UTILIZING BLOCKCHAIN TECHNOLOGY, A DATA GENERATION SYSTEM FOR CCTV VIDEO SURVEILLANCE

KRISHNAPUR SANGAMMA,
Assistant Professor,
Department of Computer Science and Engineering,

PADALA PAVAN KUMAR,
Assistant Professor,
Department of Electronics and Communications Engineering,

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

ABSTRACT

In smart cities, the footage captured by security cameras is critical for crime prevention and investigation. In a smart city, closed-circuit television cameras (CCTV) are crucial for a variety of public functions; when linked with Internet of Things (IoT) technology, they may transform into smart sensors that aid in safety and security. The camera's validity, on the other hand, raises questions about data integrity and applicability. We describe a blockchain-based system in this work that ensures the trustworthiness of saved recordings, allowing authorities to verify whether or not a video has been tampered with. It aids in distinguishing between fraudulent and genuine videos, as well as ensuring that security cameras are genuine. Because the blockchain's distributed ledger also captures the information of the CCTV video, it eliminates the possibility of data fabrication. By guaranteeing possession and identification, this immutable ledger reduces the risk of copyright infringement for law enforcement agencies and clients users.

INTRODUCTION

The rapid development of surveillance systems within urban regions and services was necessary to meet people's needs for a higher quality of life. Appropriately, the Internet of Things (IoT) market has seen a spectacular expansion of digital devices, such as smartphones, sensors, smart apps, actuators, and intelligent machines, which has led to clear commercial goals. It is now possible to link all nodes over the internet and construct connections between them. Because of the advancement of computer-aided technology, the smart city is becoming more intelligent than in the past. Smart cities use a variety of electronic applications, such as cameras in an observation

system and sensors in a transportation system. A smart city framework enhanced by IoT technology becomes a revolutionary concept, but it also raises new issues about data security. Closed-circuit television (CCTV) cameras have become a necessary component of a smart city. To a large part, blockchain is engulfing the globe 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 that do not completely trust one another. Blockchain and image and video processing techniques are used in several investigations. Deepfake video detection , medical image processing , picture encryption, and digital content rights management are some of the applications.

LITERATURE SURVEY

Smart Cities are typically represented as confusing systems structured in light, and are generally classified as networks of associated gadgets and their environment. Interdependencies in terms of resources highlighted four critical components in order of importance. Which are included in this ecosystem's notion of a smart city Interaction or involvement, balance, and Self-organization, loosely coupled actors with common aims, and ultimately, loosely coupled actors with shared objectives. IoT devices come in a variety of shapes and sizes. To cope with current computer devices, memory and computational complexity are required. a scarcity of They are unprotected against a wide range of cyber assaults due to their computing capacity.

METHODOLOGY

For the authentication and verification of data for smart cities, we employed the blockchain platform. We go over the flow of the proposed platform and its components in depth in this part. The flow of our suggested model is depicted in Figure 1. It all starts with user registration and device registration. Every peer in the system is given a unique key by the membership service provider (MSP). We're employing a private blockchain called Hyperledger Fabric, which differs from public blockchains in terms of user access. Any user can join a public blockchain, but only legitimate users with the private key provided 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 block after encryption, and each block is supported by endorsing peers. There is no consensus algorithm or block mining in Hyperledger Fabric. However, validation peers are nominated by the system administrator to suit the validation objective. The valid usage can send calls to the REST API to get access to the blockchain's digital data.

