

Visual Blockchain for Intelligent Surveillance in Smart Cities

Kasun Moolika Gedara, Minh Nguyen and Wei Qi Yan
Auckland University of Technology, 1010 New Zealand

ABSTRACT

Visual blockchain takes account of the problem of how to identify integrity of intelligent surveillance data by using computational methods for a smart city. Intelligent surveillance provides spatiotemporally-based visualization from various cameras which are deployed in smart cities. It is able to result in limited tamper of the gathered data from digital cameras. In fact, the decentralized nature of blockchain is to distribute video frames as data output over smart cities. By selecting most appropriate cryptographic algorithms using blockchain prototype, it is able to create sustainable computational methods of visual blockchain and make reliable solutions for the existing visual data. In this book chapter, the contributions are to enrich the security of surveillance data by using most appropriate cryptographic algorithm so as to achieve the data integrity and tamper resistance, a web-based prototype is created through visual blockchain so as to affirm the reality and loyalty of visual data from digital surveillance.

Keywords: Blockchain, Encryption Algorithms, Decentration, Secure, Immutability, Visual Blockchain, Smart City

INTRODUCTION

Modern society has been dramatically updated in every aspect of human beings. People are incentive to imagine these sophisticated and complicated technologies, which are crucial to the development of this community, bring great convenience for ordinary day-to-day lifestyle. However, with the modern technology, considering its negative and positive aspects is much crucial before the implementation. Therefore, with the presence, its security gets a unique place automatically. In smart cities, the real world depends on sensitive information and its most secure repository.

Blockchain was introduced in 2009 and operated as a distributed network in the large-scale industries (Nakamoto, 2009), such as global trade, insurance, banking, distributed energy, and healthcare, etc. Blockchain is adaptively connected to smart transportation systems, food supplier management, government, identity (Singhal, Dhameja, & Panda, 2018). It has been proven that blockchain has been transplanted as a state-of-the-art technology. Bitcoin (Duong *et al.*, 2018) is a popular currency implemented for blockchain, which makes bitcoins difficult to be phony in the transactions. This bitcoin was operated since 2009 (Taylor, *et al.* 2020), which has been extended to other high-tech areas such as intelligent surveillance. On the other hand, blockchain has been developed by the smart connector to end the third party between any transactions. With blockchains, transactions or any process could be conducted without involvement of the third party. Moreover, the blockchain is able to resolve the data integrity problem that is related to medical record verification, gas and electricity monitoring system in smart cities.

The idea of “smart city” is an advanced objective of many cities around the world, in response to the expanding complexity of urban areas and the potential of associated intelligent technologies (Pramod & Sankaran, 2019). Whilst considering the surveillance system, it is also important and should be a subject of

investigation in modern community at present. However, the special goal of smart cities is to ensure the safety and security of the residents by reducing crimes and accident rates (Khan, Byun, & Park, 2020).

The technology that has been widely applied to address those issues is video surveillance (Gipp, Kosti, & Breitingner, 2016). In this case, the mission is to select suitable cryptographic algorithms to create the blockchain and secure the data communication without tampering (Tian, *et al.* 2021) as well as resist any types of attacks. The kind of video surveillance designs are able to resist crimes, anomalous event detection, privacy policy breaching and many. Therefore, the recorded video footages are most important for a pretty rich assortment of purposes. But, malicious attackers, knowledgeable hackers, or other unauthorized third parties can manipulate the cameras and video repositories illegally and create unreal directions to make them useless in the events of crimes (Khan *et al.*, 2020). These types of attacks are happened potentially against the loyalty of stored data captured in intelligent surveillance.

Moreover, blockchains take the place in the tamper resistance of the saved data, the nature of decentralized chain was employed to data verification and data integrity (Fattahi, Makanju, & Fard, 2020). Hashing is one of the reliable ways that take advantage of creating the trust between each and every block in the chain.

Furthermore, cryptographic Hash function is an algorithm that maps arbitrary data to a fixed size string. Usually, Hash functions are required to meet the security requirements of one-witness and collision-resistance. There is no same Hashing value of data in this world. In order to ensure at least 80-bit security, the output length of Hash functions should be at least 160 bits. Hash function in blockchains is SHA256 that is one of the algorithms from a family of cryptographic Hash functions named SHA (Secure Hash Algorithms). Approximately, Hash functions in blockchains achieve proof-of-work (PoW), address generation, block generation (as a part of Merkle-tree paradigm), understand in signatures, pseudorandom number generation, and bridge components (e.g., Fiat-Shamir mechanism, FSM) etc.

The decentralized nature of blockchains takes use of invention of the newest trend other than cryptocurrency. At present, the research trends in intelligent surveillance and blockchain are related:

(1) A smart city collects surveillance videos and enhances the video integrity. The method related to transferring the visual data through blockchains has been proposed (Gipp, Kosti, & Breitingner, 2016) to ensure the integrity of accident videos which was recorded from a dashboard of vehicles. In the event of a vehicle accident, digital videos are collected by using built-in accelerometers, relevant videos are cryptographically hashed and recorded on distributed storage with blockchain at present.

