Enhancing Privacy Protection in Intelligent Surveillance: Video Blockchain Solutions

Kasun Moolika Gedara, Minh Nguyen, Wei Qi Yan

Auckland University of Technology, Auckland, New Zealand
e-mail: Kasun.moolikagedara@autuni.ac.nz

Abstract. Blockchain has emerged as a contemporary innovation that ensures secure operations in distributed networks, including decentralized applications, finance, logistics, and cross-border organizational control. In this paper, we introduce "Video Blockchain" as a novel method to store and manage visual data in smart cities, due to the lack of tamper resistance in existing systems. A relationship is established between video frames from surveillance videos and blockchain technology, integrating the visual data into a decentralized storage platform. A unique approach is leveraged to extract hash values and signatures from video blockchains using cryptographic functions, thereby enhancing surveillance data security. A decentralized blockchain prototype was developed, and appropriate cryptographic algorithms were selected to create a sustainable video blockchain. The contributions of this research project are to enhance blockchain security and minimize privacy-preserving gaps in intelligent surveillance, which lead to more secure, robust and reliable surveillance systems for smart cities.

Keywords: Video Blockchain · Cryptography · Intelligent Surveillance · Smart Cities.

1 Introduction

Blockchain was introduced in 2009 and has been employed in large-scale businesses across industries such as global trade, insurance, finance, distributed energy, and healthcare. It allows for transactions and processes to occur without the involvement of third parties, effectively solving complications related to data integrity and verification in the areas such as medical records, electricity, and gas systems in smart cities [4,6,7].

As smart cities become more complex and the technologies are more integrated, the idea "smart cities" has gained traction worldwide ,with a focus on improving safety and security for citizens while reducing crimes and accidentsClick or tap here to enter text.. Surveillance systems are an integral part of this need, but traditional mechanisms such as centralized client-server methods and network security measures do not always satisfy the necessary requirements [18].

One critical aspect of data storage in smart cities is privacy.With sensitive data being transmitted and stored on blockchains, there is a need to protect the privacy of citizens .Therefore, privacy-preserving techniques need to be employed so as to ensure that personal data remains confidential and secure[20].

Fortunately, blockchain technology provides an ideal platform for privacy-preserving data storage. For example, zero-knowledge proofs can be harnessed to enable secure transactions without revealing the actual data being transferred. Additionally, homomorphic encryption can be accommodated to encrypt data while still allowing computations to be performed on it without the need for decryption by incorporating privacy-preserving methods into the blockchain-based surveillance system, the smart city can ensure that the privacy and security of its citizens are adequately protected. This, in turn, will foster greater trust and confidence in the system, leading to its wider adoption and success[9].

In this paper, our aim is to find a solution for selecting the best cryptographic functionalities, combining privacy-preserving data storage - one of the main limitations in blockchain implementations - and enhancing the immutability of the blockchain to provide a secure mechanism for video surveillance in smart cities. Overall, our research aim is to contribute to the development of a new method of video blockchain for securing surveillance data in a smart city, which can improve the efficiency, effectiveness, and security of surveillance systems.

2 Background and Related Work

Securing surveillance [5] is a crucial way to face detection, human behaviour analysis and traffic rule violation detection. These tools have shown plenty of contributions in notably preventing crimes, anomalous incidents, and privacy policy violations.Also our previous works [10,16,17,26,27,28] related to blockchain and computer vision lead to enhance the more robust method to address the malicious attackers and hackers can illegally manipulate video repositories and surveillance cameras, thereby rendering the recorded footage unusable in criminal cases. To prevent tampering and attacks [12], Blockchain is employed as a solution to handle a diversity of attacks that occur within surveillance systems. For instance, attackers may manipulate or tamper with video footage, which leads to compromised integrity.

Tamper-resistant and immutability of blockchain were employed to protect stored data and ensure data integrity. Hashing is a reliable method for creating confidentiality between two blocks in the chain [8]. Cryptographic hash functions convert confidential data into a random string having a size, security requirements of one-witness and collision-resistance are necessary. Various blockchain-based systems have been proposed, such as the BlockSee method [9], which provides validation and immutability to surveillance videos.

