DOI: http://dx.doi.org/10.26483/ijarcs.v11i3.6623

Volume 11, No. 3, May-June 2020

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

BLOCK CHAIN BASED EFFICIENT MANAGEMENT OF IOT SMART VIDEO SURVEILLANCE SYSTEM

Prajval H L
PG Student, Department of
Computer Science and Engineering
R.V. College of Engineering
Bangalore, Karnataka, India

Prof. Sandhya S
Assistant Professor, Department of
Computer Science and Engineering
R.V. College of Engineering
Bangalore, Karnataka, India

Abstract: Arrangement of surveillance of video process which is based on block chain technology has been proposed. The system which has been intended contains a network of block chain with internal nodes which are trusted. The distributed ledger of block chain includes the metadata of the surveillance footage, thereby stopping the possibility of the data forgery. The architecture of proposed system saves and encrypts the footage, generates a license inside the block chain and exports the footage. Since the private database manages the decryption key for the footage in the block chain, it is not exposed by the internal nodes illegally. Also, the internal administrator can handle and export surveillance footage safely by decrypting the frames stored in the block chain and reconstructing the footage which can be later downloaded.

Keywords: Block chain, Video Surveillance System, Hyper ledger Fabric, IPFS

I. INTRODUCTION

In recent times, the block chain technology is fast lyarising as a shared database technology [1]. Fundamentally, a Block chain mechanics is a shared, circulated and enduring database register that keeps registry of resources and activity over a peer-to-peer shared network. After all, the development of bitcoin by Satoshi Nakamoto has gotten consideration, more analysis is advancing on how to what degree can it be adapted into various fields of logistics business, economics including financial sector and IoT(Internet of Things) [2].

The surveillance of video module tracks footage output from internet protocol (I.P) cameras and keeps footage data. The system is made of camera, storage device, transmission device and playback device. In past decade, surveillance systems by capturing videos have grown into progressively large scale to be handled with fast circulation of closed circuit television (CCTV) for the determination of crime avoidance[3] and facility administration[4].

The footage saved in the system of surveillance must be handled carefully, but the footages are exposed out or viewed by unauthorized individuals, which causes the infringement of private data [5]. Currently, to deal with this complication, a solution is to implementation of access control mechanism to the system of surveillance, but it is still not sufficient in preventing unauthorized exposure by the internal nodes.

Here, a management of surveillance of video process based on block chain mechanics to deal with the issue of illegal leakage of footage in the system of monitoring has been proposed. In the architecture that has been intended, the footage which is gotten back from the camera is encoded and saved in the Inter Planetary File System [6] node linked to the network of block chain. In the block, deciphering key of the footage is not stored, but it is saved in the confidential database of a node in block chain which has the exclusive authorization and can be handled only by the block chain code. For exporting and decoding the footage for anybody who needs to view the footage must validate the export for footage in the network of block chain, then a chain code API license is created. The proposed approach is an approach of securely saving and exporting in a footage surveillance process. The internal manager would not be known the decoding key of the footage and hence cannot access or export the footage without approval.

The rest of the paper is divided as follows. Section II gives a detailed background study of related work. In III section, a new system for controlling of surveillance footage based on block chain mechanics will be proposed. Section IV evaluates the security of the architecture which has been intended. Section V finishes up this paper along with future analysis direction.

II. RELATED WORK

A type of permission and personal block chain is Hyper ledger fabric [7]. Not at all like the public block chain, which can be utilized by anybody, for example, can etherium [8] or bitcoin [9], just clients enlisted in a verification management framework known as MSP (Membership Service Provider) take an interest in network of block chain. Active contract called C Chaincode, and the chaincode in fabric can be executed via Node JS and Go language.