(2) IoT devices are connected through blockchains to monitor air and water quality, transport services, worldwide goods delivery and tracking, food distribution services. The collected data will gather much accurate data timely. The methods are called as a mobility as a service (MaaS) (Anwer, Saad, & Ashfaque, 2020).

In order to ensure the integrity of the recorded videos, using the unique feature of the distributed and tamper proofing characteristics in the blockchain has been employed. In the blockchain, timestamping features are applied to verify and transfer unaltered data to a distributed repository. Similarly, the captured data from a closed-circuit television (CCTV) cameras in smart cities are further explored (Anwer, Saad, & Ashfaque, 2020).

The blockchain-based system is able to guarantee that the recorded data are stored without altered or tampered. It aids to avoid manipulating the data integrity from original videos. Because a distributed ledger of blockchain records the data with metadata (Deepak *et al.*, 2020) from CCTV system, mechanism will assist the law enforcement and clients to secure data from surveillance. As shown in Fig. 1, videos and

photos are employed to create blockchains so as to check the functionality of the implemented computational method.

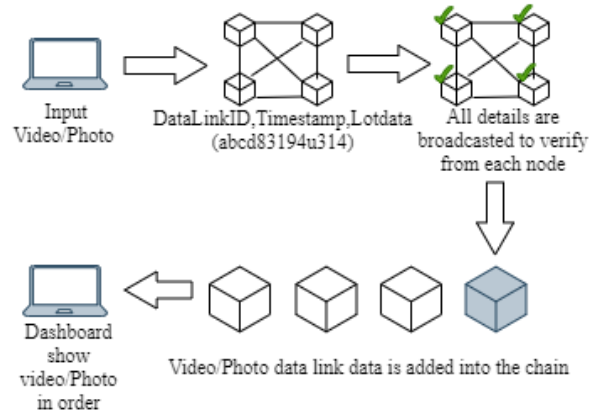


Figure 1. Design of the recommendation system

In this book chapter, following related work, the proposed methods will be iterated. The result analysis will be explicated which leads to the final conclusion of this book chapter.

RELATED WORK

Nowadays, blockchain-based development takes the pivotal place in today's world, but computer vision, intelligent surveillance, artificial intelligence, and machine learning have not combined with blockchain yet. The multidisciplinary knowledge could be combined together as the solutions effectively and efficiently.

BleddSPS is a public safety system (Xu, *et al.* 2020) with decentralized secure architecture, which supports immutability, auditability and traceability to ensure smart city safety. SD-IoD is the software-defined Internet architecture (Liao, *et al.* 2021) with smart contractor and blockchain to secure real-time monitoring systems by using drones. Maintaining the correct order of the recording data is able to ensure reliability and integrity. On the other hand, blockchain for smart cities (Hakak *et al.*, 2020) requires obvious characteristics, which are robust, incorruptible and secure, consensus, transparency, and validation of information. The data processing time and capacity as well as resistance take part to evaluate the computational methods.

According to the analysis of past research work, blockchains connect most smart cities to continue their operations without a single point of failure (Treiblmaier *et al.*, 2020). In this book chapter, the computational methods of visual blockchains are taken into consideration, a new prototype is created for visual data storage by using blockchains, all visual data is linked together by using blockchain with decentralizing or flating method, thus it ensures that the surveillance data as evidence chains from surveillance in digital and smart cities will not be tampered by using the computational methods of blockchains.

THE DESIGN

The main objective of this research project is to construct computational methods of visual blockchain for smart cities. Consequently, an efficient way is found to connect blockchain and select cryptographic

functions so as to achieve this goal. Plentiful attacks are happened against the blockchain platform (Li, *et al.*, 2020). Therefore, the main consideration is to make the solution by combining the most appropriate cryptographical function and ensure the robust fortification than anticipated.

Visual blockchain (Dziembowski, *et al.*, 2015) is a new concept for intensifying the cybersecurity resistance in intelligent surveillance. At present, blockchain is mostly widespread among the industrial, academic, and military sections (Gallo, Pongnumkul, & Nguyen, 2018). Because an effective and efficient solution is highly dependable on the functionalities, intensive solution is needed for blockchain. As the core of blockchains, cryptography and game theory (Singhal, Dhameja, & Panda, 2018) address these three main components of a blockchain and deliver a better result for blockchain-based solutions. Moreover, the existing problems of cryptographical functions include data leaking, DDoS attacks, man in the middle attacks by blockchain (Khan & Salah, 2017). Utilizing the chosen cryptographic functions solves these problems and the other main problem of attacks against blockchains.