Moreover, research trends in intelligent surveillance and blockchain include the use of dashboard cameras mounted on vehicles to capture vehicle accidents in smart cities ,connected IoT devices and monitor air and water quality[13,14], as well as food delivery tracking [19]. Decentralization, filtering, and privacy features of blockchain are applied to ensure the authenticity, time-lapse features are employed to transfer unmodified data to a shared repository.

The uniqueness of blockchain methods makes it suitable for large-scale industries such as global trade, insurance, banking, distributed energy, and healthcare.

Blockchains have been adapted to smart transportation systems, food supplier management, government, identity verification, and smart cities. The blockchain's ability to solve problems related to data integrity has been offered in medical record verification systems and intelligent gas monitoring systems [2].

To develop a computational method of video blockchain for intelligent surveillance in smart cities, [7] selecting cryptographic functions is an effective method for connecting surveillance videos and blockchains to enhance the resistant against different kinds of attacks that can improve digital surveillance systems, the design of combining different algorithms together and implementing new methods is effective, as a slew of attacks have been identified based on the existing blockchain platform [1,22].

Blockchain proves to be an effective tool for securing surveillance and ensuring data integrity in intelligent surveillance. Its tamper-resistant and immutable nature protects stored data from malicious hackers. However, the development of new methods and the integration of different algorithms to enhance resistance against attacks on existing blockchain platforms must continue. Emphasizing the importance of selecting appropriate cryptographic functions and implementing new methods is crucial to improve the privacy of blockchain-based systems in the realm of intelligent surveillance.

3 Our Proposed Solutions

An effective method for connecting blockchain function can be identified by analysing recent findings of blockchain. According to [25] myriads attacks on the blockchain platform have been reported, in order to avoid these identified and unidentified attacks, the design of combining different algorithms together and implementing a new method can enhance resistance against multiple kinds of attacks that can happen to surveillance systems recorded data repositories.

3.1 The best cryptographic functions to implement a video blockchain

Choosing the right cryptographic function is crucial for a secure and efficient video blockchain system. It must provide strong security guarantees against attacks, with options like SHA-256, SHA-3, and BLAKE2 [8] being commonly used for blockchain applications. Efficiency is also key, optimizing the function's performance on the specific hardware and software architecture of the blockchain network. Compatibility is another consideration, ensuring seamless integration and interoperability with the existing blockchain infrastructure. For instance, using Ethereum-compatible cryptographic functions like Keccak-256 or SHA-3 [14] is recommended for a video blockchain built on Ethereum.

In this paper, we choose cryptographic features and take advantage of the proposed combination to create a robust mechanism for a blockchain-based computing solution. One of the most important requirements for establishing a blockchain application solution is to ensure data integrity and confidentiality. We have also explored the

methods such as Merkel tree [16], hash list [24], H-tree [20] and SM-Tree [3] methods. After comparing different technologies, we will determine which one is most suitable for the required level of security.

The method [2] of creating a blockchain solution for the Dubai government will be employed for comparative analysis of blockchain industrial solutions. According to previous research work [11] the requirements for choosing cryptographic functions and algorithms for scalability. Moreover, energy consumption is a significant consideration for blockchain-based implementations, it is crucial to find the best algorithm that meets these requirements. Overall, the integration of selected solutions requires an in-depth investigation to build a strong and reliable computer approach. This will assist us to deliver a secure solution for intelligent surveillance in smart cities. Table 1 shows the comparisons of our selected algorithms for blockchain.

Table 1. The comparisons between conventional databases.

Characteristics	**Algorithms / Methosd**	**Conventional Databases**
Authority	Decentralized	Centralized
Architecture	Peer-to-peer model	Client-server model
Performance	Relatively slow	Fast
Cost	Costly	Cheap
Data Handling	Only read and write	Create, Read, Update, Delete
Data Integrity	Has data integrity	Doesn't have data integrity
Transparency	Transparent	Non-transparent
Cryptography	Yes	No

we selected our proposed method. First, identify the most suitable algorithm from Table 1. Assess new trends and gaps in the selected methods to construct an effective and efficient solution. Additionally, connect the algorithms to design computational methods for video blockchain.