Figure 1 offers the procedure of activity prepared by in hyper ledger fabric v1.2application. It is a procedure after validation of membership service application is finished. To start with, the application interfaces with the peers and calls the chain code to inquiry or to update record. Companion conjures chaincode to create a proposition reaction which consist the question, answer or proposed record refresh and sends it to application. Application which gets the response demands the request for the activity to the orderer. The n orderer gathers transactions from system, produces blocks and all peers get this blocks. The peer gets the block and only after checking it, updates the record.

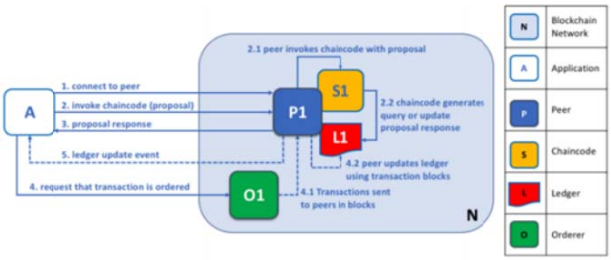

Figure 1. Transaction Processing Application of Hyper ledger Fabric [10]

Fabric can boost confidentiality and privacy by proposing the approach of a channel among the participating organizations in the block chain. Even if it endures in the identical network of block chain, the participants of identical channel split information. Nonetheless, generating some of these independent channels for some information will bring upon extra overhead.

To take care of this issue, Hyper ledger fabric v1.2 gives a method called Private Data Collection (PDC)which can gather, submit and inquiry personal information without making singular channels. The PDC comprises of private information hash. Private information can be verified distinctly by approved peers who are approved to see information in a similar channel. The peer getting the block checks the access privilege to the private information. From that point onward, if there is a benefit, bring personal information through shared convention from another peer, at that point approve the hash of personal information, submit the block, and store it to personal record or ledger.

III. PROPOSED SYSTEM

Block chain technology-based architecture that can equitably demo if the system of management is well handled. Additionally, it reduces exposure or viewing by unauthorized persons. In the architecture which has been proposed, footage is encrypted securely and saved, and licenses are enforced and securely exported during video exporting. Fig 2 shows the management system architecture based on block chain with footage saving and exporting facility.

A detailed architecture of the proposed system with various components and the work process is given in the Figure 1. The factors are:

- Inter Planetary File System (IPFS) : This is the node where the distribution and storage of encrypted footage are.
- Camera: Internet protocol enabled device for getting the video frames.
- Surveillance Application: Client side application which is used by authenticated block chain membership service of internal nodes.
- Block chain Network: Private network of block chain based on Hyper ledger fabric v1.2
- Content Delivery Network (CDN): It is a network for transmission of encrypted footage.

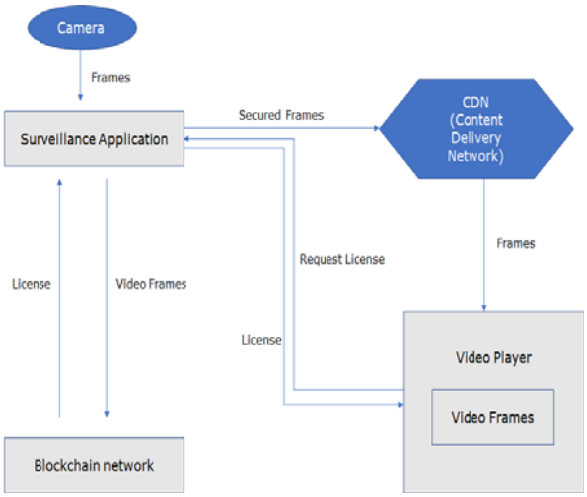

Figure 2. Architecture of the surveillance system

- Video Player: A video player which is DRM enabled that can play encrypted video frames which it receives.