The goal of this book chapter is to secure the captured visual data in intelligent surveillance so as to record and link all video frames by using visual blockchain in a peer-to-peer way (Novotny, *et al.*, 2018) and increase the availability of visual data without centralized control. With regard to the surveillance in a smart city, computational methods were employed for sorting (Hu, 2019; Hu & Yan, 2020), merging, searching, and indexing the data and mitigating complicated designs by assisting the understanding the data in experimentation (Anwer, Saad & Ashfaque, 2020), such as the position and source of spectroscopic scenes. Intelligent surveillance is a kind of pervasive and invasive security methods which are accommodated to automatically analyse digital images, videos, audios, or other types of monitoring data with limited human interventions due to real-time requirements (Majdoubi, Bakkali, & Sadki, 2020). Fig.2 shows that how the proposed system works with visual blockchains and how each relevant layer in the blockchain be involved in this process.

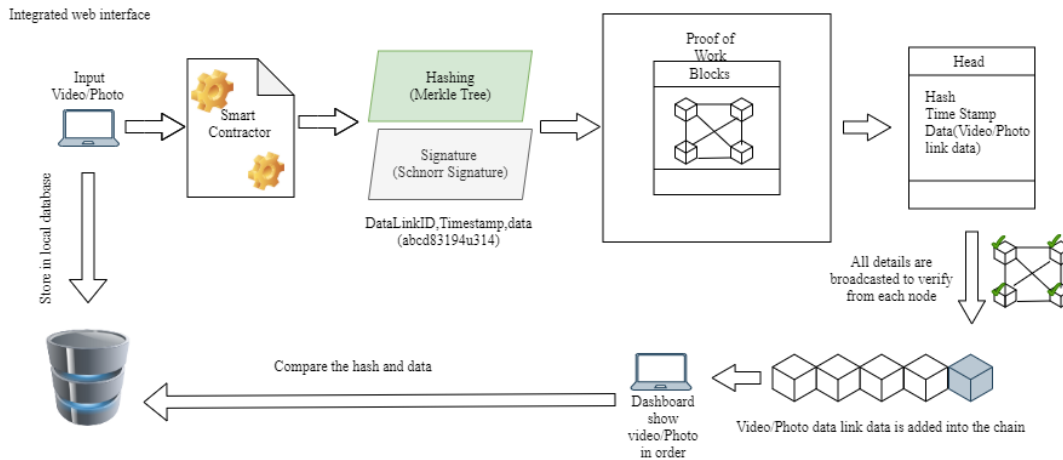


Figure 2. The design of visual blockchain

THE IMPLEMENTATION

In this book chapter, the first goal is to select the cryptographic algorithms so as to develop the computational method for visual blockchain. Thus, the private blockchain is employed for testing most appropriate cryptographic algorithms.

Previously, a method (Hao, *et al.* 2020) was proposed to find the most appropriate cryptographic algorithm. Initially, the lightweight, security, and low energy consumption were achieved. This method was based on

the communications between vehicles and control centres; therefore, the lightweight functions were considered for implementation.

On the other hand, the security problem was considered in implementation (Treiblmaier *et al.*, 2020), because of the attacks like the man-in-the-middle attacks, sniffing the transferring data between blocks is avoided (Kalbo *et al.*, 2020). Moreover, nowadays, the main focus of implementing blockchain is on low energy-consumption solution (Khrais, 2020). Thus, the best function is found for the algorithms which are relevant to the requirements.

At the first stage, the most appropriate method has been created, it is important to verify what is the correct combination to create the strong and secure computational method. Therefore, it is needed to carefully analyse the amalgamation between the selected functions. The blockchain prototype was encoded in the JavaScript to run each function and evaluated by using the parameters by selecting the most appropriate functions.

The way to implement the computational methods is figured out in this book chapter. The blockchain-based system (Xu, Weber, & Staples, 2019) needs to make decision about which part of the data and the computation should be placed on the chain or kept with the chain. Moreover, based on this explanation, the work of this book chapter is to achieve the most sophisticated implementation for the blockchain computational method, the proposed blockchain method is shown in Fig.2.

The implementation is based on the permission with less private blockchain, the implementation is conducted by using programming language Python, Golang, Java-scripts for preprogramming (Panarello, *et al.*, 2018). Fig.3. shows how to select the cryptographic algorithms to develop the visual blockchain method.

Most of surveillance videos recorded with up to 30 *fps* (frame per second), in this chapter, the videos have up to 60 *fps* to get more content in the experiments. The sample videos of the Auckland city are applied to create the dataset for the experiments of this book chapter.

In the process of implementing blockchains, one of the main requirements is to ensure the data integrity (Raman & Varshney, 2018) and tamper resistance (Hao *et al.*, 2020). Furthermore, the similar methods such as Merkle trees are investigated, it unfolds that Hash list, H-Tree, and SM-Tree methods are most suitable for resolving the problem. First of all, the comparative analysis between these method is conducted to get the idea which one is pragmatic and appropriate to reach the required level of security.

Cryptographic methods and algorithms are able to be employed for blockchains, these computational methods extract the difference of video frames and solve the loophole problems. Therefore, the intention to reutilize these functions is able to achieve the high level of security for blockchain.

