electronics

MDPI

Type of the Paper (Article)

Advancing Video Data Privacy in IoT Networks through Video Blockchain Technology

Kasun Moolikagedara [1]*, Minh Nguyen [2] and Wei Qi Yan [2,]*

School of Engineering, Computer and Mathematical Sciences, Auckland University of Technology, Auckland 1010 New Zealand

* Correspondence: kasun.moolikagedara@aut.ac.nz

Abstract: In the age of ubiquitous Internet of Things (IoT) devices, data privacy concerns have grown exponentially. This article examines the nexus of video data privacy and blockchain technology within IoT networks, aiming to devise innovative strategies leveraging video blockchain's attributes to enhance security and privacy for IoT-generated video data. A comprehensive literature review reveals the multifaceted challenges encompassing data privacy in IoT, spanning issues of data integrity, confidentiality, and trust. Recognizing blockchain's inherent immutability and decentralization, this research methodically investigates existing blockchain-based approaches and substantiates their practical implementation's tangible benefits in reinforcing video data privacy within the dynamic IoT landscape. The ensuing discussion critically evaluates these findings, emphasizing the strengths and limitations of video blockchain-based solutions within the IoT context. It underscores blockchain's transformative potential as a cornerstone for preserving data privacy in IoT ecosystems, instilling trust and security amid pervasive connectivity. In conclusion, the research highlights blockchain's significance as a catalyst for advanced data privacy, particularly concerning video content within the intricate IoT networks. As IoT applications continue to proliferate, integrating blockchain technology emerges as a promising avenue to secure sensitive video data, ultimately promoting trust and security in our evolving digital landscape. The article also looks ahead, emphasizing the need for continued exploration of innovative solutions in this ever-relevant field.

Keywords: Video Blockchain; IoT Network; Video Data Privacy

Citation: To be added by editorial staff during production.

Academic Editor: Firstname Lastname

Received: date
Revised: date
Accepted: date
Published: date

1. Introduction

In today's modern world, Internet of Things (IoT) devices have become indispensable tools in our daily lives. They play a pivotal role in simplifying tasks and providing solutions across a wide spectrum of applications. However, the proliferation of IoT devices has ushered in a new era in which our personal data is intimately entwined with these interconnected technologies. This integration has given rise to growing concerns about privacy, particularly regarding the unauthorized sharing of personal data with third parties [1]. Among the data captured by IoT devices, video data stands out as a high-risk category with significant implications for user privacy. The visual nature of video data presents unique challenges and vulnerabilities, making it particularly sensitive in the context of IoT [2]

As we embark on this exploration of data privacy in IoT networks, we introduce three central hypotheses that guide our research:

Hypothesis 1: The selecting appropriate cryptographic functions for connect the IoT network and video blockchain implementation.

Hypothesis 2: The integration of video blockchain technology into IoT networks will significantly enhance the security and privacy of video data, leading to improved data integrity, confidentiality, and trust within the interconnected ecosystem.

Hypothesis 3: Video blockchain technology will demonstrate its practical utility and effectiveness in safeguarding video data privacy in IoT networks.

The purpose of this study is to investigate these hypotheses and address the pressing issue of data privacy within IoT networks. To contextualize our research, we will review the current state of the field, highlighting the challenges and controversies related to IoT data privacy. Additionally, we will provide an overview of key publications that have contributed to the discourse on data privacy within IoT networks. By examining the current landscape, we will lay the foundation for the hypotheses and experimental analysis presented in this paper.

In assumption, this study underscores the compelling importance of blockchain technology as a catalyst for enhancing data privacy, particularly in the context of video data, within the intricate web of IoT networks. As IoT applications continue to rapidly proliferate, the integration of blockchain technology offers a promising solution to address the critical issue of data privacy, ultimately fostering trust and security in our interconnected world. We aim to provide insights that transcend disciplinary boundaries, making our findings comprehensible to scientists and researchers outside the specific field of IoT and data privacy.

2. Materials and Methods

In this section consequently address the hypothesis using relevant methodologies, while extracting related methods and comparatively analysis our employed methods to achieve the necessary results and implement a secure IoT network for transmitting video data securely.

2.1 Evaluating the Performance of Existing Hashing Functions

In the context of "Advancing Video Data Privacy in IoT Networks through Video Blockchain Technology," the choice of cryptographic functions is paramount for establishing a secure and efficient video blockchain system. In this paper not going to extract the all of the cryptographic function related to the video blockchain implementation, moreover it only discussed the chosen main hashing functions that most commonly using in the blockchain application.[3, 4]. Because here we want to test the upgrade version of Secure Hashing algorithm(SHA).

