International Journal of Future Generation Communication and Networking
Vol. 13, No.3, (2020), pp. 2284–2289

Detection of Tampered Video Using Blockchain

Dr. K.S. Wagh[1], Hitesh Bhonkar[2], Ashish Amlani[3], Nitesh Bhatt[4], [5]Aarti Dike

AISSMS IOIT, SPPU, Pune

[1]waghks@gmail.com, [2]hitesh.bhonkar98@gmail.com,[3]aamlani007@gmail.com, [4]nitsfb21@gmail.com, [5]aartidike213@gmail.com

Abstract

Block-chain is a database where the data is stored in a network. This ensures high security and avoidance of tampering of data. Thus, each and every data in the block-chain is in stored continuously and one can immediately detect any change at any point if tampered. Thus, Block-chain helps in maintaining growing records and saving them in an efficient database system.

Keyword*: IOT, Data encryption, Block chain, Certificate-less cryptography.*

1. Introduction

A blockchain is a form of database where various data records are stored in the form of list. It acts on a distributed level and consists of various blocks where each block holds specific data and the execution within it. Thus, blockchain helps in forming a network chain wherein the network, each data is stored continuously and every execution result and the transaction is visible. Thus, if there is any change at any point in the network, it is clearly detected and is totally visible. This helps in securing the data and avoiding tampering. So block-chain can be said as a database with data in a network in a continuously growing manner in the form of lists and blocks.Out of all the available protocols, we use consensus protocol under the cryptic framework to avoid tampering.

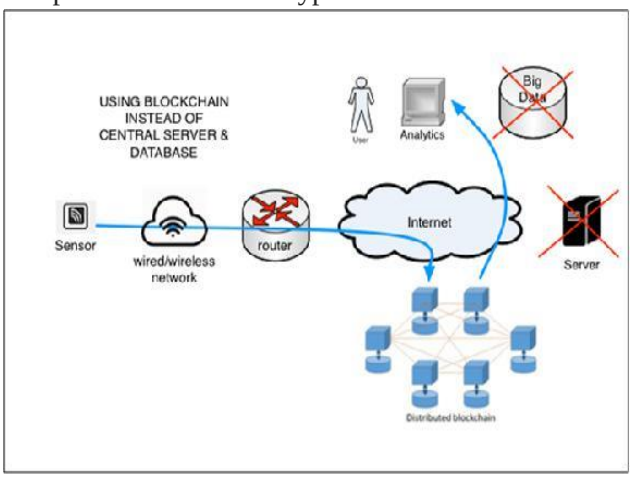

Fig 1. System architecture.

2. Literature Survey

Yuan Zhang et al [1] :-

This paper deals with the secure Time stamping.Secure Time-Stamping scheme can be derived from blockchain based storage to protect files from forward and backward dating. This time stamping scheme is also called as chronos. To enable Chronos to be well compatible with cloud storage services, a Chronos log server,who is subject to cloud service providers, is employed to maintain the outsourced files and their timestamps.

Zhengwei Ni et al [2] :-

Blockchain have been tried to be used as a transaction based autonomous system. All the block chain networks are based on consensus protocols under the crypto framework like proof of work, but this results in the problem of bottleneck as completion of transaction is done at a high latency. Thus, we aim to use shards to enable parallel processes of blockchain networks at different process rates and transaction rates. Thus, we achieve decentralized consensus by individual processes resulting into evolution of block chain selection.

Ahmed Badr et al [3]:-

While academic institutions maintain records such as transcripts and certificates, they are often requested to share these records with other institutions at the request of students for credit transfer, or prerequisites for acceptance into new academic programs. This paper presents a permissioned blockchain-based system to allow institutions to securely and dependably transfer and verify academic records at the student request.

WattanaViriyasitavat et al [4] :-

To explore the promising applications of IoT services, one of the challenges is to enable the interoperability of the services in a decentralized environment. The proposed architecture aims to solve both interoperability and trust issues for IoT services.

AsharAhmadh et al [5]:-

Blockchain-based audit trails provide a consensus-driven and tamper-proof trail of system events that are helpful in creating provenance in enterprise solutions. However, taking into account the transaction bulk generated by these applications and the throughput limitations of existing blockchjains, a single ledger for record keeping can be inefficient and costly.

Hua Zhang et al [6]:-

Cloud is used for storing resources and it provides total security against securing access of data from unauthorized users. It provides total encryption of data and helps in saving the data in another format but it increases the risk of identification of illegal data. Thus, based on the encryption attribute access control, we can use an algorithm that helps in proper identification of illegal data's as well as identifying illegal data and increasing the efficiency and security of the cloud.