Moreover, by using Python programming to generate the keys and signatures, comparative understating is given for generating results and theoretical explanation, which is the most appropriate one to develop the blockchain-based applications by using the computational methods.

Signatures still keep core trust between two parties. By the way, elliptic curve cryptography takes the part of signatures in the past decades. Schnorr signature came with solving problems of the ECC, because it takes use of multiple signature instances to verify and prove the identity. The method (Neven *et al.*, 2009) shows that Hash function for Schnorr signature, also Bitcoin, takes use of the ECC for transaction throughput its limitation with the lest signature verification speed (Elbahrawy *et al.*, 2020). The digital signature scheme is a triple,

$$DS = (Kg, Sign, Vfy) \quad (1)$$

where Kg generates a public key Pk and corresponding secret key Sk for security parameter k ; $Sign(Sk, m)$ generates a signature σ based on message $m \in \{0, 1\}$, and $Vfy(Pk, m, \sigma)$ outputs 1 if σ is a valid signature for m under Pk and 0 otherwise.

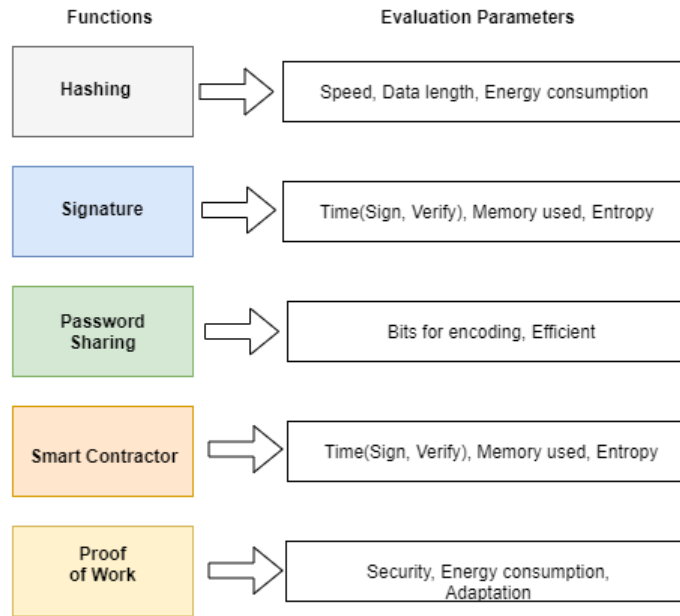


Figure 3. The evaluations of proposed methods

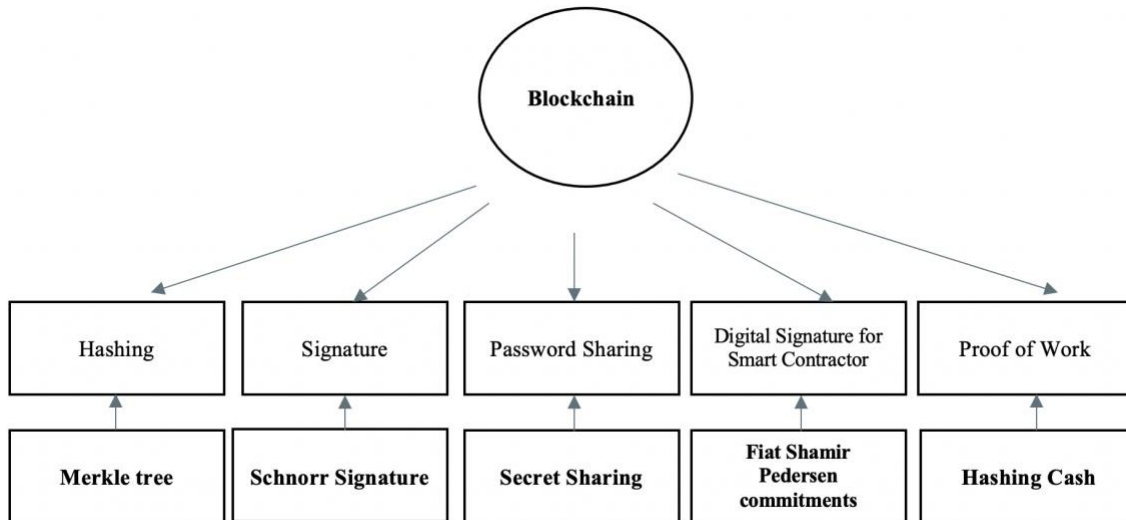


Figure 4. The selected cryptographic functions

In this method, correctness is required,

$$Vfy(Pk, m, Sign(Sk, m)) = 1. \quad (2)$$

The requirements of Schnorr signature and Hashing functions are considered in this chapter. On the other hand (Maxwell, et al., 2019), a new multiple sign Schnorr signature-based method is proposed, this multiple sign protocol is one of the best solutions to enhance the security of the BApp. Schnorr signature has multiple ways to be implemented for various requirements such as SECP256K1, NIST P-256, MuSig, etc.