Therefore, these functions must offer robust security measures against potential attacks, with commonly used options including SHA-256 and SHA-3 [5] specifically tailored for blockchain applications [6]. Efficiency is another critical factor, necessitating optimization of the function's performance to align with the unique hardware and software architecture [7]of the blockchain network. Moreover, ensuring compatibility is essential to guarantee smooth integration and interoperability with the existing blockchain infrastructure. For instance, in the case of a video blockchain built on the Ethereum platform, it is advisable to employ Ethereum-compatible cryptographic functions such as Keccak-256 or SHA-3 [14].

The performance of both SHA-256 and SHA-3 hashing is assessed through the utilization of a Python script designed for benchmarking. The script is responsible for determining the average time required to execute SHA-256 hashing on a designated sample data string. To ensure precision, the script iterates through the hashing process 1000 times, resulting in a more precise measurement. Subsequently, the calculated average time for SHA-256 hashing is presented for analysis. Below algorithm 1 explain the process of performance measuring our selected hashing functions of SHA-3 and SHA-256

Algorithm 1: Used for Performance Evaluation

Input: Data to be hashed (data_to_hash**), Number of iterations (**num_iterations**)**

Output: Average time for SHA-xx hashing (average_time_sha_X**)**

Initialize: A timer to record the starting time (start_time).

Initialize: A variable to store the cumulative time (cumulative_time) as 0.

For _ in range(num_iterations): Start the timer.

1) Perform SHA-XXX hashing on the input data (data_to_hash).
2) Stop the timer and record the ending time (end_time).
3) Calculate the elapsed time for this iteration as elapsed_time = end_time - start_time.
4) Add elapsed_time to cumulative_time.

Calculate: the average time for SHA-XXX hashing as average_time_sha_XX = cumulative_time / num_iterations.

Return: the average_time_sha_XX as the result.

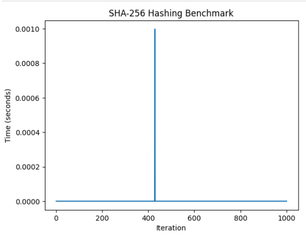


Figure 1.SHA-256 analysis

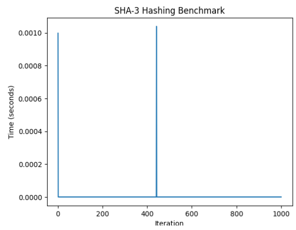


Figure 2. SHA-3 analysis

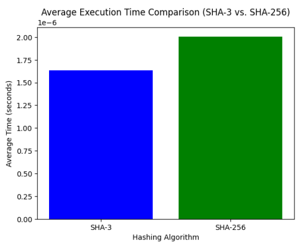


Figure 3. Comparison of Average Execution Times for SHA-3 and SHA-256 Hashing Algorithms

The bar chart above presents a comparative analysis of the average execution times for two widely used cryptographic hashing algorithms, SHA-3 and SHA-256 These algorithms are fundamental for data integrity and security in various applications, including blockchain technology and data verification.

The results clearly indicate that SHA-3 exhibits a slightly faster average execution time compared to SHA-256. SHA-3, which utilizes a 256-bit hash value, demonstrated an average execution time of approximately 1.63 microseconds, while SHA-256, which employs a 256-bit hash value, had an average execution time of approximately 2.01 microseconds. Both algorithms offer fast performance, and this analysis provides valuable insights into their efficiency.

Additionally, the standard deviation values for both algorithms are comparable, suggesting consistent and reliable performance across multiple iterations.

These findings have significant implications for applications requiring secure and efficient data hashing. Researchers and practitioners can consider these results when selecting an appropriate hashing algorithm based on their specific needs and performance criteria. In summary, while both SHA-3 and SHA-256 are secure hash functions, SHA-3 is designed with a stronger focus on security, especially against emerging threats like quantum attacks. SHA-256, on the other hand, is efficient and remains widely used for various cryptographic purposes. The choice between them depends on the specific security requirements of the application.

2.1 Evaluating the Performance of Cryptographic Data Structures

Within the scope of this paper, we meticulously select cryptographic features and leverage their combination to formulate a robust mechanism for a blockchain-based computational solution. A fundamental objective in the development of blockchain applications is to uphold the integrity and confidentiality of data. Because if the implementation can achieve the confidentiality of the data, it's possible archive the data privacy requirements. Therefore, we explore a range of data structures, including Merkel tree [8], hash list [9], H-tree [10], and SM-Tree (Sparse Merkle Tree) [11] approaches. After comprehensive evaluation and comparison of these technologies, we will identify the most suitable one that aligns with our desired level of security.

