID generated that will secure the file content and only authorized person can access the multimedia content.

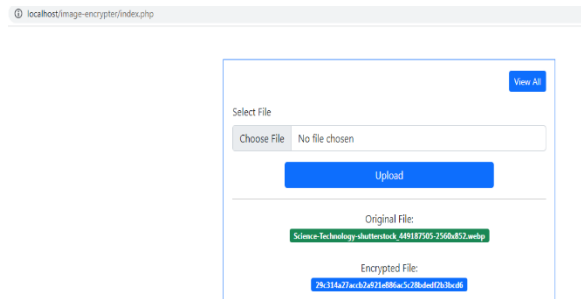


Fig.5.4

Fig.5.4 shows that encryption is done though SHA-1 Algorithm. It shows original as well as encrypted file.

S.No	Real File	Encrypted File	File
1	VID-20140419-WA0012.mp4	00a9b555db9fa9b363cc83a9711801cb7db5ee	
2	VID-20140415-WA0002.mp4	84c46036534b28e5e43788134fca48ca21d85c	
3	VID-20140614-WA0007.mp4	940846599bab613737a4071020a3deec5e8004	
4	FB_IMG_14989209826343788.jpg	c78ba0e6e4d40d3064c394112115129a7f95a93	
5	FB_IMG_1499591663254242.jpg	6a8a73878d9980a716232c7790c222c5bca79a	
6	VID-20170119-WA0038.mp4	3a671a32c50eac5d71126d3143d8182ee744208c	
7	png-transparent-free-download-icon-down-computer-system-blue-...	54b1323a8f910D5e58e8a51dd0c08095db	

Fig.5.5

Fig.5.5 shows that the secure hash encrypted key is generated and protection is given to original multimedia content.

6.CONCLUSION

The conclusion of our study shows that encryption of multimedia content(such as audio, video, images, files) using SHA-1 algorithm in blockchain technology has been successfully implemented. Also this system helps the use of technologies to restrict the limit of copyright and provide protection to multimedia content.

ACKNOWLEDGMENT

1. Consumable and chemicals: Nil
 2. Equipment: Nil
 3. Contingency and local travel:
 - a. Books and Journals 1800
 - b. Stationary, Xerox charges 3600
 - c. Minor repairs etc: Nil
 - d. Travel 3600
 - e. Miscellaneous 9000
- Total: - 18000

REFERENCE

- [1] Ruffing, T.; Moreno-Sanchez, P.; Kate, A. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In Computer Security—ESORICS 2014; Kutyłowski, M., Vaidya, J., Eds.; Springer International Publishing: Berlin/Heidelberg, Germany, 2014; pp. 345–364.
- [2] Valley, S. Netflix. 2007. Available online: <http://www.netflix.com/> (accessed on 21 December 2020). 2. Cohen, B. BitTorrent. 2005. Available online: <https://www.utorrent.com/> (accessed on 21 December 2020)
- [3] M. Nehe and S. A. Jain, "A Survey on Data Security using Blockchain: Merits, Demerits and Applications," 2019 International Conference on Recent Advances in Energy efficient Computing and Communication (ICRAECC), pp.1-5, 2019

AUTHORS PROFILE:



Ms. Shweta Sanjay Patil
MSc in Information technology
Assistant Professor in department of
information technology, Changu
Kana Thakur College New Panvel
(Autonomous)



Mrs. Pooja Sachin Dandge
Master in computer application
(MCA)
Assistant Professor in department of
information technology, Changu
Kana Thakur College New Panvel
(Autonomous)