At the point when footage which is recorded in the internet protocol camera is transferred to the surveillance application, the footage is encoded and put away inside IPFS hub. The surveillance application enforces the footage transaction for transferring to the network of block chain with hash and content key (footage decoding key) created in IPFS node and the footage metadata. In the event that video transfer is finished in the block chain, the metadata of the footage is shown in the surveillance application. Footage player which is appropriate to the surveillance application is given from internal node ahead of time to individual who needs to see the footage. The player which is issued sends a license and exports the issuance solicitation to see the footage. At the point when a solicitation for the permit is gotten from the footage display maker, the surveillance application executes and gets a reply from a transaction to create a permit to network of block chain. The surveillance application which gets the reply transmits the encoded footage and a permit to the footage displayer, and deciphers the footage with key of content which is remembered for the permit in the footage displayer's CDN system to display the footage. Permitting & decoding of DRM empowered footage displayers is done distinctly via the CDN modules and isn't legitimately presented to the client.

In the event that the key of content is utilized in footage decoding is uncovered, then the footage can be decoded from the exterior, that prompts security attack issue of the person. Thusly, the key of content ought to be overseen safely with the goal that internal manager cannot export it. Along these lines, a structure to forestall the key of content is utilized while decoding footage utilizing PDC that is an element of personal information handling from hyper ledger fabric is proposed.

The network of block chain estimates that the footage administration destination is inside of school A and it shapes a channel supporting peer 1, embracing peer 2, submitting peer, orderer are validated nodes from MSP (Membership Service Provider). Welcoming peers who are peer approved by PDC module and possess personal state database. Inside

structure including the planned network of block chain, the footage transferring system is as per the following:

- The camera videotapes the footage F (video) in which is in the video buffer and then sends it to surveillance application.
- Encryption of F using AES-256 k1 (content key) inside the encryption module implemented in surveillance application.
- The EF = E_{k1}(F) which is encrypted is sent to the node IPFS from surveillance application.
- EF which is encrypted is are disseminated and saved in the IPFS node.
- Gets back h1 = Hash(EF) of encrypted footage from node IPFS.
- Surveillance application sends a transaction offer to the commending peer 1 that runs the code of footage upload with h1, mF (metadata of Footage)k1.
- A commending peer 1 mimics chain code and achieves endorsement work.
- At a point when approval is finished, approving peer 1 briefly saves the solution of k1 in transient information save and offers k1 with shared convention just to the credible peer (approving peer 2).
- Approving peer 1 sends the authentication hash and the result that verifies k1 to the application of surveillance.
- The surveillance application sends the authentication conclusion with the k1's hash to the orderer.
- The orderer creates blocks consisting of activities and transmits them to the peers.
- The peer, who will get the block, executes the process of block authentication in the executing peer than the commissioned peer. Block authentication process is carried out in a state where the constituents of the k1's hash are not known.
- Approving peers, who are commissioned peers, analyze the group guidelines to check whether they possess approach rights to the reciprocal k1. At that point, the information coordinating with k1's hash coordinating for the block is confirmed. On the off chance that there is no variation from the norm, k1 is put away in the personal state database and k1 briefly saved in the transient information store is erased. Just h1 and mF are saved in the State DB.

The way toward getting footage via the internal node is appeared as four through eight in Figure two. The internal administrator except which the footage displayer has been given to client ahead of time, and the way toward sending out the footage from the structured surveillance system is as per the following.

- The candidate broadcasts the nP (Player Serial Number) and the mF data relating the footage to the internal administrator.
- Internal administrator transmits the transaction proposition to approving peer 1 or approving peer 2 that runs the permit which results in creating chain code which includes mF and nP, t(term), c(count) for the requested footage in the surveillance Application.
- Approving peer 1 or approving peer 2 runs the chain code and achieves support work. At the point when the execution of chain code takes places, k1 put away in personal state database which is recovered utilizing Get Private Data (), a chain code API, and a L(license) is produced dependent on nP, t, and c and saved in a chain code information struct.
- Approving peer 1 or approving peer 2 sends the authentication conclusion to the surveillance application when the approval is finished.
- The surveillance application sends the authentication conclusion to the orderer.
- The peer getting the block back executes the it and the authentication system and restores the record by saving the created L in its State database.
- At the point, the record of the peers is restored; the surveillance application runs the inquiry to approve the L.
- The surveillance implementation that gets back the decision by inquiring the peer loads the EF from Inter Planetary File System node.
- The surveillance implementation sends the L to the footage displayer and sends the EF via the CDN.
- Decodes and runs the footage from CDN of footage displayer.

