International Journal of Psychosocial Rehabilitation, Vol. 18, Issue 02, 2014
ISSN: 1475-7192

A Privacy Preserving Based Using Block Chain Method

A. Viswanathan,

Associate Professor in CSE,

KSR College of Engineering,Tiruchengode-637 215.

professorvichu@gmail.com

M. Umamaheswari,

Assistant Professor in CSE,

KSR College of Engineering,Tiruchengode-637 215.

umadeena@gmail.com

T. Sudhakar

Assistant Professor,

Dept. of Computer Technology

Anna University, MIT Campus. Chennai.

tsudhakar105@gmail.com

M. Sathya,

Assistant Professor in CSE

K.S.R College of Engineering, Tiruchengode 637215

sathimanogaran@gmail.com

ABSTRACT

Security camera video is crucial for crime prevention and investigation in smart cities. Closed-circuit television (CCTV) cameras are critical for a range of public tasks in a smart city; when coupled with Internet of Things (IoT) technology, they may morph into smart sensors that help in safety and security. The veracity of the camera, on the other hand, raises concerns regarding data integrity and application. In this paper, we present a blockchain-based method for ensuring the trustworthiness of preserved recordings, allowing authorities to determine whether or not a video has been tampered with. It enables in differentiating

between real and fake recordings, as well as assuring the authenticity of security cameras.Because the blockchain's distributed ledger also records the information from the CCTV camera, the danger of data manipulation is eliminated. This immutable ledger decreases the risk of copyright infringement for law enforcement agencies and clients users by ensuring possession and identification.

1. INTRODUCTION

Rapid growth of surveillance systems and services within metropolitan areas was required to fulfill people's expectations for an improved quality of life. Appropriately, the Internet of Things (IoT) industry has experienced a phenomenal increase of digital devices such as smartphones, sensors, smart applications, actuators, and intelligent machines, resulting in obvious business objectives. It is now feasible to join all nodes on the internet and link them together. The smart city is becoming more sophisticated than in the past as computer-aided technology advances.

Cameras in an observation system and sensors in a transportation system are two examples of electronic applications used in smart cities. A smart city framework augmented by IoT technology is a revolutionary notion, but it also poses new data security concerns. Closed-circuit television (CCTV) cameras have evolved into an essential component of a smart city.

Surveillance is critical in assisting governments in monitoring and evaluating developing disease patterns and trends. Surveillance is critical because it helps to better noncommunicable disease prevention and treatment. Countries may define goals and design focused programs to counteract the noncommunicable illness epidemic using the data obtained.

2. RELATED WORKS

Much research has been conducted in the field of video forensics. Video evidence may now be used in court cases as a result of this advancement. Among the most recent technologies used for video forgery detection include an autoencoder with recurrent convolutional neural networks, an autoencoder with a goturn algorithm, watermarking techniques, and digital signatures. The reference proposed an architecture based on autoencoders and recurrent neural networks to detect video counterfeiting. To exploit dependencies, they developed a long short-term memory (LSTM) model. provides a model for determining the trustworthiness of digital videos that employs an auto-encoder and a goturn algorithm. Furthermore, a number of variables throw the veracity of CCTV video data into doubt.

CCTV-based administrations, on the other hand, are expanding and diversifying. The reliability of a photograph in order to give appropriate guidance The Privacy Act considers CCTV camera installation in public places, which involves contacting CCTV owners for video information. This procedure, however, is time-consuming. It is difficult to use a movie

in open organizations regardless of how it was obtained since the film cannot be guaranteed to be original and unedited.

The Privacy Act considers CCTV camera installation in public places, which involves contacting CCTV owners for video information. This procedure, however, is time-consuming. It is difficult to use a movie in open organizations regardless of how it was obtained since the film cannot be guaranteed to be original and unedited. After some time, created a framework that employs cryptographic approaches to verify sensor data by creating a log sealing system and providing permanent pieces of evidence that can be utilized for log verification.

Smart Cities are frequently shown as perplexing light-structured systems, and are commonly characterized as networks of related gadgets and their surroundings. In terms of resource interdependence, four important components were identified in order of significance. Which of these are included in this ecosystem's concept of a smart city? Interaction or engagement, balance, and self-organization, loosely coupled actors with similar goals, and, finally, loosely coupled actors with shared goals IoT devices are available in a range of designs and sizes. Memory and computational complexity are necessary to deal with today's computing gadgets. there is a shortage of Because of their computer power, they are vulnerable to a wide range of cyber-attacks.