In addition to security considerations, we also assess the performance of these four cryptographic data structures. To ensure a fair and objective evaluation, we utilize the same algorithm employed in Algorithm 1 to measure the computational efficiency of each approach. This performance assessment enables us to not only select the most secure method but also the one that offers the best balance between security and computational speed. This multi-faceted approach ensures that the blockchain-based computational solution we propose in this paper is both robust in its security features and efficient in its operation. As the landscape of blockchain technology continues to evolve, it is imperative to strike the right balance between security and performance, and our research aims to achieve precisely that.

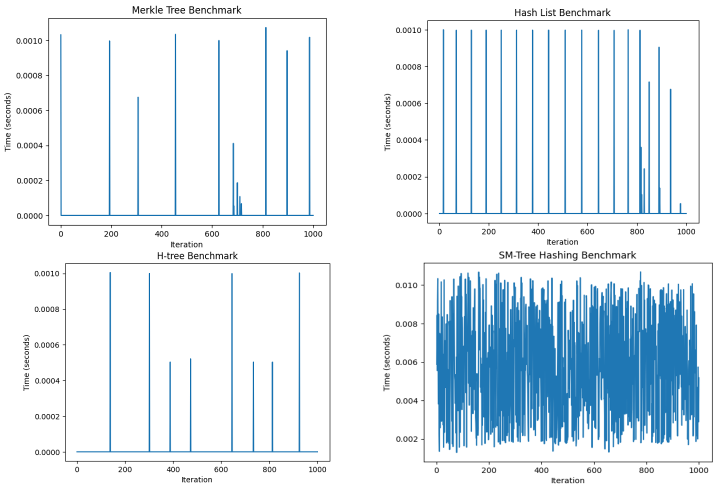


Figure 4.Performance analysis of 4 selected cryptographic data structures

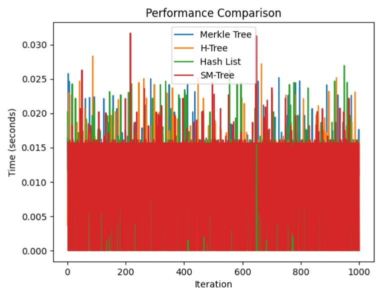


Figure 5.Performance Comparison cryptographic data structures

In summary, the choice of data structure depends on the specific application and requirements. Merkle trees are commonly used for ensuring data integrity in blockchain technology. Hash lists are simple but less scalable. H-Trees are versatile but may be more complex. SM-Trees are efficient for scenarios with sparse data and limited storage requirements.

To facilitate our comparative analysis of blockchain industrial solutions, we employ the methodology [2] used in creating a blockchain solution for the Dubai government. Drawing from previous research work [12], we acknowledge the importance of selecting cryptographic functions and algorithms that can scale effectively. Additionally, given the energy consumption considerations inherent to blockchain-based implementations [13], it becomes imperative to identify the most fitting algorithm that aligns with these requirements. In sum, the integration of these chosen solutions necessitates a thorough examination to establish a robust and dependable computational approach. This, in turn, will enable us to deliver a secure solution for intelligent surveillance within smart cities [14].

2.2 The integration of video blockchain technology into IoT networks.

In this section, we introduce a novel approach aimed at strengthening data integrity within smart cities [15]. Our method seamlessly integrates a Merkle tree, hashing functions, and peer-to-peer data storage into IoT networks to ensure the utmost security and privacy of surveillance data[16–19].

The core of our methodology lies in the verification process, a meticulous procedure designed to identify alterations in image frame sequences and pinpoint specific image modifications. To accomplish this, we generate a dedicated Merkle tree for each data block, securely storing its root hash within the blockchain. This architectural design acts as a safeguard for data integrity, laying the foundation for a robust and secure blockchain implementation [19–21].

To rigorously test our methodology, we've meticulously curated multiple datasets containing sample videos for system integration. These surveillance videos, conventionally recorded at 25 frames per second [22], have been augmented to 30 frames per second in our project to include more comprehensive content in our experiments. Our dataset, comprising 7,000 video frames, focuses on the city of Auckland. The core objective of our research is to generate hash values for video frames, thereby enhancing resistance against potential attacks., focuses on the city of Auckland. The core objective of our research is to generate hash values for video frames, thus bolstering resistance against potential attacks.

