BLOCKCHAIN BASED VIDEO ANALYSIS

KIRANMAI KOSANAM,
Assistant Professor,
Department of Computer Science and Engineering,

NAFIZA SYED,
Associate 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. Closed-circuit television cameras (CCTV) are critical for a range of public tasks in a smart city; when connected to the Internet of Things (IoT), 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.

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.

LITERATURE SURVEY

In the realm of video forensics, a lot of work has been done. As a result of this innovation, video evidence may now be utilised in court trials. An autoencoder with recurrent convolutional neural networks, an auto-encoder with a goturn algorithm, watermarking techniques, and digital signatures are among the most recent approaches utilised for video forgery detection. To identify video counterfeiting, the reference presented an architecture based on autoencoders and recurrent neural networks. To exploit dependencies, they developed a long short-term memory (LSTM) model. proposes a model that uses an auto-encoder and a goturn algorithm to determine the trustworthiness of digital videos. In addition, a variety of factors call into question the reliability of video data captured by CCTV.

CCTV-based administrations, on the other hand, are being strengthened and varied. The credibility of a picture in order to provide proper guidance. 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.

METHODOLOGY

A blockchain is a distributed system that simulates a central computer function and is run by nodes linked across the Internet. In theory, the blockchain is replacing centralised ledger systems with decentralised ledgers. A blockchain relies on encryption techniques and does not require a third party, making it trustworthy. A blockchain is made up of a series of data blocks linked together. Entries are changeless, transparent, and accessible, and blocks may be created and read by specified members.

On a constantly growing database, transactions are recorded in chronological order. Over the framework, information is replicated and stored on a shared system. It promotes the exchange of considerable value without the need of a central mediator.

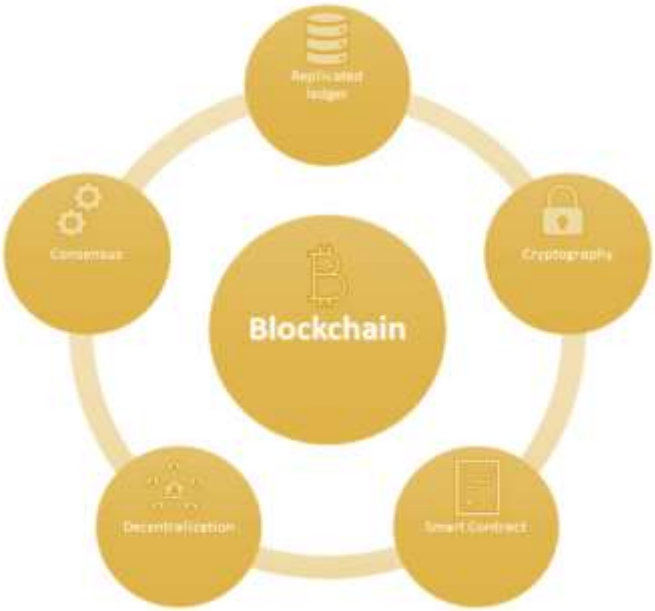

FIGURE 1: BLOCK CHAIN FLOW

Hyperledger Fabric is a distributed ledger technology for private blockchains that is open source. It has a lot of scalability and has been utilised in a lot of different sectors. Blockchain technology is expected to have enormous potential for delivering dramatic changes to a wide range of businesses, business models, and working methods, such as installation, bookkeeping, and inspection. Because of its specialised, complex character and the necessity to acknowledge these broad changes in the private, public, and commercial sectors, this breakthrough, like other disruptive innovations before it, will take time to catch on with a steady increase in speed throughout time.

RESULT AND DISCUSSION

Model, query definition, script, and access control rules are the four elements that make up a hyperledger smart contract. Between LevelDB and CouchDB, Hyperledger Fabric allows for the use of state databases dependent on data type. Core chaincode transactions are supported by these two databases. The default state database is LevelDB, which is used to save smart contract data as a key-value pair. It's built right into the system's peer node.

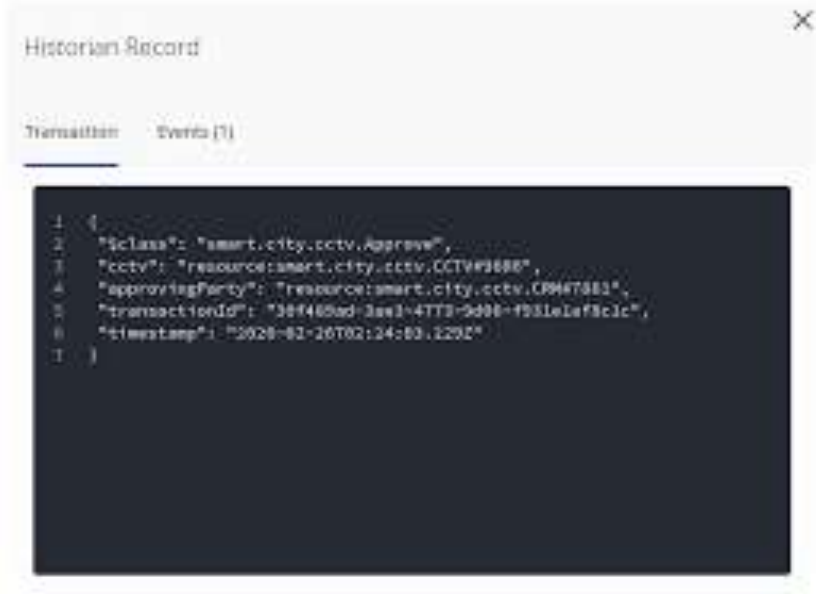

FIGURE 2: TRANSCATION RECORD

CONCLUSION

The distributed ledger of the blockchain also collects the information from the CCTV 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. This application is well-suited to blockchain technology since it assures data security and allows for the safe storage of image data via a distributed ledger. One thing to examine is the difficulty of a large bandwidth and incentive mechanism, which can be addressed in a future study.

REFERENCES

1. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
2. S.H.; Faghri, F.; Campbell, R.H. Decentralized user-centric access control using pubsub over blockchain. arXiv 2017, arXiv:1710.00110.
3. Kiyomoto, S.; Rahman, M.S.; Basu, A. On blockchain-based anonymized dataset distribution platform. In Proceedings of the 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA), London, UK, 7–9 June 2017; pp. 85–92.

4. Danzi, P.; Angjelichinoski, M.; Stefanovi´c, C.; Popovski, P. Distributed proportional-fairness control in microgrids via blockchain smart contracts. In Proceedings of the 2017 IEEE International Conference onSmart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 45–51.
5. Sikorski, J.J.; Haughton, J.; Kraft, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. Appl. Energy 2017, 195, 234–246.
6. Sharma, P.K.; Moon, S.Y.; Park, J.H. Block-VN: A distributed Blockchain based vehicular network architecture in smart city. J. Inf. Process. Syst. 2017, 13.