3.2 Solution for privacy preserving over the blockchain

The proposed method for enhancing surveillance data integrity in smart cities involves using a Merkle tree, hashing function, and peer-to-peer data storage. The verification process detects changes in image frame order and identifies the specific image modifications. A Merkle tree is generated for each block, and its root is stored in the blockchain to ensure integrity. The experimental design utilizes selected cryptographic algorithms, generating output from video frames to validate the blockchain implementation. An interface is designed to test functionality and address video frame-related issues.

The solution emphasizes lightweight functions for inter-block communication to enhance security and prevent attacks like man-in-the-middle interception. Selected cryptographic features create a robust mechanism for blockchain-based computing. The

initial computational method incorporates connection hashing and block matrix functions for video blockchain, bridging gaps between frames and improving security. However, adversaries may still estimate the amount of legal data, even with blocked public information equity for verification rate, hash value, and sibling path size.

For experimental analysis, multiple datasets with sample videos were created to be loaded into the system. The surveillance videos, usually recorded at 25 fps, were increased to 30 fps in this project to include more content in the experiments. Using a Samsung S7 (G930F) smartphone, our own dataset of 7,000 video frames was created, focusing on the Auckland city. The objective of this research is to generate hash values for video frames, enhancing resistance against potential attacks.

This paper establishes a connection between surveillance video footage and blockchains, storing the data in a decentralized repository. The main contribution is enhancing the security of observational data through the use of cryptographic algorithms for hashing and signature, distinguishing it from other works. These algorithms ensure accurate connection of video frames and enable detection and location of any frame changes. The verification procedure, using Merkle trees and hashing functions, further strengthens the security measures.

Privacy-preserving problem exists in blockchain implementation [15]. We propose a blockchain-based solution for ensuring and improving the integrity of surveillance data in smart cities, aiming for increased loyalty, reliable results, and controlled disclosures. Combining computational approaches and video blockchain regulates data security, reducing unauthorized access. This enables close monitoring of law enforcement, insurance firms, and traffic management systems, facilitating necessary modifications for improved security and compliance in smart city video surveillance.

To verify frame integrity, a Merkle tree is constructed from the block matrix hash values. The Merkle tree's root hash is stored in the blockchain, allowing detection of any modifications by comparing block and Merkle tree hashes. This tamper-resistant approach enhances system security.

In addition, block matrix operations [21], such as matrix multiplication and matrix inverse, can be employed for video processing tasks, such as compression, filtering, and restoration. These operations can be performed on the block matrices stored in the blockchain, which allows for highly efficient and secure video processing.

Overall, storing video frames in a blockchain-based system using block matrices provides a secure and efficient method for video storage. The use of hash values, Merkle trees, and block matrix operations enhances the tamper-resistance, integrity, and reliability of the system.

In this implementation, the Merkle Tree function takes in an array of data and recursively constructs a Merkle tree. In the base case (when there is only one data item left), the function returns the data item itself. Otherwise, it recursively constructs the left and right subtrees, hashes them together using SHA-256 algorithm, and returns the resulting hash. The resultant hash is the root of Merkle tree.

Algorithm 1: Merkle Tree

Input: A list of data blocks.

1) Divide the data blocks into fixed-size chunks (usually 1-2KB).

2) Compute the hash of each data chunk using a cryptographic hash function.
3) Pair up adjacent data chunk hashes and compute the hash of each pair.
4) Repeat step 4 until there is only one hash left, which is the Merkle root hash.
5) Store the Merkle root hash as the identifier of the data blocks.

Algorithm 2: Block Matrix

Input: A video file consisting of frames.