Our paper serves as a pivotal link between surveillance video data and blockchain technology. We've established a decentralized repository for storing this critical data, with a primary focus on enhancing security. This enhancement is primarily driven by the strategic use of cryptographic algorithms for hashing and signature, setting our work apart from previous research. These algorithms play a pivotal role in ensuring the seamless connection of video frames, thereby facilitating the detection and localization of any frame alterations. Moreover, our verification procedure, incorporating Merkle trees and hashing functions, adds an additional layer of security.

Recognizing the importance of preserving privacy in blockchain implementation, we propose a blockchain-based solution that not only ensures but also improves the integrity of surveillance data within smart cities. Our aim is to foster increased trust, deliver reliable results, and carefully manage data disclosures. The fusion of computational methods and video blockchain technology effectively regulates data security, curbing unauthorized access and enabling close monitoring in domains such as law enforcement, insurance, and traffic management systems. This, in turn, streamlines necessary enhancements for improved security and compliance in the realm of smart city video surveillance.

To ascertain frame integrity, we construct a Merkle tree from the block matrix hash values. Storing the Merkle tree's root hash in the blockchain enables us to detect any alterations by comparing block and Merkle tree hashes, adding an invaluable layer of tamper resistance to our system.

Additionally, we explore the potential of block matrix operations [23] including matrix multiplication and matrix inversion, for video processing tasks such as compression, filtering, and restoration. These operations are executed on the block matrices stored within the blockchain, allowing for highly efficient and secure video processing.

Our implementation of the Merkle Tree function plays a pivotal role in this system. It takes an array of data and recursively constructs a Merkle tree. In the base case, where only one data item remains, the function returns the data item itself. In all other cases, it constructs the left and right subtrees, hashes them together using the SHA-3 algorithm, and returns the resulting hash, which becomes the root of the Merkle tree.

The composite plot provides a comprehensive visualization of the blockchain privacy-secure methodology, integrating SHA-3, Merkle Tree, and Block Matrix processes. In Subplot 1 (SHA-3), the blue line depicts the output of the SHA-3 hashing process over time, showcasing how input data blocks are transformed into cryptographic hashes. Subplot 2 (Merkle Tree), represented by the green line, illustrates the evolution of the Merkle root hash as adjacent data chunk hashes are paired and hashed, with the final point indicating the unique identifier for the entire set of data blocks. In Subplot 3 (Block Matrix), the orange line portrays the compression of data blocks organized in a matrix, highlighting the reduction in data size over time. The overall trends and interdependencies between these processes offer valuable insights into the efficiency of cryptographic hashing, Merkle Tree construction, and data compression, contributing to a more secure and private blockchain methodology.

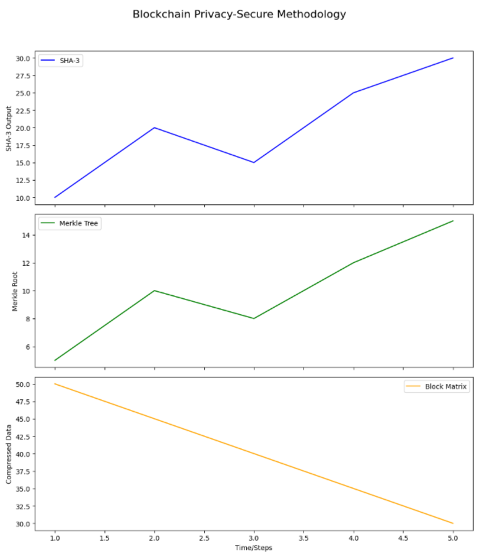


Figure 6.Data analysis for SHA-3, Merkle Tree and Block Matrix

The results portrayed in the composite plot provide several significant conclusions for the blockchain privacy-secure methodology. Firstly, the SHA-3 hashing process demonstrates consistent and efficient transformation of input data blocks into cryptographic hashes, indicating the robustness of the chosen hashing algorithm. The evolving trend in the Merkle Tree construction reveals a systematic pairing and hashing of data chunk hashes, culminating in a unique Merkle root hash that serves as a reliable identifier for the entire dataset. Additionally, the Block Matrix subplot underscores the effectiveness of compression algorithms, such as JPEG, in reducing the data size of video frames organized in a matrix. The interconnectedness of these processes, as evidenced by the integration points in the plot, signifies a cohesive and secure methodology. The reduction in data size through compression, coupled with the cryptographic integrity provided by SHA-3 and the Merkle Tree's unique identification, collectively contribute to the enhancement of privacy and security [24–26] within the blockchain framework. Overall, the results affirm the efficacy of the integrated approach, offering insights into the efficiency of individual components and their collaborative impact on the privacy and security attributes of the blockchain system.