Compared with the existing methods without key aggregations (Maxwell, *et al.* 2019), the results show what the main requirement is for Schnorr signature which utilizes multisign method. In summary, the requirement of secure signature mechanism is fulfilled by using Schnorr signature multi-signature method accordingly.

In Shamir's Secret Sharing (SSS) for blockchain smart contractor (Harris, 2019), because secret sharing method is distributed way to share the secret for smart contractor in the blockchain. On the other hand, secret sharing with Chinese Remainder Theorem (CRT) (Shyu & Chen, 2008), RSA secret sharing, and SIKE secret sharing are the similar sharing methods implemented by various inventors.

There are different schemes that are similar to Fiat-Shamir's methods which were employed for sharing the secret between two parties without actually revealing the actual value, ZKP method has similar implementations, competitive analysis between these similar methods is conducted to figure out the best one for blockchain implementation. In addition (Gabay, Akkaya, & Cebe 2020), we take advantage of the ZKP method to create the privacy-preserving authentication scheme so as to link videos related to on-road vehicles by using blockchains, the research work aims to secure the user data among the electronic vehicles for charging at service stations. This design has been combined with zkSNARKs (Bitansky, *et al.* 2012) method to prove the knowledge in a single message transfer between one to another location.

In addition, with this method, the features of malleable are acquired. The problem was solved by using the method (Groth & Maller, 2017) with enhanced security of proof generating. From the results, the methods were identified in ZKP. In the ZKP, various implementation plans were conducted. But each of these method has different loophole. Thus, the way has been found to enhance the security of chosen methods. The ZKP is implemented by using Fiat-Shamir and connected with Pedersen commitment scheme. According to the findings of this book chapter, the improved ZKP method is secure more than others. With Fiat-Shamir ZKP method, the security of blockchain is enhanced, the analysis shows that the known value without revealing original value has been proved.

The similar method (Gabay et al., 2020) was employed for connecting electric vehicle charging station by using blockchain (Fill & Haerer, 2018). In future, this method will be employed to achieve the result by using experiments to prove this method immutable and tamper resistant. In summary, the Fiat-Shamir ZKP method is employed for this implementation.

Pedersen commitment is the necessary primitive in cryptography, in this method, the message is sent to a receiver but the receiver could not access to the message until given time period, this is the commitment between the sender and the receiver (Pedersen, 1992). In the method (Yu, 2020), the security of commitment scheme is enhanced by using Schnorr signature to make the blockchain resistance against various attacks, Hash cash is a Proof-of-Work (PoW) algorithm (Back, 1997, 2002) in the cryptocurrencies and blockchain, the PoW is based on the consensus machines of blockchain.

Based on the outcome of this analysis, the selected structure of blockchain implementation is provided in this book chapter. Because the combination is the most sustainable one to achieve the required feature to

satisfy this implementation. Thus, the focus of this book chapter is on the implementation of computational methods of visual blockchain.

In the well-designed experiments, the main part is to test the computational methods developed by using cryptographic algorithms. Therefore, it is needed to ensure that blockchain functionalities are implemented correctly with generating output into the tables by using video frames. The interface contains Hashes of each video frame uploaded to the web site that ensures each frame is able to create or update the entire chain with generating Hashes.

After sorted out the issues related to video frames, the developed interface is applied to check the functionality of the blockchain implementation. Then, the table is visualized with the video frames in the web site after this uploading. The goal of this book chapter is to generate the Hash value to video frames and identify the video frames, ultimately to resist the attacks. Multiple datasets were created with sample videos to run the experimental analysis for a number of images that can be upload into the system.