The term "cloud computing environment" refers to a group of resources or services that are made accessible over the Internet. Their objective was to, among other things, provide producers, developers, and users of cloud computing a good awareness of the security issues that affect cloud computing the most as well as the many frameworks that are available to address them. A technique for differentiating Distributed Denial of Service (DDoS) assaults has been found. Authors presented in this work a security model for cloud computing data transmission that properly analyzes the empirical capability of a competing authentication system for data transmission protection. This is good news because the experiment results show that the proposed design is more efficient than the frameworks already.

They discussed a technique based on the I-AES algorithm, as well as a private database architecture that they created. This research also provides a theoretical framework, which is important given the large number of 5G devices that might be deployed in the Internet of Things. According to the study's findings, the proposed algorithm outperformed the previously used methods in terms of execution time and throughput .

3. METHODOLOGY

A blockchain is a distributed system that is operated by nodes connected over the Internet and replicates a central computer function. Theoretically, decentralized ledgers are taking the place of centralised ledger systems in blockchain technology. A blockchain is trusted because it uses encryption methods and operates independently of a third party. A network of

connected data blocks makes up a blockchain. Entries are permanent, transparent, and readable, and only certain members are permitted to generate and view blocks.

Transactions are stored in chronological order on a continually increasing database. Information is copied and stored on a common system across the framework. It encourages the exchange of significant value without the necessity for a central middleman.

Hyperledger Fabric is an open source distributed ledger solution for private blockchains. It is very scalable and has been used in a wide range of industries. Blockchain technology has the ability to transform a wide range of organizations, business models, and working techniques, including installation, bookkeeping, and inspection. Because of its specialized, complicated nature, as well as the need to recognize these wide shifts in the private, public, and commercial sectors, this breakthrough, like previous disruptive inventions, will take time to catch on, with a gradual rise in pace over time.

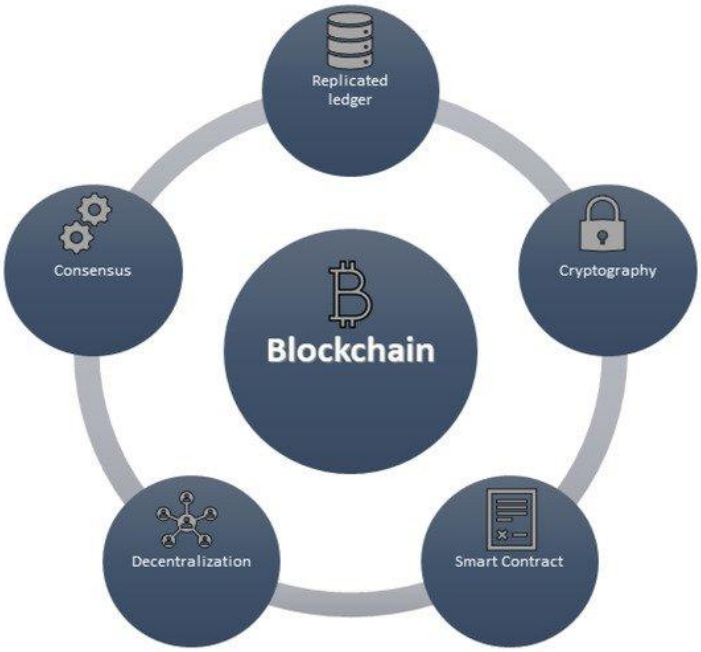

FIGURE 1: BLOCK CHAIN FLOW

For participants and CCTV nodes, the proposed solution establishes a blockchain interface. Certain frames of the image are picked and broadcast across the blockchain network for image fraud and modulation verification. If all of the continuously created CCTV video frames are stored in the blockchain, the transaction becomes too large, lowering data size and boosting the chance of practical application by using only a few frames from each movie. Several frames are examined to see whether the picture is manufactured.

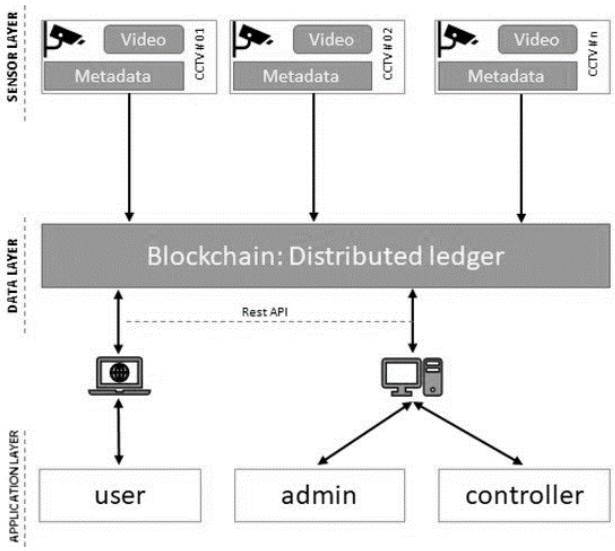

FIGURE 2: BLOCK DIAGRAM

Each user must be given a private key, which is the responsibility of the membership service provider (MSP). Additionally, it provides an event notice after issuing the command. a transcript of records A task can be made by a registered user on an IP video server. Every every CCTV The device is connected to the blockchain via the distinct hashed key value.