The pivotal element in our system is the implementation of the Merkle Tree function. This function takes an array of data and recursively constructs a Merkle tree algorithm 2. In the base case, where only one data item remains, the function simply returns the data item itself. However, in all other cases, it constructs both the left and right subtrees, hashes them together using the SHA-256 algorithm, and returns the resulting hash, which ultimately becomes the root of the Merkle tree.

Algorithm 2: Merkle Tree

Input: A list of data blocks.

1) Break down the data blocks into consistent fixed-size chunks, typically ranging from 1 to 2KB.
2) Utilize a cryptographic hash function to calculate the hash for each data chunk
3) Form pairs of neighboring data chunk hashes and compute the hash for each pair.
4) Iterate through step 3 until only one hash remains, representing the Merkle root hash.
5) Save the Merkle root hash as the distinctive identifier for the data blocks.

Algorithm 3: Block Matrix

Input: A video file consisting of frames.

1) Partition each frame into fixed-size blocks (16x16 pixels).
2) Organize the blocks of each frame into a matrix, where rows represent blocks and columns represent frames.
3) Employ compression algorithms (such as JPEG) on each block to reduce data size.
4) Save the compressed block matrix as a binary file.
5) For accessing a particular frame, load the compressed block matrix and extract the corresponding column of blocks.
6) To access a specific block within a frame, retrieve the relevant row from the block matrix and decompress the block.

The block matrix algoritem 3 function takes in an array of data and a block size, and con-structs 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.

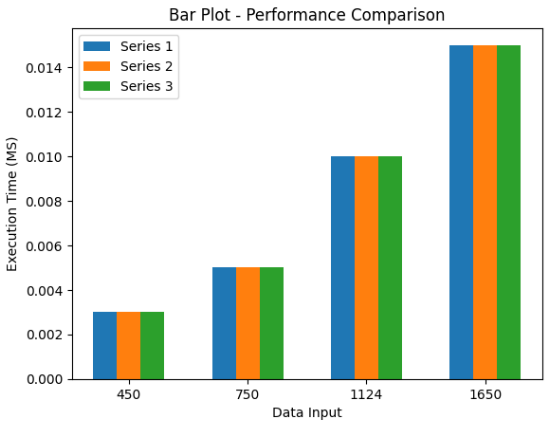


Figure 7.Average computational time (millisecond) for authentication based on Merkle tree by data size.

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 transfer-ring from the surveillance systems.

The throughput (TP) can be mathematically expressed as:

$$TP = \frac{T}{\Delta t}$$

Where:

TP is the throughput, measured in transactions (or blocks) per second (TPS).

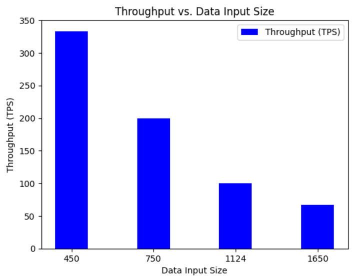
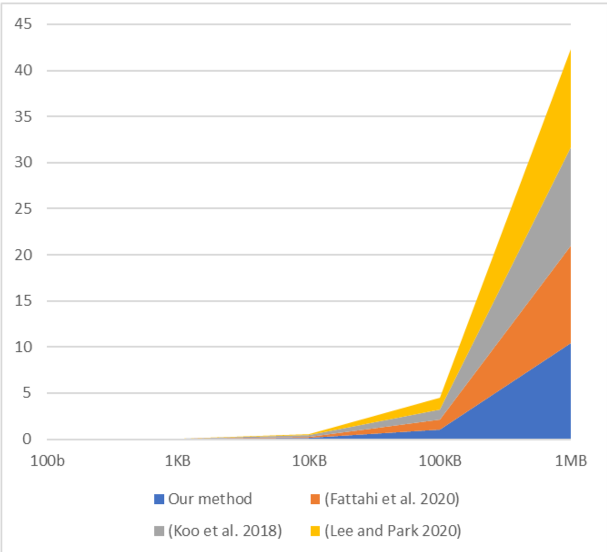


Figure 8.Analysis the Throughput vs. Data Input Size

3. Results Analysist and Discussion

This project seeks to investigate the application of video blockchain in surveillance systems. The approach involves converting recorded videos into individual frames, with each frame ranging from 50KB to 1024KB in size. These frames are utilized to establish a private blockchain system on a Windows 11 64-bit operating system. An experimental setup was implemented to assess the efficacy of this novel method against various types of attacks. The experiment resulted in the development of innovative computational techniques for video blockchains, incorporating specific cryptographic algorithms into the video blockchain framework. In summary, this research contributes technologically to the video blockchain domain by introducing a fresh approach to securing video data in surveillance systems. The outcomes of this research project can serve as a basis for future endeavors in the realms of video blockchain and cryptographic algorithms.



