Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 05, May-2021

Visual Cryptography with Cloud Computing for Personal Security of the User

Dr. Deepak Sharma
HOD, computer engineering department
K. J. Somaiya college of engineering
Mumbai, India

Harita Kundalia
Department of computer engineering
K. J. Somaiya college of engineering
Mumbai, India

***Abstract*— Cloud computing with blockchain is the growing technology of today. This project uses blockchain technology along with cloud computing. IPFS is a cloud service, it is a convention and shared organization for putting away and sharing information during a circulated recording framework. Blockchain utilizes computerized signature (SHA 256) calculation to keep up/confirm respectability of the information. Security is essential and curial for cloud computing and blockchain. The security is provided by using MD 5encryption and visual cryptography. Visual cryptography (VC) is an encryption procedure on pictures (or text) during which decoding is finished by human tactile framework. during this strategy, an image is scrambled into number of pieces (known as offers). At the point when the printed shares are superimposed together, the picture are regularly decoded with human vision. In visual cryptography a seed is divided into shares which is distributed between a user and stored in blockchain. When all the shares overlap seed image or also known as secret image is revealed to the user. This report gives exhaustive comparative study of visual cryptography technique based on cloud computing and MD5 algorithm. It also presents similarities between the systems, differences in approaches used in the systems, algorithms used and pros and cons of each technology.**

Keywords*— *Cloud computing, Blockchain, visual cryptography, MD5 algorithm, secret images, shares

I. INTRODUCTION

Cloud computing with blockchain is the growing technology of today. This project uses blockchain technology along with cloud computing. IPFS is a cloud service, it is a convention and shared organization for putting away and sharing information during a circulated recording framework. Blockchain utilizes computerized signature (SHA 256) calculation to keep up/confirm respectability of the information. Blockchain uses digital signature (SHA 256) algorithm to maintain/verify integrity of the data. This report gives exhaustive comparative study of visual cryptography technique based on cloud computing and MD5 algorithm. It also presents similarities between the systems, differences in approaches used in the systems, algorithms used and pros and cons of each technology. Objectives: Implementing visual cryptography for user data protection. To provide higher security for data protection with MD 5. To avoid data leaks and dictionary attacks. Create a blockchain to communicate with cloud using IPFS.

The foremost step involved in implementation of project is to define the problem that we are looking at possible solutions to that. It is mandatory to chalk down a problem statement for the project and define it, so that it is easier to analyze further steps involved. Problem

statement for this project is: Security in cloud computing is very important. Blockchain provides some security to the system when used with cloud but still the security can be breached. In this project blockchain and cloud are used as storage solution which provides security for users. Security algorithms like MD 5 and visual cryptography are used to achieve a secure hash value which is created with seed that has username and password, from which shares are created and stored over blockchain and cloud. IPFS server is used for providing storage solution for this project.

II. LITERATURE SURVEY

Visual cryptography might be a cryptographic method which permits visual data (pictures, text, and so on) to be encoded in such how that the unscrambling is regularly performed by people (without PCs). The principal visual cryptographic method was created by MoniNaor and Adi Shamir in 1994. It included separating the picture into n partakes all together that solitary somebody with all n offers could decode the picture by overlaying every one of the offers more than each other. For all intents and purposes, this will be finished by printing each offer on a different straightforwardness and afterward putting the entirety of the transparencies on top of one another. In their strategy n-1 offers uncovers no data about the main picture. [8]

1:(2, 2) – Threshold VCS: this is frequently a least complex edge plot that takes a mysterious picture and scrambles it into two distinct offers that uncover the mysterious picture whenever they are overlaid. No extra data is needed to make this sort of access structure. 2 :(2, n) – Threshold VCS: This plan scrambles the mysterious picture into n offers such when any (at least two) of the offers are overlaid the key picture is uncovered. The client will be provoked for n, the measure of members. 3 :(n, n) – Threshold VCS: This plan encodes the mysterious picture into n offers such just the entirety of the offers is joined will the key picture be uncovered. The client will be incited for n, the measure of members. 4:(k, n) – Threshold VCS: This plan encodes the mysterious picture into n offers such when any gathering of at any rate k offers are overlaid the key picture will be uncovered. The client will be incited fork, the limit, and n, the measure of members. The fundamental motivation behind a visual cryptography is security and in this way the utilization of a visual cryptography conspire is to separate the machine and human. The

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 05, May-2021

interpreting of the visual cryptography encoded picture must be fixed by an individual and not by PC. A typical flowchart of visual cryptography scheme is shown in Fig.2.1. A secret image to be hidden are going to be divided into n binary share using VCS, on stacking these qualified shares will give the first recovered image.