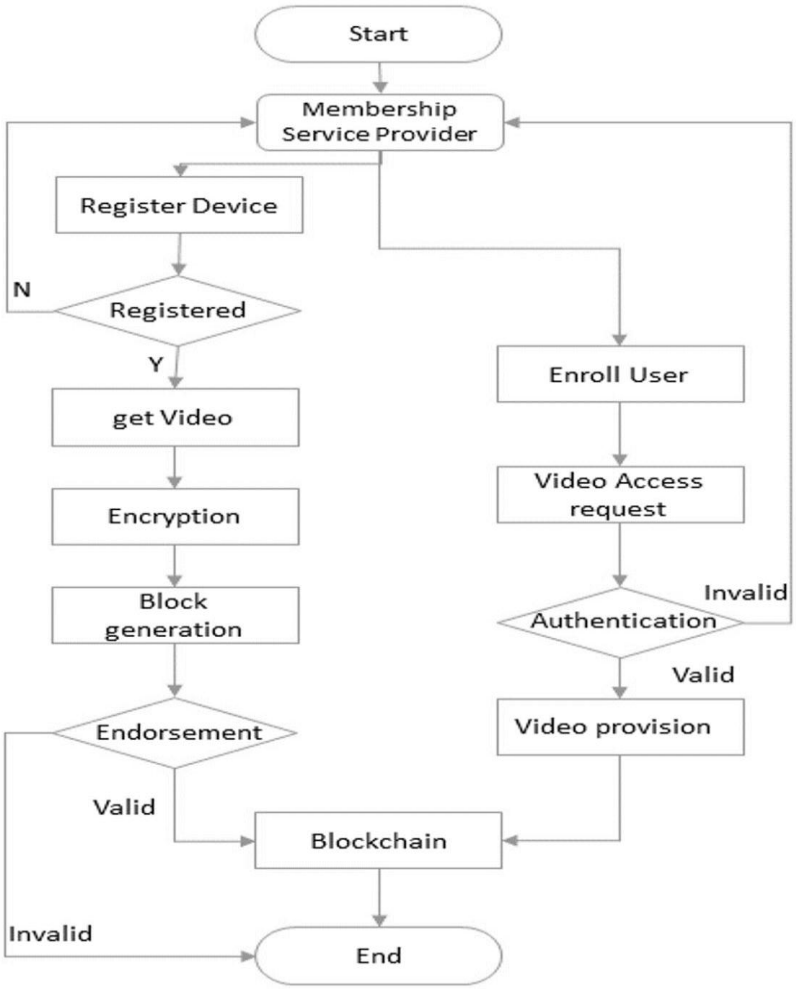

FIGURE 3: WORK FLOW

On a regular basis, each node delivers the same message. Metadata will be recorded on the blockchain alongside video and image data. A blockchain network is a distributed ledger that tracks transactions using encryption. When the system is configured, the network administrator provides validating nodes. Each block must be approved by an authenticating peer before being added to the chain.

We used the blockchain technology for data authentication and verification in smart cities. In this section, we go over the flow of the proposed platform and its components in detail. Figure 1 depicts the flow of our proposed model. Everything begins with user and device registration. The membership service provider assigns a unique key to each peer in the system (MSP). We're using Hyperledger Fabric, a private blockchain that varies from public blockchains in terms of user access. A public blockchain may be joined by anybody, but only genuine users with the private key issued by the system administrator can access a private blockchain.

The suggested approach obtains the image sensor's video and information and encrypts it.The suggested system encrypts the data from the image sensor's video and metadata. It creates a

The proposed method acquires and encrypts the image sensor's video and information. The proposed system encrypts the video and metadata data from the image sensor. After encryption, it generates a block, and each block is supported by endorsing peers. In Hyperledger Fabric, there is no consensus method or block mining. The system administrator, on the other hand, selects validation peers based on the validation aim. The approved use can make REST API requests to gain access to the blockchain's digital data.