1) Divide each frame into fixed-size blocks (16x16 pixels).
2) Store the blocks of each frame in a matrix, where each row represents a block, and each column represents a frame.
3) Apply compression algorithms (JPEG) to each block to reduce the amount of data.
4) Store the compressed block matrix as a binary file.
5) To access a specific frame, load the compressed block matrix and retrieve the corresponding column of blocks.
6) To access a specific block within a frame, retrieve the corresponding row of the block matrix and decompress the block.

The block matrix function takes in an array of data and a block size, and constructs a matrix where each row represents a block of data. The matrix is filled in by iterating over the data array, slicing it into blocks of the given size, and placing each block in the appropriate row of the matrix. If the length of the data array is not a multiple of the block size, the last row of the matrix will contain padding to fill out the remaining space.

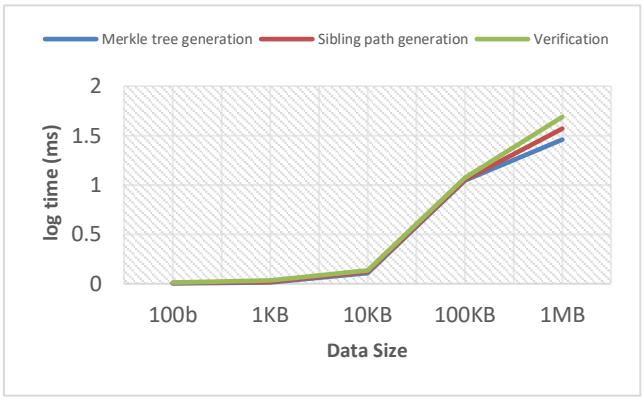

Fig.1. Average computational time (millisecond) for authentication based on Merkle tree by data size.

Together, these algorithms can be employed to store video frame data in a secure and efficient manner. The video frames can be split into blocks, and a Merkle tree can be constructed over the blocks to provide integrity and authentication for the data. This

method supports the distributed storage facility to be store data transferring from the surveillance systems.

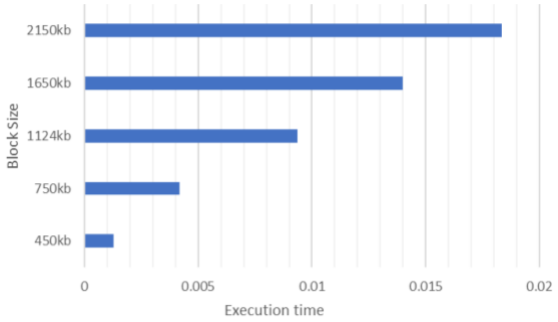

Fig.2. Computational time for different input sizes and block sizes.

4 Result analysis and Discussion

This project aims to explore the use of video blockchain for surveillance systems. The method includes converting recorded videos into video frames, each frame has 50KB~1024KB, which was employed to implement a private blockchain system based on a Windows 11 64-bit operating system; an experimental setup was conducted to test the effectiveness of the newly proposed method against various attacks. The experimental results in the creation of new computational methods of video blockchains, integrating selected cryptographic algorithms and video blockchains together. Overall, this research provides a technological contribution to the field of video blockchain, as it presents a new method of securing video data for surveillance systems. The findings of this research project can be offered as a foundation for future work in video blockchain and cryptographic algorithms.

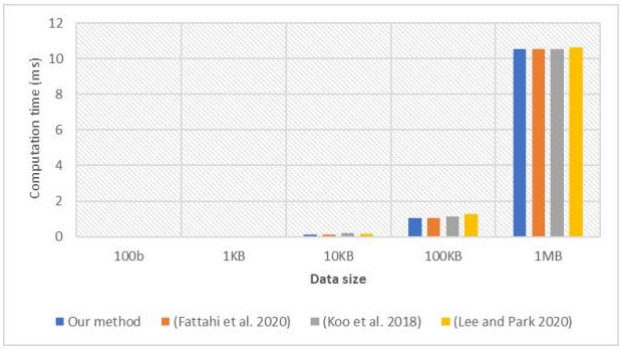

Fig.3. Comparisons of computational time between ours and other similar projects

Each root structure in the Merkle tree guarantees the connection between video frames and hashing order, preventing changes to the order of images without changing the entire root structure of the tree. Our future work aims to add a real-time change

detection feature to the implementation, enhance its reliability and resistance against privacy-pervasive and quantum computer attacks. Overall, the result provides insights into the development of web interfaces for video blockchain systems, and its findings can be utilized to enhance the reliability and security of such systems in the future.