NirKshetri et al[7]:-

Block chain and smart contracts are transforming international trade activities by introducing new methods and policies. It helps a lot by elimination of documentary fraud, cost reduction and improvement in efficiency. There are various parties involved including an agent and an inspector. It saves a lot of time by increasing the speed of the transaction. The advantages of block-chain based solutions in international trade activities include faster settlement of international payments, faster

access to working capital financing at cheaper rates, and availability of one-stop solution for all needs related to international trades.

3. Proposed Methodology

As there is no current video detection system that can be easily developed without any training of models and with less time consumption, we propose a system where block-chain will help us overcome this problem. First, the original video will be uploaded on the cloud where it will be totally secured with the help of security provided by various cloud providers. The video will then be converted into a number of images frames and will be stored inside the cloud. Next, each frame will get its unique key or identity. The frames will be formed into a block-chain network. Thus, we totally have the original video saved securely. Then the video that needs to be checked whether it is tampered or not will be uploaded on the cloud. The same process will be carried out until key generation and block-chain network. Then, the keys of both the videos which are in a block-chain network will be compared and if not similar, will give the result as yes i.e the video is tampered or vice versa. For additional security, we will combine all the keys into a single unique key for a single video. Thus, we obtain the result of the video being tampered or not in “YES” or “NO” format.

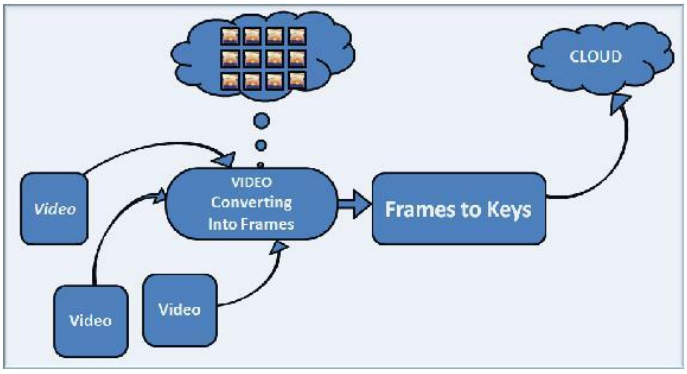

Fig 2. Proposed system

Video is nothing but flow of sequenced static images, Thus, In Figure(a), the specific video will be generated into the number of image frames.

Fig3a. (Video-Frame conversion)

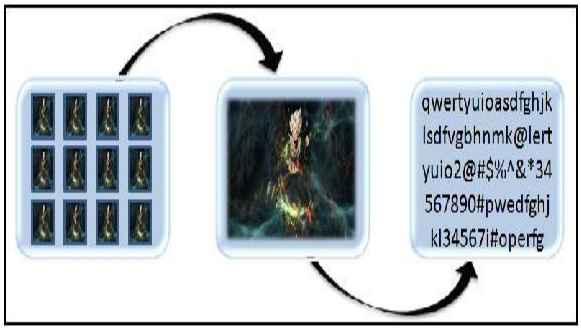

Fig 3b. (Key Generation)

A. Mathematical Model

Let 'S' be the Error detection in big data as the final set

S = ...

Identify the inputs as D

S = D, ...

D = D1, D2, D3, D4| 'D' given Data files

Identify the outputs as O

S = D, L, A...

D = D1, D2, D3, D4| 'D' gives data files.

L = L1, L2 . . . | 'L' gives the log les for upload and download and repair.

A = A1, A2, A3, . . . | 'A' gives alerts

MATHEMATICAL MODEL

Identify the functions as 'F'

S = D, L, A, F...

Function = F1(), F2(), F3(), F4(), F5(), F6()

F1(V) :: Data Collection

F2 (V`) :: Data Encryption

F3 (V ``) :: Proof of Work

F4 (T) :: Block chain Updation

F5 (D) :: Chain Analysis

B. Algorithm

The algorithm that we are using here is the Proof Of Work (POW). This is a consensus type of algorithm. This helps us in building new blocks or nodes in the block-chain network. The users send the unique keys which we have generated for each video frame with each other. This results into a collection and formation of a long chain of blocks or nodes. Thus, each of the block's key is dependent on the previous block as well. If anyone tries to tamper a particular node, the nodes up ahead of that node or block will change their own unique keys and thus it can be easily detected. Here, the chain is formed by competition among users to complete the process and the one that win can establish their block in the network. It takes some more time for computation but is totally secure.Fig 4. Shows exactly how the process is carried out and how the block-chain network is formed.