4. RESULT & DISCUSSION

An access control rule, a script, a model, and a query specification are the four components that make up a hyperledger smart contract. Hyperledger Fabric supports the usage of state databases based on the kind of data, such as LevelDB and CouchDB. These two databases are capable of supporting fundamental chaincode transactions. Smart contract data is saved as a key-value pair in LevelDB, the default state database. The peer node of the system already has it.

The cost-benefit analysis takes into account the steps necessary to decide if a system is viable. The market for surveillance technology for smart cities is expanding quickly. This may total 19.5 billion euros by 2023, according to certain data. Asia, particularly China, is the largest market for surveillance equipment, according to studies. Eight of the top 10 most monitored cities worldwide are located in China. The top ten cities worldwide in terms of installed cameras are shown in Figure 2, along with a ranking of each city's safety.

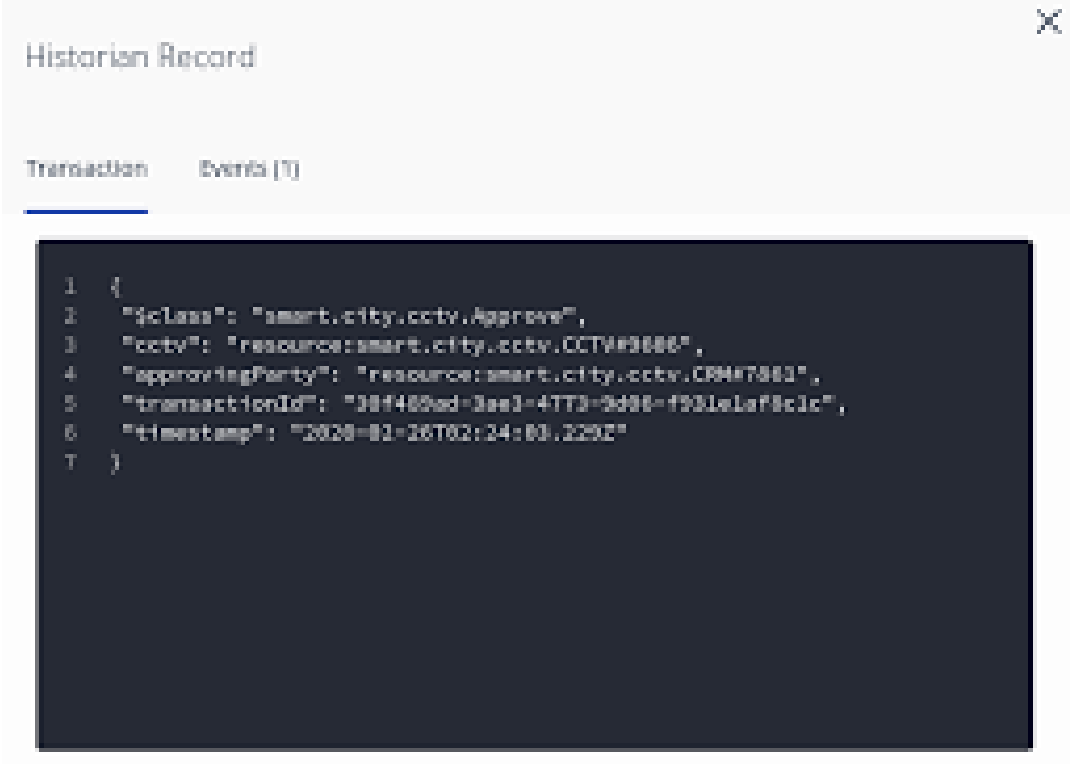

FIGURE 4: TRANSCATION RECORD

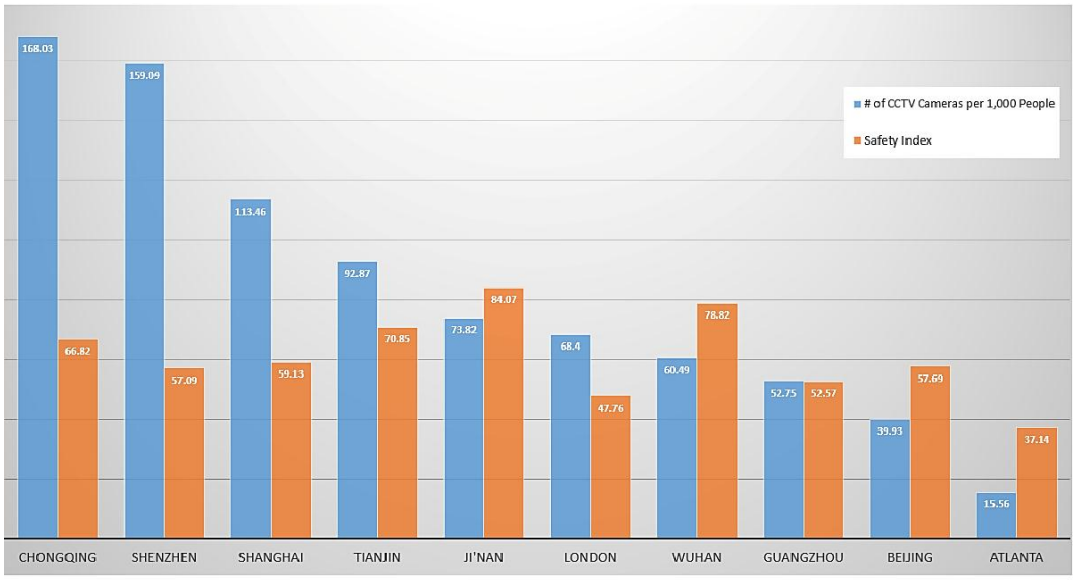

FIGURE 5: COUNTRY BASED SAFETY MEASURES

CONCLUSION

Additionally, the blockchain's distributed ledger gathers data from CCTV cameras, reducing the possibility of data fraud. By establishing ownership and identity, this immutable ledger lowers the danger of copyright infringement for law enforcement organizations and clients users. The fact that this application ensures data security and permits the secure storing of

picture data via a distributed ledger makes it a good fit for blockchain technology. A future research may address the challenge of a wide bandwidth and incentive mechanism as one area to investigate.

REFERENCES

1. Song, J.; Yang, Y.; Huang, Z.; Shen, H.T.; Luo, J. Effective multiple feature hashing for large-scale near-duplicate video retrieval. IEEE Trans. Multimed. 2013, 15, 1997–2008.
2. Nassauer, A. How robberies succeed or fail: Analyzing crime caught on CCTV. J. Res. Crime Delinq. 2018, 55, 125–154.
3. Kwon, B.W.; Sharma, P.K.; Park, J.H. CCTV-Based Multi-Factor Authentication System. J. Inf. Process. Syst. 2019, 15, 904–919.