In this paper, we focus on Merkle tree-based approaches for data verification. The evaluation was conducted by measuring the computational time and data size of each experiment, with each experiment being repeated 100 times to minimize errors caused by outliers.

Figure 1 shows an upward trend in computational time related to the increase in data size for the three Merkle tree-based approaches. However, after 100KB of data, these approaches exhibit only a slight difference, as generating a Merkle tree for a 1 MB data file accounts for 99.9% of the computational time required by the prover. We plot the results to determine the time complexity. The time is subject to different input sizes and block sizes, this results in determining the function's time complexity.

In Fig.2, the computational time on *y*-axis and the input size or block size on *x*-axis for different input sizes or block sizes to compare the performance of the function. In Fig.3, we compare the computation time and data size metrics of the study with those of other similar works. The results show a significant change with the data size 100KB, which indicates that the study's outcomes are comparatively reliable. These findings can be applied to improve the efficiency and accuracy of Merkle tree-based approaches for data verification.

The use of blockchain technology in intelligent surveillance faces a many of challenges such as scalability, interoperability, and regulatory compliance. Scaling blockchain to handle large volumes of data and transactions, integrating it with the existing systems, and navigating regulatory frameworks are crucial issues. In our future work, we will plan to solve these problems.

5 Conclusion and Future Work

In this project, our primary objective is to establish the relationship between video frames captured by intelligent surveillance systems and blockchain, integrating the data into a decentralized storage platform for video surveillance. Our approach is distinct from the existing studies as it leverages cryptographic functions to extract hash values and signatures from video blockchains, thereby augmenting the security of surveillance data. Furthermore, this research work primarily targets the enhancement of tamper-resistant data storage within surveillance systems rather than focusing on mitigating the risks posed by considering quantum computer attacks on blockchains. Nevertheless, in future, we will explore the solutions outlined in Section 3.2 to bolster the resilience of blockchains against quantum threats. Privacy concern is one of the main problems in blockchain implementation. However, in the future, there is a need to further address limitations of scalability, interoperability, and regulatory issues.

This research aims to propose a blockchain-based approach that enhances the security and integrity of surveillance data while fostering significant levels of trust, reliability, and controlled disclosure in smart cities. By integrating computer vision

with video blockchain, we concentrate on fortifying the security of surveillance data, offering a solution that deters tampering and unauthorized access by external parties. The contributions of this project pave the way for necessary advancements to achieve heightened security and adaptability for video surveillance in smart urban environments.