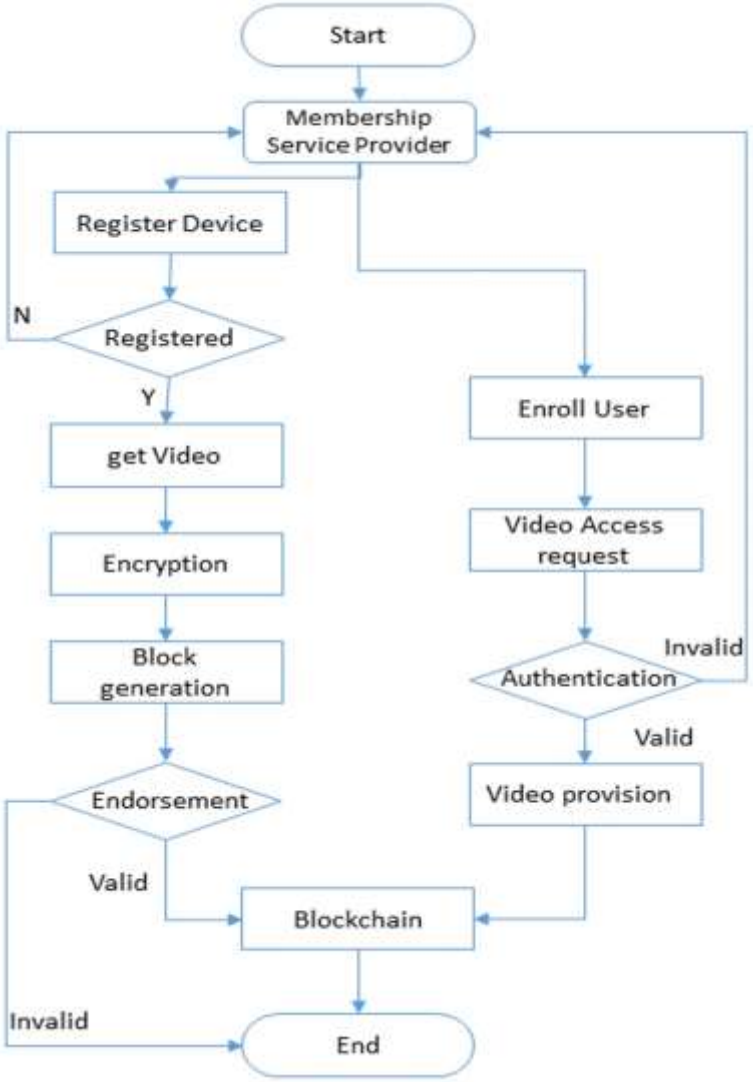
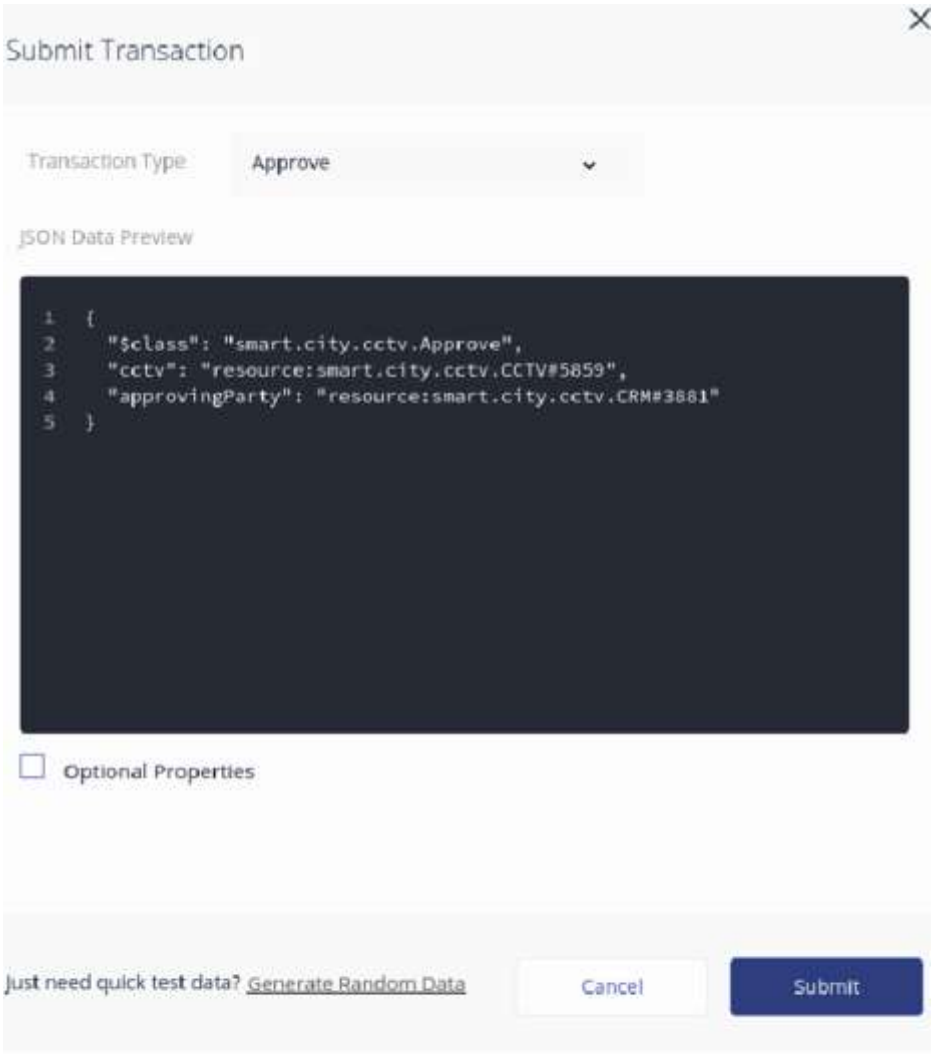