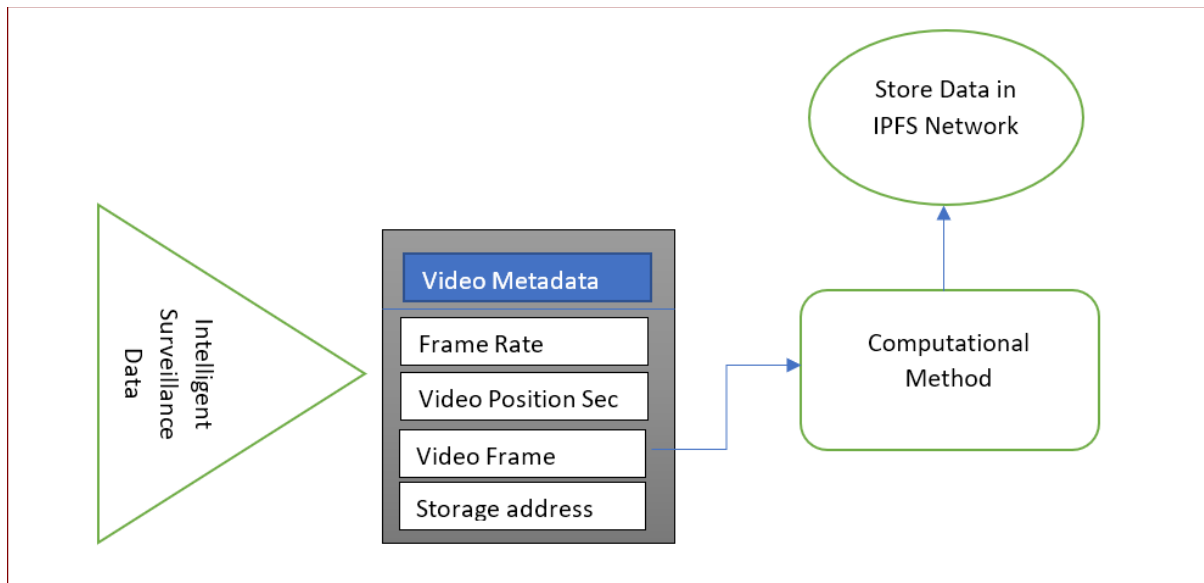
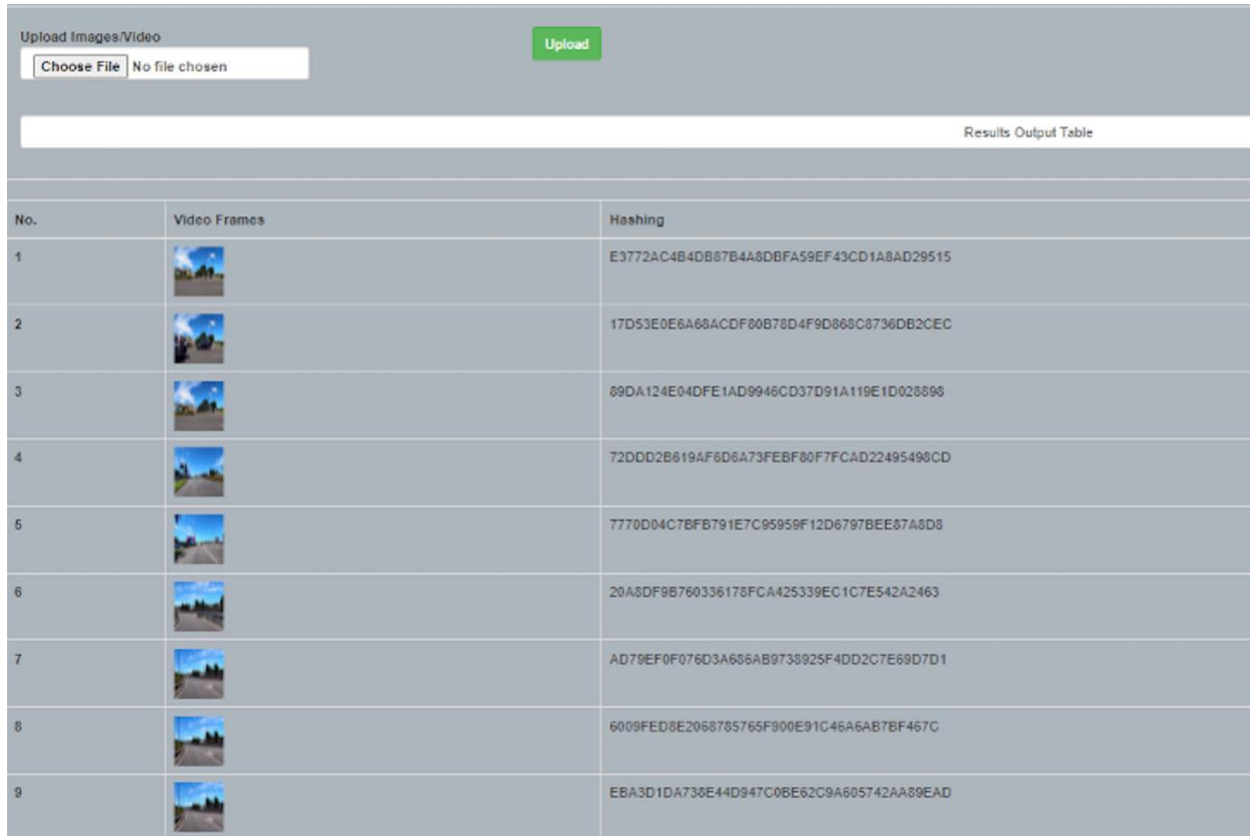


Figure 5: Video frames storing methods

The surveillance data storing problem is resolved by utilizing blockchain-based file storing system. As a result, the verified data couldn't be changed, unauthorized access or modified after storing. Nowadays, most of the solutions came up with the cloud storing faculties. But indeed, they couldn't assure the security of store data other than backup for in case of lost. Therefore, we took a part to secure end of the tunnel by using IPFS (i.e., Interplanetary File System) a peer-to-peer network. Based on the process of the implementation, video frames go through the computational process and are stored in the IPFS network. Regarding surveillance data, we are able to observe video frame rate (Fr), video positions (VPs), number of video frames (Vf), and the storing address (Sa). The computational methods generate the Hash for the surveillance video frames with $HashCm = Hash(Fr, VPs, Vf)$ which will ensure the integrity of the video data.