Commented [KMG1]: Need to add new one

Figure 9.Comparisons of computational time between ours and other similar projects [13–15]

Every root structure within the Merkle tree ensures the correlation between video frames and their hashing order, preventing alterations to the image sequence without modifying the entire root structure of the tree. Our ongoing efforts aim to incorporate a real-time change detection feature into the system, enhancing its dependability and fortifying it against privacy-invading and quantum computer attacks. The outcomes of this study offer valuable insights into the evolution of web interfaces for video blockchain systems, laying the groundwork for improving the reliability and security of such systems in the years to come.

This paper concentrates on Merkle tree-based methodologies for data structure. The evaluation involved measuring the computational time and data size for each experiment, with each iteration repeated 100 times to mitigate errors stemming from outliers. Figure x illustrates an ascending trend in computational time in relation to the increase in data size for the three Merkle tree-based approaches. However, beyond 100KB of data, these approaches display only minor differences, as the generation of a Merkle tree for a 1 MB data file constitutes 99.9% of the computational time required by the prover. We graphically depict the results to ascertain time complexity, which is contingent on varying input sizes and block sizes, contributing to the determination of the function's time complexity.

The incorporation of blockchain technology into intelligent surveillance confronts several challenges, including scalability, interoperability, and regulatory compliance. Addressing these challenges entails scaling blockchain to manage substantial data volumes and transactions, seamlessly integrating it with existing systems, and navigating complex regulatory frameworks. In our forthcoming work, we plan to devise solutions to tackle these issues.

5. Conclusions

Within this project, our central objective revolves around establishing a symbiotic relationship between video frames, as captured by intelligent surveillance systems, and the blockchain. Our innovative approach lies in the seamless integration of this data into a decentralized storage platform purpose-built for video surveillance. What sets our work apart from existing studies is its heavy reliance on cryptographic functions, which are instrumental in extracting hash values and signatures from video blockchains. This, in turn, fortifies the security of surveillance data, ensuring its integrity in a tamper-resistant environment.

Notably, our research primarily focuses on enhancing the robustness of data storage within surveillance systems rather than centering on the mitigation of potential risks posed by quantum computer attacks on blockchains. While our current emphasis is on bolstering data security, we acknowledge that the landscape of blockchain technology is evolving. In the future, we intend to delve into the solutions outlined in Section 3.2 to fortify blockchains against quantum threats.

Privacy concerns remain a significant challenge in blockchain implementation, and we acknowledge this aspect as a crucial consideration in our work. However, our vision extends beyond this immediate concern. In the future, there will be a need to address broader challenges such as scalability, interoperability, and regulatory issues that affect the effective deployment of blockchain technology.

The overarching goal of this research is to propose a blockchain-based approach that not only enhances the security and integrity of surveillance data but also cultivates substantial levels of trust, reliability, and controlled data disclosure within smart cities. By harmonizing computer vision with video blockchain technology, our focus is firmly on strengthening the security of surveillance data. The solution we present serves as a robust deterrent against tampering and unauthorized access by external entities.

The contributions stemming from this project open new avenues for necessary advancements in the realm of heightened security and adaptability for video surveillance in the dynamic landscape of smart urban environments. Our work aligns with the evolving needs of these cities, where intelligent surveillance is an integral component of public safety and urban management.

6. Patents – N/A

Supplementary Materials: The following supporting information can be downloaded at: www.mdpi.com/xxx/s1, Figure S1: title; Table S1: title; Video S1: title.

Author Contributions: Conceptualization, M.G. and W.Q.Y.; methodology, M.G.; software, M.G.; validation, M.G.; formal analysis, M.G.; investigation, M.G.; resources, M.G., W.Q.Y.; data curation, M.G.; writing—original draft preparation, M.G.; writing—review and editing, M.G. W.Q.Y., M.N. and X.J.L.; visualization, M.G.; supervision, W.Q.Y. and M.N.; project administration W.Q.Y. and M.N. All authors have read and agreed to the published version of the manuscript.

Funding: This research has not external fundings.