4. Panwar, N.; Sharma, S.; Wang, G.; Mehrotra, S.; Venkatasubramanian, N.; Diallo, M.H.; Sani, A.A. IoT Notary: Sensor data attestation in smart environment. In Proceedings of the 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 26–28, September 2019; pp. 1–9.
5. Qayyum, A.; Qadir, J.; Janjua, M.U.; Sher, F. Using Blockchain to Rein in the New Post-Truth World and Check the Spread of Fake News. IT Prof. 2019, 21, 16–24.
6. Ghimire, S.; Choi, J.Y.; Lee, B. Using Blockchain for Improved Video Integrity Verification. IEEE Trans. Multimed. 2019, 22, 108–121.
7. Kerr, M.; Han, F.; van Schyndel, R. A blockchain implementation for the cataloguing of cctv video evidence. In Proceedings of the 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand, 27–30 November 2018; pp. 1–6.
8. Karame, G. On the security and scalability of bitcoin's blockchain. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1861–1862.
9. Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling blockchain: A data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. 2018, 30, 1366–1385. [CrossRef] Electronics 2020, 9, 484 21 of 21
10. Cachin, C.; others. Architecture of the hyperledger blockchain fabric. In Proceedings of the Workshop on Distributed Cryptocurrencies and Consensus Ledgers, Chicago, IL, USA, 25 July 2016; Volume 310, p. 4.
11. Lai, K. Blockchain as AML tool: A work in progress. Int. Financ. Law Rev. 2018. Available online: https://www.iflr.com/Article/3804315/Blockchain-as-AML-tool-a-work-in-progress. html?ArticleId=3804315 (accessed on 10 March 2020)
12. M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, "An efficient image encryption technique based on two-level security for internet of things," Multimedia Tools and Applications, 2022.
13. E. M. Onyema, P. K. Shukla, S. Dalal, M. N. Mathur, M. Zakariah, and B. Tiwari, "Enhancement of patient facial recognition through deep learning algorithm: ConvNet," Journal of Healthcare Engineering, vol. 2021, Article ID 5196000, 8 pages, 2021.
14. S. Stalin, V. Roy, P. K. Shukla et al., "A machine learning-based big EEG data artifact detection and wavelet-based removal: an empirical approach," Mathematical Problems in Engineering, vol. 2021, Article ID 2942808, 11 pages, 2021.

15. D. Jain, P. K. Shukla, and S. Varma, “Energy efficient architecture for mitigating the hot-spot problem in wireless sensor networks,” Journal of Ambient Intelligence and Humanized Computing, 2022.