FIGURE 1: WORK FLOW

RESULT AND DISCUSSION

Every certified participant of the proposed network can start a new transaction based on the rules defined in smart contracts. After successfully executing the transaction, smart contracts generate a response to the participant.



(a) Approval transaction

CONCLUSION

In this paper, we present a blockchain-based method for ensuring the integrity of preserved recordings, allowing authorities to determine whether or not a video has been tampered with. It assists in the identification of fake and real movies, as well as the verification of security cameras. 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. Talari, S.; Shafie-Khah, M.; Siano, P.; Loia, V.; Tommasetti, A.; Catalão, J.P. A review of smart cities based on the internet of things concept. Energies 2017, 10, 421.
2. Wu, T.Y.; Fan, X.; Wang, K.H.; Lai, C.F.; Xiong, N.; Wu, J.M.T. A DNA Computation-Based Image Encryption Scheme for Cloud CCTV Systems. IEEE Access 2019, 7, 181434–181443.

3. Li, Y.; Lyu, S. Exposing deepfake videos by detecting face warping artifacts. arXiv 2018, arXiv:1811.00656.
4. Ravi, H.; Subramanyam, A.V.; Gupta, G.; Kumar, B.A. Compression noise based video forgery detection. In Proceedings of the 2014 IEEE International Conference on Image Processing (ICIP), Paris, France, 27–30 October 2014; pp. 5352–5356.
5. Hasan, H.R.; Salah, K. Combating deepfake videos using blockchain and smart contracts. IEEE Access 2019, 7, 41596–41606.
6. Shen, M.; Deng, Y.; Zhu, L.; Du, X.; Guizani, N. Privacy-preserving image retrieval for medical iot systems: A blockchain-based approach. IEEE Netw. 2019, 33, 27–33.
7. Khan, P.W.; Byun, Y. A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things. Entropy 2020, 22, 175.
8. Ma, Z.; Jiang, M.; Gao, H.; Wang, Z. Blockchain for digital rights management. Future Gener. Comput. Syst. 2018, 89, 746–764.
9. Gipp, B.; Kosti, J.; Breitinger, C. Securing Video Integrity Using Decentralized Trusted Timestamping on the Bitcoin Blockchain; MCIS: Selangor, Malaysia, 2016; p. 51. 10. Lee, J.H. BIDaaS: Blockchain based ID as a service. IEEE Access 2017, 6, 2274–2278.