RESULT ANALYSIS AND DISCUSSION

In this project, the results of this project are obtained as shown in Fig.6. In order to continue the analysis, video frames are extracted from the road videos. This image set is uploaded into web interface for testing our system. In conventional surveillance, the video data is only uploaded to a web location. Some videos were encrypted but limited to video storing path or metadata only.



The screenshot shows a web application interface. At the top, there is a section titled "Upload Images/Video" with a "Choose File" button and a "No file chosen" message. To the right is a green "Upload" button. Below this is a "Results Output Table" header. The table contains 9 rows, each with a number, a video frame image, and a corresponding hash value.










| No. | Video Frames | Hashing |
|-----|---|--|
| 1 |  | E3772AC4B4DB87B4A8DBFA59EF43CD1A8AD29515 |
| 2 |  | 17D53E0E6A66ACDF80B78D4F9D868C8736DB2CEC |
| 3 |  | 89DA124E04DFE1AD9946CD37D91A119E1D028898 |
| 4 |  | 72DDD2B619AF6D6A73FEBF80F7FCAD22495498CD |
| 5 |  | 7770D04C7BFB791E7C95959F12D6797BEE87A8D8 |
| 6 |  | 20A8DF9B760336178FCA425339EC1C7E542A2463 |
| 7 |  | AD79EF0F076D3A686AB9738925F4DD2C7E69D7D1 |
| 8 |  | 6008FED8E2058785765F900E91C46A6AB7BF467C |
| 9 |  | EBA3D1DA738E44D947C0BE62C9A605742AA89EAD |

Figure 6: Web application frontend

CONCLUSION

In this project, the main contribution is to identify the connection of video frames from intelligent surveillance to blockchains and enter that data into the decentralized repository for video surveillance. This is a different approach from other published work because the Hash and signature of visual blockchains are extracted based on cryptographical functions to enhance the security of surveillance data.

In this book chapter, a blockchain-based solution is presented to secure and increase the integrity of surveillance data and achieve the goals of higher loyalty, trust outcome, and uncontrolled disclosures in smart cities. With the combination of computational methods and visual blockchain, the focus is on the security of surveillance data, providing a solution to mitigate the tampering and accessing for unauthorised third-party. This project assists us closely to monitor law enforcement, insurance companies and traffic management systems, which makes necessary adjustments to achieve the video surveillance in the smart city with higher security and suitability.

REFERENCES

- Anwer, M., Saad, A., Ashfaq, A. (2020) Security of IoT using block chain: A review. In *Proceedings of International Conference on Information Science and Communication Technology* (pp. 1–5).
- Bitansky, N., Canetti, R., Chiesa, A., Tromer, E. (2012) From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In *Proceedings of Innovations in Theoretical Computer Science Conference* (pp 326–349).
- Deepak, K., Badiger, A., Akshay, J., Awomi, A., Deepak, G., Kumar, N. (2020) Blockchain-based management of video surveillance systems: A survey. In *Proceedings of Int. Conf. Adv. Comput. Commun. Syst* (pp. 1256–1258)
- Duong, T., Chepurnoy, A., Fan, L., Zhou, H. (2018) TwinsCoin: A cryptocurrency via proof-of-work and proof-of-stake. In *Proceedings of the ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, Co-located with ASIA CCS* (pp 1–13).
- Dziembowski, S., Faust, S., Kolmogorov, V., Pietrzak, K. (2015) Proofs of space. In *Lecture Notes in Computer Science*, 9216 (616160), 585–605.
- Elbahrawy, J., Lovejoy, J., Ouyang, A., Perez, J. (2020) Analysis of Bitcoin improvement proposal 340 — Schnorr signatures, *MIT Report* (pp.1–15)
- Fattahi, S., Mekanju, A., Fard, A. (2020) SIMBA: An efficient simulator for blockchain applications. In *Proceedings of IEEE/IFIP Int. Conf. Dependable Syst. Networks* (pp. 51–52).
- Fill, H., Haerer, F. (2018) Knowledge Blockchains: Applying Blockchain technologies to enterprise modelling. In *Proceedings of the Hawaii International Conference on System Sciences* (pp 4045–4054).
- Frisby, D. (2014) Who is Satoshi Nakamoto? In *Bitcoin: the Future of Money* (pp. 85–149)
- Gallo, P., Pongnumkul, S., Nguyen, U. (2018) BlockSee: Blockchain for IoT video surveillance in smart cities. In *Proceedings of IEEE Int. Conf. Environ. Electr. Eng., IEEE Ind. Commer. Power Syst. Eur.*
- Gabay D., Akkaya K., Cebe M. (2020) Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs. *IEEE Transactions on Vehicular Technology*, 5760–5772.
- Gipp, B., Kosti, J., Breiter, C. (2016) Securing video integrity using decentralized trusted timestamping on the bitcoin blockchain. In *Proceedings of Mediterr. Conf. Inf. Syst.* (pp. 51).
- Groth, J., Maller, M. (2017) Snarky signatures: Minimal signatures of knowledge from simulation-extractable SNARKs. In *Lecture Notes in Computer Science* (pp 581–612).
- Hakak, S., Khan, W., Gilkar, G., Imran, M., Guizani, N. (2020) Securing smart cities through blockchain technology: Architecture, requirements, and challenges. *IEEE Network*, 34(1):8–14.
- Hao, Z., Mao, D., Zhang, B., Zuo, M., Zhao, Z. (2020) A novel visual analysis method of food safety risk traceability based on blockchain, *Int. J. Environ. Res. Public Health*, 17 (17).
- Harris, C. (2019) Consensus-based secret sharing in blockchain smart contracts. In *Int Work Big Data Inf Secur* (pp. 79–84).
- Hu, R. (2019) *Visual blockchain using Merkle tree*. Master’s Thesis, Auckland University of Technology, New Zealand.

