Blockchain-based Management of Video Surveillance Systems: A Survey

Deepak K, Aditya Nagaraj Badiger,
Akshay J, Kika A Awomi
dept. of Computer science & Engineering
Dayananda Sagar College of Engineering
Bangalore, India
akshayj1814@gmail.com

Deepak G, Harish Kumar N
dept. of Computer science &
Engineering Dayananda Sagar College of
Engineering Bangalore, India

***Abstract*— In this survey, we go through all the papers that lead up to our idea of a smart video surveillance system and make a comparative study of available technologies. The increase in efficiency by using hyper ledger for blockchain is analyzed along with the study of modern data sharing techniques like CDN and IPFS.**

***Keywords*— Blockchain; Hyperledger Fabric; Video Surveillance System; InterPlanetary File System.**

I. INTRODUCTION

Due to an increasing number of crime rates, day by day, CCTV cameras and video surveillance systems have become a necessity. But due to insecure storage and sharing methods, the videos stored are accessible by unauthorized personnel. The currently available security protocols and techniques have been broken several times by the attackers. It calls for an alternative system that is not only much safer but also intangible. With the advent of new blockchain technology, privacy and data security field is seeing a change. Blockchain is an interconnected ledger that stores data which is intangible, but blockchain cannot store data which is greater than 1MB. Hence, we have to store the data in an off-site database. The primary role of blockchain here is to validate the request for data access by a person and to issue him a license, on getting of which the person can access the data. Even though we use CCTV as a unique case, the same technique can be used for different types of privately shared data which opens a vast field for research.

II. PROBLEM STATEMENT

- Recently, the blockchain is rapidly emerging as a distributed database technology. Blockchain technology is fundamentally a decentralized, shared, and immutable database ledger that stores registry of assets and transactions across a peer-to-peer (P2P) network.
- The videos stored in the video surveillance system must be managed safely, but the videos are leaked out to unauthorized persons or viewed, resulting in the infringement of personal information.
- To solve this problem, a system has been developed that applies access control to the video surveillance system.

III. LITERATURE SURVEY

A paper published by Arunmozhi Manimuthu, Raja Sreedharan, Rejikumar and Drishti Marwah [1] covers both the technical and economic aspects of the bitcoin currency. It provides a clear picture of how it all started starting from the paper by Sathoshi Nakumoto. The need for an intangible, mediation less and a secure currency is clearly mentioned. The bitcoin works using a public ledger called blockchain, which has developed as its domain. Every user has to have a bitcoin wallet and one or more bitcoin addresses for a bitcoin transaction to take place. Any transaction, without any conditions, should be verified and validated by all the systems in the Bitcoin Network. This makes it an intangible network of distributed data that can not be modified easily. The users are not asked for any identification, and hence their identity remains private. This also means that the network does not discriminate among users based on their status. It is one of the advantages of using the bitcoin network. There are a number of applications of bitcoins compared to state-issued currencies that are being used worldwide. It can be used to prevent fraudulent transactions; it includes trust and integrity among users etc. But like every technology, bitcoin has its drawbacks. One of the main ones is the lack of understanding of the working of bitcoin. But due to the awareness of Information technology among younger generations, bitcoins seem to have a bright future.

A paper by Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang [2] clearly illustrates the working of blockchain technology in a detailed manner. Blockchain technology gained its popularity when people started using Bitcoins all over the world. Technologies like blockchain play a vital role in a world full of attackers trying to take advantage of loopholes in the existing systems. A blockchain is an interconnected link of blocks containing any data. The genesis block is the first block of a blockchain network that has no parent block. Every block includes data like the hash of the parent node, timestamp(when the block was created), the hash of the data, Nonce etc. The standard public key and private key encryption are used in the signing and verification of transactions.

The blockchain is decentralized, persistent, editable, and it keeps the transactions anonymous. There are a lot of algorithms

978-1-7281-5197-7/20/$31.00 ©2020 IEEE

used in blockchain to reach a consensus between nodes since they are widely distributed. They include Pow(proof of work, also called as mining), PoS(proof of stake), PBFT (Practical byzantine fault tolerance), DPOS (Delegated proof of stake), Ripple and Tendermint. One of the main problems here is the consensus between a lot of untrustworthy nodes. This is a transformation of the Byzantine Generals(BG) Problem.

A paper by Leslie Lamport, Robert Shostak and Marshall Pease [3] explain the Byzantine Generals(BG) Problem in detail. When several divisions of the Byzantine army are camping in the enemy territory, each division will be led by a general. But there is a difference of opinion on the next action to be taken. But due to the variation of views, it's challenging to come to a consensus. This is a BG problem. This problem can be solved by only through the proper flow of information from general to general according to their opinions on the situation. The same method is followed in the Blockchain using different algorithms mentioned in the previous paper.

Sathoshi Nakumoto [4], in his paper on bitcoins, explains the working of the Pow(Proof of Work) consensus protocol. It is nothing but the process of scanning for a value the hash of which is a zero bit value. In general terms its called mining. Specifically, in the case of bitcoins, it was done by incrementing the nonce in the block. This makes any given block in the ledger inaccessible as the nonce is incremented from time to time and accordingly the hash is changed for every block in the network. This is how consensus in a blockchain network works.

The paper by Juan Benet [5] discusses the shortcomings of the current use of Http and the web services provided by it and how it will be irrelevant soon as the future is all about the transfer and streaming of the large files. The Http is suitable for small files, and the cost is very less when transferring a large number of them, but when it comes to petabytes of data, it falls short.