Data Availability Statement: Data sharing not applicable

Acknowledgments: In this section, you can acknowledge any support given which is not covered by the author contribution or funding sections. This may include administrative and technical support, or donations in kind (e.g., materials used for experiments).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Aldairi, A., Tawalbeh, L.: Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. Procedia Comput Sci. 109, 1086–1091 (2017). https://doi.org/10.1016/j.procs.2017.05.391
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). https://doi.org/10.1007/s13198-020-00971-2
3. Gedara, K., Nguyen, M., Yan, W.Q., Li, X.J.: Video Blockchain: A Decentralized Approach for Secure and Sustainable Networks with Distributed Video Footage from Vehicle-Mounted Cameras in Smart Cities. Electronics (Switzerland). 12, (2023). https://doi.org/10.3390/electronics12173621
4. Gedara, K.M., Nguyen, M., Yan, W.Q.: Visual Blockchain for Intelligent Surveillance in a Smart City. Blockchain Technologies for Sustainable Development in Smart Cities, 210–222 (2022). https://doi.org/10.4018/978-1-7998-9274-8.ch012
5. Fu, J., Qiao, S., Huang, Y., Si, X., Li, B., Yuan, C.: A Study on the Optimization of Blockchain Hashing Algorithm Based on PRCA. (2020). https://doi.org/10.1155/2020/8876317
6. Priyadharshini, K., Canessane, R.A.: Blockchain-based security algorithm on IoT framework for shielded communication in smart cities. Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021. 320–327 (2021). https://doi.org/10.1109/ICICV50876.2021.9388497
7. Lin, I.C., Liao, T.C.: A survey of blockchain security issues and challenges. International Journal of Network Security. 19, 653–659 (2017). https://doi.org/10.6633/IJNS.201709.19(5).01
8. 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). https://doi.org/10.3390/electronics9030484
9. George, R.V., Harsh, H.O., Ray, P., Babu, A.K.: Food quality traceability prototype for restaurants using blockchain and food quality data index. J Clean Prod. 240, (2019). https://doi.org/10.1016/j.jclepro.2019.118021
10. Chen, J., Ruan, Y., Guo, L., Lu, H.: BCVehis: A Blockchain-Based Service Prototype of Vehicle History Tracking for Used-Car Trades in China. IEEE Access. 8, 214842–214851 (2020). https://doi.org/10.1109/ACCESS.2020.3040229
11. Deepak, K., Badiger, A.N., Akshay, J., Awomi, K.A., Deepak, G., Harish Kumar, N.: Blockchain-based Management of Video Surveillance Systems: A Survey. 2020 6th International Conference on Advanced Computing and Communication Systems, ICACCS 2020. 1256–1258 (2020). https://doi.org/10.1109/ICACCS48705.2020.9074197
12. Hou, L., Zheng, K., Liu, Z., Xu, X., Wu, T.: Design and Prototype Implementation of a Blockchain-Enabled LoRa System with Edge Computing. IEEE Internet Things J. 8, 2419–2430 (2021). https://doi.org/10.1109/JIOT.2020.3027713
13. Khrais, L.T.: The Combination of IoT-Sensors in Appliances and block-chain Technology in Smart Cities Energy Solutions. 2020 6th International Conference on Advanced Computing and Communication Systems, ICACCS 2020. 1373–1378 (2020). https://doi.org/10.1109/ICACCS48705.2020.9074362