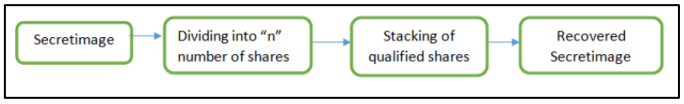

Fig 2.1: flowchart of visual cryptography

Visual cryptography scheme is often performed by Boolean functions like OR, XOR and NOT. The performance of the VCS is assessed using two parameters namely, the pixel expansion and therefore the contrast. Smaller the pixel expansion better the standard of the VCS. to elucidate the principle of VC, consider a (2, 2) VCS. The probability of getting a white (black) pixel is equal, that's fifty percentage probability. Construction of a 2-out-of-2 scheme (2, 2) shown in Fig. 2.2. An example of (2, 2) VCS is shown in Fig. 2.3, secret image (SI) to be encoded is shown. Every pixel of the SI is split into two sub-pixels in each of the 2 shares.

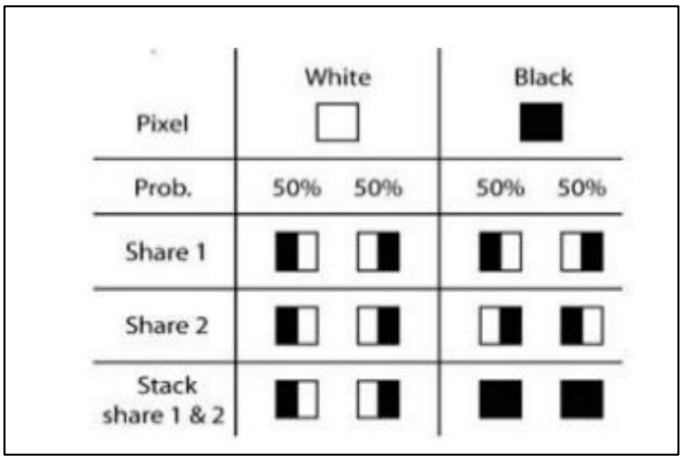

Fig 2.2: example of (2,2) shares

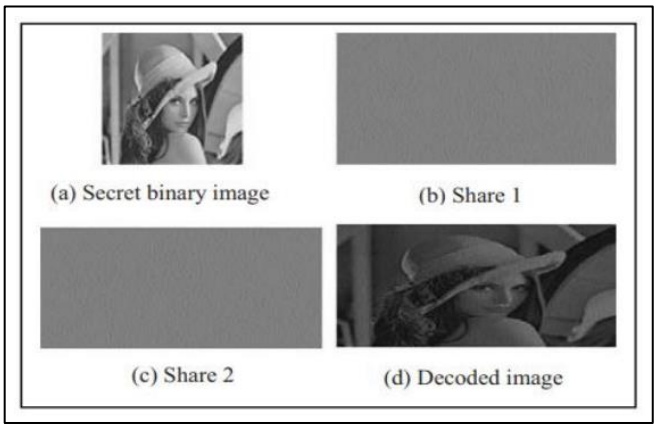

Fig 2.3: visual cryptography scheme

Binary picture type Xiao-qing Tan utilized one secret picture having one pixel development. Feng Lin et.al actualized one mystery picture however had a pixel extension of six. Thomas Monoth et.al and Shouchao Song et.al likewise utilized one mystery picture yet pixel development m was client characterized. Tzung – Her Chen et.a likewise had one mystery picture yet pixel extension was client characterized as m more prominent than or equivalent to two. WenPinn Fang and TsungLich-Lin et.al utilized two mystery picture though Zhengxin Fu et.al utilized 4 pictures having pixel extension of one, four, and nine individually. N secret pictures was utilized by plans created by Jonathan Weir et.al having a pixel extension of four and characterized m+1. In dim scale picture type Zhongmin Wang et.al conspire utilized two secret picture and had four pixel extension. In shading plan picture type Wei-Qiao et.al utilized single secret picture having m characterized pixel development. Joes J Tharayil utilized two secret picture having a pixel development of two. In Binary picture type F.Lin built up a plan with single secret picture, having m client characterized pixel development. In Gray scale picture type Feng Liu et.al and Arun Ross et.al having one and three offers individually had a pixel extension of nine and m characterized pixel extension. In Color picture type Jenila Vincent M et.al shared two secret pictures having a pixel extension of n and Inkoo Kang et.al had four mystery pictures having a pixel extension of six .YoungChangHou et.al actualized a plan in which fourteen secret pictures of twofold or dark scale or shading are utilized giving a pixel extension of n.