References

1. Aldairi, A., Tawalbeh, L.: Cyber security attacks on smart cities and associated mobile technologies. Procedia Comput Sci. 109, 1086–1091 (2017).
2. Alketbi, A., Nasir, Q., Abu Talib, M.: Novel blockchain reference model for government services: Dubai government case study. International Journal of Systems Assurance Engineering and Management. 11, 1170–1191 (2020).
3. Becker, G.: Merkle Signature Schemes, Merkle Trees and Their Cryptanalysis. Master's Thesis. Seminararbeit Ruhr-Universit¨at Bochum. (2008)
4. Chen, X., Xing, Z., Karki, B., Li, Y., Chen, Z.: Blockchain simulation: A web application for IT education. Annual Computing and Communication Workshop and Conference (CCWC), 486–491 (2021).
5. Deepak, K., Badiger, A.N., Akshay, J., Awomi, K.A., Deepak, G., Harish Kumar, N.: Blockchain-based management of video surveillance systems: A survey. International Conference on Advanced Computing and Communication Systems (ICACCS), 1256–1258 (2020).
6. Engelhardt, M.A.: Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. Technology Innovation Management Review, 7, 22–34 (2017).
7. Fill, H., Haerer, F.: Knowledge blockchains: Applying blockchain technologies to enterprise modelling. Hawaii International Conference on System Sciences, 4045–4054 (2018).
8. Fu, J., Qiao, S., Huang, Y., Si, X., Li, B., Yuan, C.: A study on the optimization of blockchain hashing algorithm based on PRCA. Security and Communication Networks (2020).
9. Gallo, P., Pongnumkul, S., Nguyen, U.Q.: BlockSee: Blockchain for IoT video surveillance in smart cities. IEEE International Conference on Environment and Electrical Engineering and IEEE Industrial and Commercial Power Systems Europe (EEEIC/I and CPS), (2018).
10. Gedara, K., Nguyen, M., Yan, W.: Visual blockchain for intelligent surveillance in a smart city. Blockchain Technologies for Sustainable Development in Smart Cities, IGI Global. (2021) .
11. George, R.V., Harsh, H.O., Ray, P., Babu, A.K.: Food quality traceability prototype for restaurants using blockchain and food quality data index. Journal of Clean Prod. 240, (2019).
12. Gergely, A.M., Crainicu, B.: Randadminsuite: A new privacy-enhancing solution for private blockchains. Procedia Manuf. 46, 562–569 (2020).

13. Gřivna, T., Drápal, J.: Attacks on the confidentiality, integrity and availability of data and computer systems in the criminal case law of the Czech Republic. Digit Investig., 28, 1–13 (2019).
14. Hartwig, M.: ECDSA security in bitcoin and Ethereum: A research survey. Blog. Coinfabrik, 1–10 (2016).
15. Hasan, O., Brunie, L., Bertino, E.: Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey. ACM Computing Surveys, 55(2): 1-37 (2023).
16. Hu, R.: Visual Blockchain Using Merkle Tree. Master's Thesis, Auckland University of Technology, New Zealand (2019)
17. Hu, R., Yan, W.: Design and implementation of visual blockchain with Merkle tree. Handbook of Research on Multimedia Cyber Security, 282-295, IGI Global (2020)
18. Khan, P.W., Byun, Y.C., Park, N.: A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. Electronics (Switzerland). 9, (2020).
19. Khan, M.A., Salah, K.: IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411 (2018).
20. Koo, D., Shin, Y., Yun, J., Hur, J.: Improving security and reliability in Merkle tree-based online data authentication with leakage resilience. Applied Sciences (Switzerland), 8, (2018).
21. Kumar, M., Kaur, G.: High performance scalable recursive block matrix inverse for multicore architectures. International Conference on Parallel, Distributed and Grid Computing, pp. 45–49 (2022).
22. Li, T., Chen, Y., Wang, Y., Wang, Y., Zhao, M., Zhu, H., Tian, Y., Yu, X., Yang, Y.: Rational protocols and attacks in blockchain system. Security and Communication Networks (2020).
23. Majdoubi, D.E.L., El Bakkali, H., Sadki, S.: Towards smart blockchain-based system for privacy and security in a smart city environment. International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech), (2020).
24. Michael, M.M.: High performance dynamic lock-free hash tables and list-based sets. Annual ACM Symposium on Parallel Algorithms and Architectures. 73–82 (2002).
25. Mosakheil, J.H.: Security threats classification in blockchains. Culminating Projects in Information Assurance. 141 (2018).
26. Shu, Y.: Blockchain for Security of a Cloud-based Online Auction System. Master's Thesis, Auckland University of Technology, New Zealand (2018).
27. Shu, Y., Yu, J., Yan, W.: Blockchain for security of a cloud-based online auction system. Exploring Security in Software Architecture and Design, 189-210, IGI Global (2019)
28. Shu, Y., Yu, J., Yan, W.: Blockchain for security of cloud-based online auction. Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government, IGI Global (2021)
29. Yan, W.: Introduction to Intelligent Surveillance: Surveillance Data Capture, Transmission, and Analytics. Springer (2019)