14. Lee, D., Park, N.: Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree. Multimed Tools Appl. (2020). https://doi.org/10.1007/s11042-020-08776-y
15. Michelin, R.A., Ahmed, N., Kanhere, S.S., Seneviratne, A., Jha, S.: Leveraging lightweight blockchain to establish data integrity for surveillance cameras. In: IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2020. pp. 3–5 (2020)
16. Gergely, A.M., Crainicu, B.: Randadminsuite: A new privacy-enhancing solution for private blockchains. Procedia Manuf. 46, 562–569 (2020). https://doi.org/10.1016/j.promfg.2020.03.081
17. Fitwi, A., Chen, Y.: Secure and Privacy-Preserving Stored Surveillance Video Sharing atop Permissioned Blockchain. 1–8
18. Hasan, O., Brunie, L., Bertino, E.: Privacy-Preserving Reputation Systems Based on Blockchain and Other Cryptographic Building Blocks: A Survey, (2023)
19. Du, J., Jiang, C., Gelenbe, E., Xu, L., Li, J., Ren, Y.: Distributed Data Privacy Preservation in IoT Applications. IEEE Wirel Commun. 25, 68–76 (2018). https://doi.org/10.1109/MWC.2017.1800094
20. Ali, M.S., Dolui, K., Antonelli, F.: IoT data privacy via blockchains and IPFS. In: ACM International Conference Proceeding Series. Association for Computing Machinery (2017)
21. Loukil, F., Ghedira-Guegan, C., Boukadi, K., Benharkat, A.N., Benkhelifa, E.: Data Privacy Based on IoT Device Behavior Control Using Blockchain. ACM Trans Internet Technol. 21, (2021). https://doi.org/10.1145/3434776
22. Kalbo, N., Mirsky, Y., Shabtai, A., Elovici, Y.: The security of ip-based video surveillance systems. Sensors (Switzerland). 20, 1–27 (2020). https://doi.org/10.3390/s20174806
23. Zhu, G., Ding, Y., Cao, Y.: The Effect of Block-Matrix Interface of SRM with High Volumetric Block Proportion on Its Uniaxial Compressive Strength. Applied Sciences. 13, 3463 (2023). https://doi.org/10.3390/app13063463
24. Majdoubi, D.E.L., El Bakkali, H., Sadki, S.: Towards Smart Blockchain-Based System for Privacy and Security in a Smart City environment. Proceedings of 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications, CloudTech 2020. (2020). https://doi.org/10.1109/CloudTech49835.2020.9365905
25. Drijvers, M., Edalatnejad, K., Ford, B., Kiltz, E., Loss, J., Neven, G., Stepanovs, I.: On the security of two-round multi-signatures. Proc IEEE Symp Secur Priv. 2019-May, 1084–1101 (2019). https://doi.org/10.1109/SP.2019.00050
26. Anajemba, J.H., Tang, Y., Iwendi, C., Ohwoekevwo, A., Srivastava, G., Jo, O.: Realizing efficient security and privacy in IoT networks. Sensors (Switzerland). 20, (2020). https://doi.org/10.3390/s20092609
27. Hu, R. Visual Blockchain Using Merkle Tree. Master's Thesis, Auckland University of Technology, New Zealand (2019)
28. Hu, R., Yan, W. (2020) Design and implementation of visual blockchain with Merkle tree. Handbook of Research on Multimedia Cyber Security, 282-295.
29. Gedara, K., Nguyen, M., Yan, W. Enhancing privacy protection in intelligent surveillance: Video blockchain solutions. International Congress on Blockchain and Applications, 778, 42.
30. Shu, Y (2018) Blockchain for Security of A Cloud-Based Online Auction System. Master's Thesis, Auckland University of Technology, New Zealand.
31. Shu, Y., Yu, J., Yan, W. (2019) Blockchain for security of a cloud-based online auction system. Exploring Security in Software Architecture and Design.
32. Shu, Y., Yu, J., Yan, W. (2019) State actor model for cloud-based online auction. Exploring Security in Software Architecture and Design.

33. Shu, Y., Yu, J. Yan, W. (2020) Blockchain for security of cloud-based online auction. Research Anthology on Blockchain Technology in Business, Healthcare.
34. Atrey, P., Yan, W., Chang, E., Kankanhalli, M. (2004) A hierarchical signature scheme for robust video authentication using secret sharing. International Multimedia Modelling Conference, 330-337.
35. Atrey, P., Yan, W., Kankanhalli, M. (2007) A scalable signature scheme for video authentication. Multimedia Tools and Applications 34 (1), 107-135.
36. Gupta, M., Yan, W. (2022) Video watermarking with digital signature and fingerprinting. Applications of Encryption and Watermarking for Information Security, IGI Global.
37. Gupta, M. (2021) Improving Security for Video Watermarking. Master's Thesis. Auckland University of Technology, New Zealand.
38. Ling, H., Cheng, H., Ma, Q., Zou, F., Yan, W. (2011) Efficient image copy detection using multi-scale fingerprints. IEEE Multimedia, 19, 60–69
39. Ling, H., Wang, L., Zou, F., Yan, W. (2011) Fine-search for image copy detection based on local affine-invariant descriptor and spatial dependent matching. Multimedia Tools and Applications 52 (2), 551-568.
40. Yan, W. (2019) Introduction to Intelligent Surveillance: Surveillance Data Capture, Transmission, and Analytics. Springer Nature.
41. Vallayil, M., Nand, P., Yan, W., Allende-Cid, H. (2023) Explainability of automated fact verification systems: A comprehensive review. Applied Science, 13(23) 1260.
42. Liu, J., Yan, W. (2022) Crime prediction from surveillance videos using deep learning. Aiding Forensic Investigation Through Deep Learning and Machine Learning Frameworks. IGI Global.