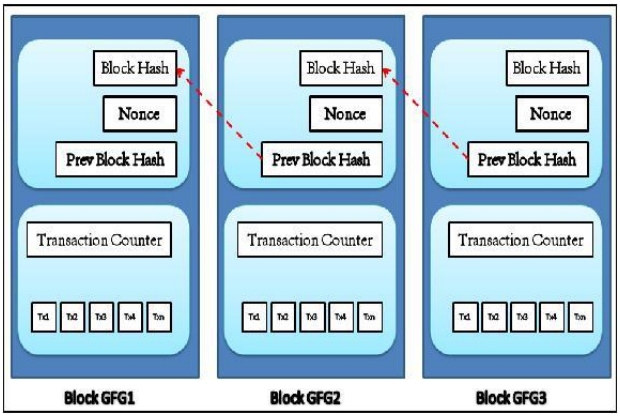

Fig 4. Proof of work

4. System Design

We are trying to develop a system of Block-chain which will be working in a distributed environment. Thus, we will be able to store a large amount of data and avoid it from being tampered by any unauthorized users. The block-chain creates a long chain network of both the original video and the video that needs to be checked for tampering. Thus, it is very easy to check for tampering by just comparing these 2 chains. Videos are continuous frames that are being run simultaneously. They can be easily tampered by changing any frame using modern editing tools. There are no current solutions that efficiently secure this data and enable only the authorized access and authentication. Our system provides these properties. We are using a secured cloud for the storage of these data. Thus, we are providing a framework that helps us in tracing the original source content from the tampered content and also find the exact point where the video is tampered and help us in securing it even if the video is tampered multiple times.

5. Expected Outcome

Based on the comparison of keys generated uniquely, they will be checked for similarity and the outcome would be in the form of yes or no telling us whether a video is tampered or not. We have uploaded a video on cloud which will be considered as the original one. We have taken 10 videos as test cases and we have tampered some of these test cases at different parts. Each video will be broken down into numerous frames and each frame will be allotted a unique key. These frames will be connected in a long block-chain network. Based on the algorithm, each frame's key is formed by unique generation and also the key of the frame previous to it. Thus, each of these test case's frame will be compared to the original one and thus checked whether the keys are similar or not. If the keys are not similar, the entire video is tampered ahead. The keys of all the frames further from the frame of dissimilar key will have different keys. Thus, we will get the expected outcome as a binary yes or no saying that the video is tampered or not.

6. Conclusion

Hence, we have proposed a new secure framework for the avoidance of tampering in videos. We have used block-chain as means of securing the videos. At the base of our framework, we are using cloud as storage and block-chain for encryption and key generation. The key to its design is the observation that a number of frames can be created from a single video. Thus, each frame having its unique key and dependent on the previous frame and the logic of creating a single key from the group of keys of frames helps in increasing the security. Hence, the original recorded video is broken down as such. Then the video to be checked for tampering is put in and the same process of key generation is followed and we have use the algorithm of Proof of Work overall. If the new video is tampered the video fails in matching the keys and it gives the output as yes or no. Thus, It gives high performance result and total security to the videos.

Acknowledgement

The authors also would like to regard to Prof. KishorWagh, AISSMS IOIT, Pune University for informative discussion and a lot of suggestions by to the methods reported in the paper.

References

[1] Secure and Accurate Time-stamping Scheme for Digital Files via Block chain.Department of Electrical and Computer Engineering, University of Waterloo, Canada,2019.

[2] Evolutionary Game for Consensus Provision in Permission less Block-chain Networks with Shards.Department of Electrical Engineering & Computer Science, York University, Toronto, Canada ON M3J 1P3,2019.

[3] A Permissioned Block-chain-Based System for Verification of Academic Records.Tech University Oshawa, Ontario, Canada,2019.

[4] New Block-chain-Based Architecture for Service Interoperations in Internet of Things.Senior Member, IEEE, and Assadaporn Sapsom-boon,2019.

[5] BlockTrail: A Scalable Multichain Solution for Block-chain-based Audit Trail. University of Central Florida,2019.

[6] Research on Data Protection Based on En-crypted Attribute Access Control in Cloud Computing.Institute of Computer Applications China Academy of Engineering Physics Mianyang, China,2019.

[7] Block-chains and International Business. The University of North Carolina at Greensboro,2019.

[8] A Blockchain-based Trusted Data Management Scheme in Edge ComputingMaZhaofeng, Wang Xiaochang, Deepak Kumar Jain, Hanees Khan, GaoHongmin, Wang Zhen.

[9] Towards an End-to-End Architecture for Run-timeData Protection in the CloudNazilaGolMohammadi, Zoltan´ Ad´ am Mann, Andreas Metzger, MarittaHeisel.

[10] Security of Medical Big Data Images using DecoyTechnique.