SURVEILLANCE CAMERA FOR SECURITY MEASURES USING BLOCK CHAIN METHOD

KOTHAGATTU RAMU,
Associate Professor,
Department of Computer Science and Engineering,

GATTU SANDEEP,
Assistant Professor,
Department of Electronics and Communications Engineering,

Siddhartha Institute of Technology and Sciences,
Narapally, Hyderabad, Telangana – 500 088.

ABSTRACT

The footage acquired by security cameras is crucial for crime prevention and investigation in smart cities. Restricted television cameras (RTC) are critical for a range of public tasks in a smart city; when connected to the Internet of Things, they may morph into smart sensors that help in safety and security. On the other hand, the camera's authenticity raises concerns regarding data integrity and application. In this paper, we present a blockchain-based method for ensuring the integrity of preserved recordings and allowing authorities to check whether or not a video has been tampered with. It can help identify between fake and real recordings, as well as verify the authenticity of security cameras. The distributed ledger of the blockchain also collects the information from the Surveillance camera, which removes the risk of data falsification. This immutable ledger decreases the risk of copyright infringement for law enforcement agencies and clients users by ensuring possession and identification.

INTRODUCTION

To satisfy people's demands for a better quality of life, rapid growth of monitoring systems and services within metropolitan areas was required. Appropriately, the Internet of Things (IoT) industry has experienced a rapid proliferation of digital devices such as smartphones, sensors, smart applications, actuators, and intelligent machines, resulting in obvious economic goals. It is now feasible to connect all nodes throughout the internet and build links between them.

A smart city framework augmented by IoT technology is a game-changing notion, but it also creates new data security concerns. Closed-circuit television (CCTV) cameras have become an indispensable part of a smart city's infrastructure. Blockchain is consuming the globe in large part

as a result of the success of digital money. A blockchain, also known as a distributed ledger, is a write-only data structure that is maintained by a large number of nodes with varying degrees of trust. Several studies make use of blockchain technology as well as image and video processing tools. Deepfake video detection, medical image processing, and picture encryption are some of the techniques used to identify fake videos.

LITERATURE SURVEY

The Privacy Act takes into consideration the installation of CCTV cameras in public locations, which necessitates contacting the CCTV owners for video information. This technique, however, takes a long time. Regardless of how a video is obtained, it is difficult to utilise in open organisations since the film cannot be guaranteed to be original and unaltered. After some pasts, developed a framework that uses cryptographic techniques to corroborate sensor information by developing a log sealing system and producing permanent bits of evidence that may be used for log verification.

The structure ensures that sensor data and log-fixed data can be stored in untrustworthy storage while the suggested verification mechanism ensures their integrity. This structure, however, is dependent on the instrument's dependability; for example, Intel SGX is used to store fixed data in an integrated manner. False news has grown into a global problem that poses serious challenges to human civilization and the majority rule system. This problem has arisen as a result of the advancement of numerous technological wonders.

METHODOLOGY

The proposed method creates a blockchain interface for participants and CCTV nodes. For picture forgery and modulation verification, certain frames of the image are chosen and broadcast via the blockchain network. If all of the continually produced CCTV video frames are recorded in the blockchain, the blockchain transaction becomes too huge, reducing data size and increasing the likelihood of practical application by using only a few frames from each movie. To see if the image is fabricated, several frames are checked.