III. ARCHITECTURE

The proposed system will be using technologies namely, blockchain, cloud computing, visual cryptography, and MD 5 algorithm for security. The flow of encryption of data is as follows, firstly user will register and then use those credentials while login. When user registers for the 1st time, it makes a folder with the username and creates share 1 out of the seed that is username and password. A seed image is the image from which shares will further be created. When share 1 is made it is stored on the blockchain using hash function and for encryption of the data. For the share 2, user has to login, when the user completes 1st login share 2 is created and along with it an overlay image is also created for the system to verify the image later. Encryption of seed image is done using MD 5 algorithm, which uses hash function for encryption of data. Once MD 5 algorithm is applied, data moves forward, and shares are made. IPFS server is responsible for storing the shares over blockchain and user's system. Since the proposed system uses 2 hash functions, the shares generated are also in hash values. OCR is used to detect 1st 10 characters of the hash value to overlap and match the shares. The overlap shares produce an image in which the hash function is visible. In visual cryptography binary color image type is used.

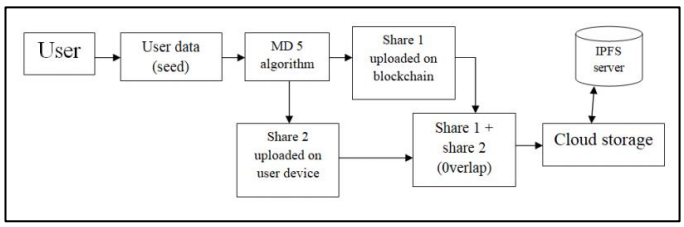

Fig 3.1: flowchart for visual cryptography

The architectural design of a system emphasizes the design of the system architecture that describes the structure, behaviour and more views of that system and analysis. The architectural

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 05, May-2021

model defines the data set that we are going to be taking for the purpose of analysis. The methodology which is going to be followed by the various components like the dataset, the algorithm, the final visualization and the sequence in which they will follow each other have been clearly depicted in the Figure.