IV. SECURITY ANALYSIS

Guaranteeing the stability of the information and also maintaining a strategic distance from the security infringement of the data storage device, for example, CCTV recording the face-head of the person. To tackle those issues, a private control framework is introduced in the footage surveillance process. Be that as it may, since the private control framework commands the entrance all things considered yet the control of the approved internal manager is not performed, the issue of unapproved perusing and emptying from the interior manager keeps on arising. By implementing a surveillance framework dependent on a personal block chain, it is conceivable to demonstrate impartially if the footage data in activity is very much overseen. After all, the content is saved to the distributed ledger via the block following demonstration; it favors to be distributed amidst the internal managers and demonstrated authentic activity. Furthermore, specialized action can be implemented to confine unapproved perusing and trading from the internal node in the proposed framework. The footage is encoded and saved in the Inter Planetary File System node associated with the network of block chain and decrypting key of the footage is saved in the database of the particular high level administration node inside the network of block chain. After the entire decoding key could be gotten just via the chain code API without being straightforwardly presented to the block, the inside administrator cannot affirm the decryption key, and hence the footage cannot be seen or traded vindictively.

V. CONCLUSION AND FUTURE DIRECTION

Here, a surveillance of footage process based on technology called block chain has been proposed. Footages documented from internet protocol cameras are encoded and saved in Inter Planetary File System node via a personal network of block chain which consists of credible internal nodes. The decoding key of footage will not be saved inside the block but saved inside the database of a particular node containing the group authentication authorization so that the internal administrator can not approve the decoding key. Additionally, when an individual who needs to see footage gets endorsement from network of block chain or an internal node keeps track of footage on display, the internal admin runs a chain code for transmitting the footage. In the chain code API and the license is created by utilizing the decoding key, the understanding of time frame, and the quantity of browsing. The surveillance framework can safely oversee recordings from outside people and internal managers in the block chain structure which is proposed. Additionally, it is conceivable to deal with the target record whether the footage export is well handled.

VI. REFERENCES

[1] Yena Jeong, DongYeop Hwang, Ki-Hyung Kim. "Block chain-Based Management of Video Surveillance Systems" , 2019 International Conference on Information Networking (ICOIN), 2019

[2] Andreas M, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, pp.49-68, O'REILLY, 2015.

[3] Zheng, Zibin, et al. "An overview of block chain technology: Architecture, consensus, and future trends." Big Data (BigData Congress), 2017 IEEE International Congress on. IEEE, 2017.

[4] Piza, Eric L., et al. "The effects of merging proactive CCTV monitoring with directed police patrol: A randomized controlled trial." Journal of Experimental Criminology 11.1 (2015): 43-69.

[5] Hwang, Jeonghwan, and Hyun Yoe. "Study of the ubiquitous hog farm system using wireless sensor networks for environmental monitoring and facilities control." Sensors 10.12 (2010): 10752-10777.

[6] Jho, Whasun. "Challenges for e-governance: protests from civil society on the protection of privacy in e-government in Korea." International Review of Administrative Sciences 71.1 (2005): 151-166.

[7] Androulaki, Elli, et al. "Hyperledger fabric: a distributed operating system for permissioned block chains." Proceedings of the Thirteenth EuroSys Conference. ACM, 2018.

[8] Benet, Juan. "IPFS-content addressed, versioned, P2P file system." arXiv preprint arXiv:1407.3561 (2014).

[9] The Cointelegraph. A Brief History of Ethereum From Vitalik Buterins Idea to Release, 2015.

[10] Hyperledger, hyperledger-fabric.readthedocs, [online]: https://hyperledger-fabric.readthedocs.io/en/release-2.0/

[11] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.