- Hu, R., Yan, W. (2020) Design and implementation of visual blockchain with Merkle tree. In *Handbook of Research on Multimedia Cyber Security* (pp. 282 – 295).
- Kalbo N, Mirsky Y, Shabtai A, Elovici Y (2020) The security of IP-based video surveillance systems. *Sensors*, 20(17).
- Khan, M. Salah, K. (2018) IoT security: Review, blockchain solutions, and open challenges. *Futur. Gener. Comput. Syst.*, 82, 395–411.
- Khrais, L. (2020) The combination of IoT-sensors in appliances and block-chain technology in smart cities energy solutions. In *Proceedings of Int Conf Adv Comput Commun Syst* (pp. 1373–1378).
- Khan, P., Byun, Y., Park, N. (2020) A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. *Electron*, 9(3).
- Liao, S., Wu, J., Li, J., Bashir, A., Yang, W. (2021) Securing collaborative environment monitoring in smart cities using Blockchain enabled software-defined Internet of drones. *IEEE Internet Things (Mag)*, 4(1):12–18.
- Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q. (2020) A survey on the security of blockchain systems, *Futur. Gener. Comput. Syst.*, 107, 841–853
- Majdoubi, D., Bakkali, H., Sadki, S. (2020) Towards smart blockchain-based system for privacy and security in a smart city environment. In *Proceedings of Int. Conf. Cloud Comput. Artif. Intell. Technol. Appl (CloudTech)*
- Maxwell, G., Poelstra, A., Seurin, Y., Wuille, P. (2019) Simple Schnorr multi-signatures with applications to Bitcoin. *Des Codes, Cryptogr*, 87(9):2139–2164.
- Neven, G., Smart, N., Warinschi, B. (2009) Hash function requirements for Schnorr signatures. *J. Math Cryptol*, 3(1):69–87.
- Novotny, P., et al. (2018) Permissioned blockchain technologies for academic publishing, *Inf. Serv. Use*, 38(3) pp. 159–171.
- Panarello, Aa, Tapas, N., Merlino, G., Longo, F., Puliafito, A. (2018) Blockchain and IoT integration: A systematic survey. *Sensors*, 18(8), 2575.
- Pedersen, T. (1992) Non-interactive and information-theoretic secure verifiable secret sharing. In *Lect Notes Comput Sci*, 576, 129–140.
- Pramod, N. Sankaran, S. (2019) Blockchain-based framework for driver profiling in smart cities. In *Proceedings of Int. Symp. Adv. Networks Telecommun. Syst.* (pp. 1–6).
- Raman, R., Varshney, L. (2018) Distributed storage meets secret sharing on the blockchain. *Inf Theory Appl Work ITA*.
- Shyu, S., Chen, Y. (2008) Threshold secret image sharing by Chinese remainder theorem. In *Proceedings of IEEE Asia-Pacific Serv Comput Conf.* (pp.1332–1337).
- Singhal, B., Dhameja, G., Panda, P. (2018) *Beginning blockchain – A beginner’s guide to building blockchain solutions*, Jenson Books Inc.
- Taylor, P., Dargahi, T., Dehghantaha, A., Parizi, R., Choo, K. (2020) A systematic literature review of blockchain cyber security. *Digit. Commun. Networks*, 6(2), 147–156.
- Tian, S., Liu, Y., Zhang, Y., Zhao, Y. (2021) A byzantine fault-tolerant raft algorithm combined with Schnorr signature. In *Proceedings of Int. Conf. Ubiquitous Inf. Manag. Commun* (pp. 1–5).
- Treiblmaier, H., Rejeb, A., Strebinger, A. (2020) Blockchain as a driver for smart city development: Application fields and a comprehensive research agenda. *Smart Cities*, 3(3):853–872.

- Xu, R., Nikouei, S., Nagothu, D., Fitwi, A., Chen, Y. (2020) BlendSPS: A Blockchain-enabled decentralized smart public safety system. *Smart Cities*, 3(3):928–951.
- Yu, G. (2020) Simple Schnorr signature with Pedersen commitment as key. *IACR Cryptol ePrint Arch* (pp. 61).