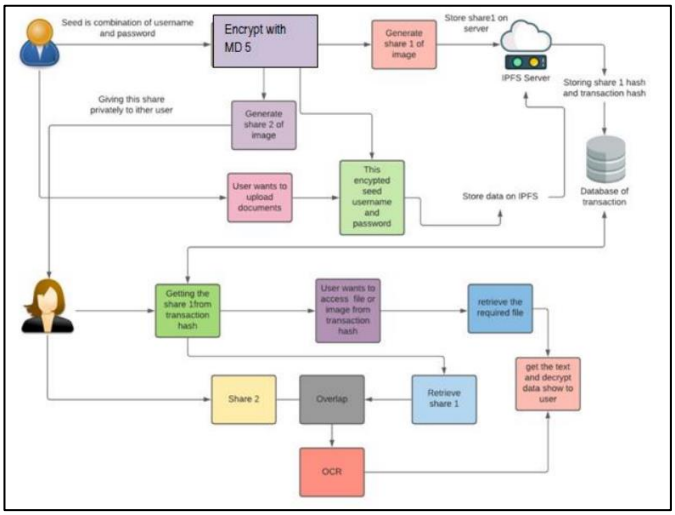

Fig 3.2: Architecture

IV. RESULTS AND CONCLUSION

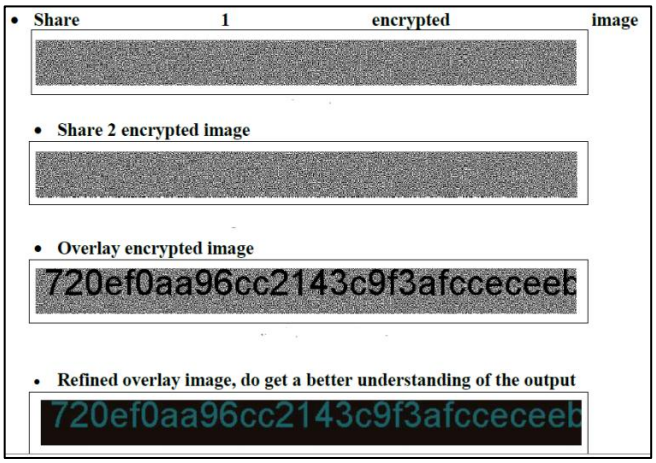

Fig 4.1: results

1) Conclusions

In this system, we have presented a way to analyse information which is obtained from extraction of real time data. This proposed system will help user to have higher security while using cloud computing. Our recommender system enable users to have blockchain and cloud computing technologies with new look of security while authentication and storage. Security algorithms like MD 5 and Visual cryptography are implements together to achieve security goals for the system. goals. It is an integrated approach towards blockchain, cloud computing and security goals. One can make cloud and blockchain storage choices satisfying their data security while authentication as well as storage security. Lastly, we hope that this kind of system could contribute to the evolution of blockchain based on cloud computing and security provided for the same.

ACKNOWLEDGMENT

I would like to thank my mentor Dr. Deepak Sharma. through his guidance and vigilance, I've accomplished this, thank you sir.

REFERENCES

[1] AkshayArora,Abhirup Khanna, Anmol Rastogi, Amit Agarwal (2017), "Cloud Security Ecosystem for Data Security and Privacy", IEEE.
[2] Weiwei Kong, Yang Lei, Jing Ma (2017),"Data Security and Privacy Information Challenges in Cloud Computing", International Conference on Intelligent Networking and Collaborative Systems, IEEE.
[3] Hongbing Cheng, ChunmingRong, ManyunQian, and Weihong Wang (2018), "Accountable Privacy-Preserving Mechanism For Cloud Computing Based On Identity-Based Encryption", IEEE
[4] https://en.wikipedia.org/wiki/Blockchain
[5] Stephen S Kirkman,(2018) A Data Movement Policy Framework for Improving Trust in the Cloud Using Smart Contracts and Blockchains, IEEE International Conference on Cloud Engineering.
[6] SambitNayak, Nanjangud C Narendra, Anshu ,JamesKempf (2018), IEEE 11th International Conference on Cloud Computing, Saranyu: Using Smart Contracts and Blockchain for Cloud Tenant Management.
[7] QiwuZou, Yuzhe Tang, Ju Chen, Kai Li, Charles A. Kamhoua, Kevin Kwiat, Laurent Njilla, (2018),IEEE 11th International Conference on Cloud Computing ,ChainFS: Blockchain-Secured Cloud Storage.
[8] Thomas Monoth and BabuAnto P, "Tamperproof Transmission of Fingerprints Using Visual Cryptography Schemes," Procedia Computer Science, vol. 2, pp. 143-148, 2010.
[9] M. T. de Oliveira et al., "Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICC.2019.8761307.
[10] B. L. Radhakrishnan, A. S. Joseph and S. Sudhakar, "Securing Blockchain based Electronic Health Record using Multilevel Authentication," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 699- 703, doi: 10.1109/ICACCS.2019.8728483.
[11] S. A. Thomas and S. Gharge, "Review on Various Visual Cryptography Schemes," 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), Mysore, 2017, pp. 1164-1167, doi: 10.1109/CTCEEC.2017.8455136.27.
[12] S. Pavithra, S. Ramya and S. Prathibha, "A Survey On Cloud Security Issues And Blockchain," 2019 3rd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 2019, pp. 136-140, doi: 10.1109/ICCCT2.2019.8824891.
[13] Ashutosh and S. D. Sen, "Visual Cryptography," 2008 International Conference on Advanced Computer Theory and Engineering, Phuket, 2008, pp. 805-807, doi: 0.1109/ICACTE.2008.184.
[14] D. Jena and S. K. Jena, "A Novel Visual Cryptography Scheme," 2009 International Conference on Advanced Computer Control, Singapore, 2009, pp. 207-211, doi: 10.1109/ICACC.2009.109.
[15] W. Tsai, T. Chou, J. Chen, Y. Ma and C. Huang, "Blockchain as a Platform for Secure Cloud Computing Services," 2020 22nd International Conference on Advanced Communication Technology (ICACT), Phoenix Park, PyeongChang,, Korea (South), 2020, pp. 155-158, doi: 10.23919/ICACT48636.2020.9061435.