The paper is about building a robust IPFS for transfer and storage of large files safely. The design uses several technologies such as kademlia distributed hash table for identifying nodes, for networking, it can use any of the transfer protocol. For routing, it uses coral or again kademlia DHT. The exchange of data is through bit swapping.

It has DAG for storing the hash code for a target data location. This IPFS system has any uses such as- It can be used as an encrypted file or data sharing system, as a database, also as a permanent web system wherein the links don't die.

A paper by Andrej Binder and Ivan Kotuliak [6] sheds light on the working and importance of content delivery networks. This system works in the application layer of the network architecture. It helps in delivering digital data like videos and photos to many endpoints without any modifications to the underlying architecture of the network. Without CDN, a single source has to send data to multiple systems leading to inefficient data transfer and problems in data transmission. The CDN divides every system parsing the data from the source as nodes. Each node will have its unique address for identification and request routing. When a system requests the data, instead of connecting it to the source, the data is pulled from these nodes that store the pieces of data. This decreases the load on the server as well as the traffic in the medium used. The IETF(Internet Engineering task force) group has suggested a standard for essential CDN interconnection. This will lead to the widespread use of CDNs as their advantages become more and more evident.

A paper by Jeonghwan Hwang, Hyun Yoe [7] illustrates the use of WSN and CCTV technology to improve the production and lifespan of pigs on a Hog farm. The primary purpose was to boost the production and standard by using the scientific farming technique. A systematic management system was designed considering the environmental scenarios such as temperature setting, Air ventilation Quantity system and temperature variations. CCTVs are deployed to keep an eye on the animals and also notice odd behaviour in them. WSN sensors are used to accumulate details and facts of the surroundings and habitat to make a database which suits best to help shape the required design and tool for better operation. The proposed system offers effective habitat monitoring and traceability for farmers and can further be deployed in other fields such as greenhouse management, warehouse management, etc.

A paper by Eric L Piza, Joel M Caplan, Leslie W Kennedy and Andrew M Gilchrist [8] strides over the issues of CCTV surveillance and adequate safety measures in case of emergencies in certain areas of Newark, NJ. The paper addresses two main obstacles, i.e. high camera-to-operator ratio and different response mechanism of police inference for safety. The methods discussed and used in this paper is an area-based controlled randomized trials and block design. The experiment was designed by the team and police officials based on the areas where the CCTVs were deployed. Also, an additional CCTV operator is used to keep an eye on the rest of the CCTVs. Digitization of the line of sight is done using GIS(Geographic Information System). Usage of two patrol vehicles to respond to emergencies which is a part of the real solution to the safety and security issues. Combination of these technical and physical mechanisms proved to be a great success compared to the stand-alone CCTV deployment and effectively prevented crime incidents, especially on street scenarios.

A paper published by Everett Hildenbrandt, Manasvi Saxena, Nishant Rodrigues, and Xiaoran Zhu [9] covers KEVM, an executable formal specification of the EVM's bytecode stack-based language built with the K framework. The primary analysis of the paper is to evaluate the correctness and performance of KEVM with the help of the official Ethereum test suite. To illustrate this purpose, two different-language implementations of the ERC20 Standard Token is verified against the ERC20 specification.

Ethereum is a smart contract system that is self-executing financial instruments that synchronize their state, often through

a blockchain. It implements a general-purpose replicated "world" with a quasi-Turing complete programming language. The main goal of Ethereum is to allow arbitrary applications and scripts that execute in blockchain transactions, using the blockchain to synchronize their state.

Kristian Lauslahti, Juri Mattila, Timo Seppälä [10] in their paper on Smart contracts discuss the possibilities we have to replace the traditional way of contracts and agreements using the blockchain technology. Due to its intangible nature, it can be helped to replace stamped bonds. We use a similar architecture in our system where there is a multilevel agreement on any transaction that has to be done on the video footage data that is stored in the IPFS.

IV. CONCLUSION

The survey of the above papers reflects an edge of modern technologies in terms of both security and efficiency. Data sharing techniques like IPFS and CDN are much faster and safer compared to traditional database systems. These can be implemented in an interconnected and efficient manner to achieve a better and secure system than the existing ones.

V. REFERENCES

[1] A. Manimuthu, R. Sreedharan V., R. G. and D. Marwaha, "A Literature Review on Bitcoin: Transformation of Crypto Currency Into a Global Phenomenon", IEEE Engineering Management Review, vol. 47, no. 1, pp. 28-35

[2] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017.

[3] L. Lamport, M. Pease and R. Shostak, *The Byzantine generals problem*. Menlo Park, Calif: SRI International, 1982.

[4] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*.

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

[6] A. Binder and I. Kotuliak, "Content Delivery Network Interconnect: Practical experience", *2013 IEEE 11th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 2013.

[7] J. Hwang and H. Yoe, "Study of the Ubiquitous Hog Farm System Using Wireless Sensor Networks for Environmental Monitoring and Facilities Control", *Sensors*, vol. 10, no. 12, pp. 10752-10777, 2010.

[8] 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.

[9] E. Hildenbrandt et al., "KEVM: A Complete Formal Semantics of the Ethereum Virtual Machine", *2018 IEEE 31st Computer Security Foundations Symposium (CSF)*, 2018.

[10] K. Lauslahti, J. Mattila and T. Seppälä, *Smart Contracts – How will Blockchain Technology Affect Contractual Practices?*. 2017.