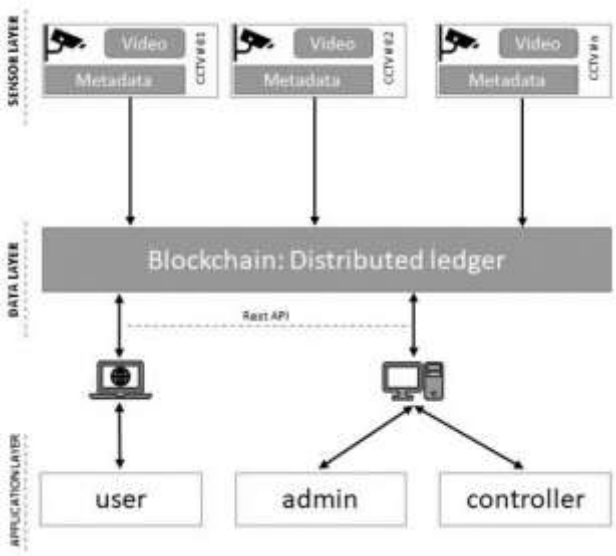

FIGURE 1: BLOCK DIAGRAM

The membership service provider (MSP) is in charge of providing each user with a private key. After issuing the command, it also sends an event notification. a certificate of enrolment An IP video server allows a registered user to create a task. Each and every CCTV With the unique hashed key value, the gadget is connected to the blockchain.

Every node sends out the same message on a regular basis. Along with the video and picture data, metadata will be stored on the blockchain. A blockchain network is a distributed ledger that uses cryptography to keep track of transactions. Validating nodes are provided by the network administrator when the system is configured. Each Before being added to the chain, a block must be approved by an authenticating peer.

RESULT AND DISCUSSION

The procedures required in deciding on a system's viability are included in the cost-benefit analysis. The smart city surveillance equipment industry is growing at a rapid pace. According to some statistics, by 2023, this might amount to 19.5 billion Euros. According to research from Asia, and notably China, is the greatest market for surveillance equipment. China has eight of the top ten most-surveilled cities in the world. Figure 2 depicts the top ten cities in the globe in terms of the number of cameras installed, as well as the cities' safety ratings.

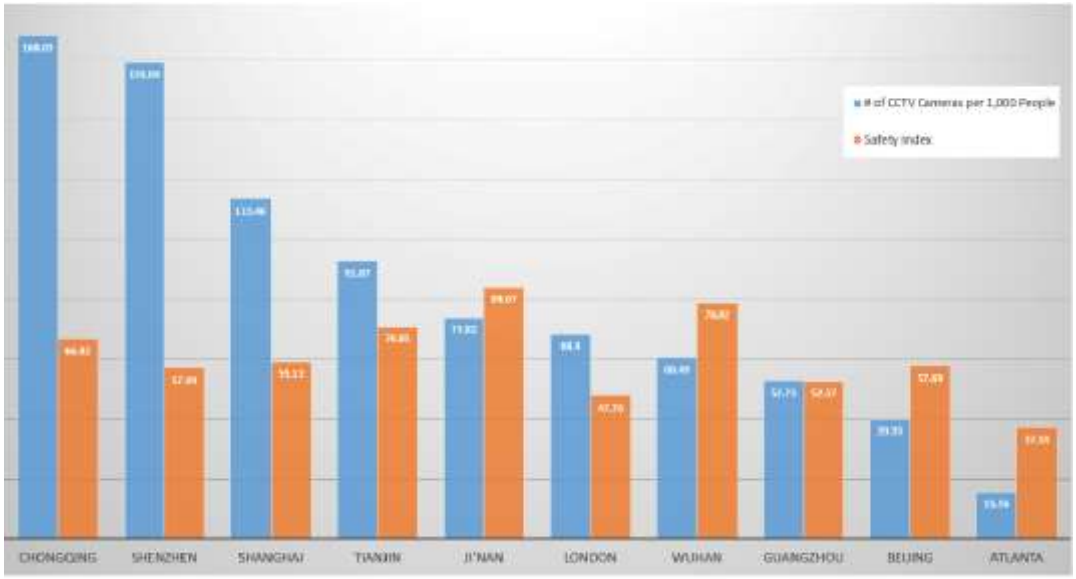

FIGURE 2: COUNTRY BASED SAFETY MEASURES

CONCLUSION

The ideas that underpin smart cities and surveillance technology are inextricably linked. Personal privacy is an issue with CCTV video surveillance equipment. Blockchain technology is a modern answer to challenges of integrity and security. Blockchain technology is appropriate for this application because it ensures data security and is also great for the secure storing of picture data via a distributed ledger. The problem of a huge bandwidth and incentive mechanism, which can be addressed in future study, is one factor that has to be considered.

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)