Data Structure and Modeling: A Proposal for Blockchain-Based Video Management System for Smart City Safety

Ji-Woon Lee[1], Hee-Suk Seo[2]

[1]*Technical Researcher, Department of Future Technology, Korea University of Technology and Education, 1600, Chungjeol-ro, Byeongcheon-myeon, Dongnam-gu, Cheonan-si, Chungcheongnam-do, 31253, Republic of Korea*
[2]*Professor, School of Computer Science and Engineering, Korea University of Technology and Education, 1600, Chungjeol-ro, Byeongcheon-myeon, Dongnam-gu, Cheonan-si, Chungcheongnam-do, 31253, Republic of Korea*

In this study, we propose the structure and data modeling of a blockchain-based video management system to enhance safety in smart cities. Video surveillance systems, which play an important role in smart cities, face many challenges including data security, privacy, and system reliability. To address these challenges, this study explores recent research on blockchain's distributed trust, data integrity, and security enhancement, and describes how blockchain ensures the authenticity and accessibility of video data through its core functions, such as digital identity management, video input detection, and object detection, and how blockchain ensures the integrity and traceability of video data through data models, such as camera identity and video. It also highlights security and management mechanisms, including the system's security policy, access control, and network management, and suggests ways to improve the efficiency and safety of video management systems through the interaction of blockchain and surveillance cameras.

Keywords: Blockchain, Smart City Safety, Data Integrity, Decentralized Trust.

1. Introduction

The development of smart cities aims to improve the quality of life of citizens and maximize the efficiency of urban management through technological innovation. In this context, video management systems play a pivotal role in various areas such as public safety, traffic management, and emergency response. However, issues, such as data security, privacy protection, and system reliability, have been identified. Recent studies have highlighted the potential of blockchain technology to provide decentralized trust, data integrity, and enhanced security.

The integration of blockchain and IoT is essential for public safety and the construction of smart cities by enhancing edge computing capabilities and providing a decentralized trust solution for video computation across various trust domains[1]. Moolikagedara et al. [2] argue that blockchain technology combined with vehicle-mounted cameras offers a safe and sustainable network that improves situational awareness and privacy protection in smart city surveillance. According to Brandão et al. [3], blockchain technology supports the safety and reliability of data in smart cities, providing a secure framework for e-governance and data collection, which are essential for the smart city ecosystem. The blockchain-based video surveillance system BlockSee ensures the validity and immutability of camera settings and surveillance videos, addressing the risks of digital and physical manipulation[4]. This study emphasizes the applicability and importance of blockchain technology in the safety domain of smart cities by detailing the system's structure, data structure, and model as an approach to system reliability, security, and data management efficiency.

First, the overall structure of the system is presented, explaining how the reliability and accessibility of video data are ensured through core functions, such as Digital Identity Management (DID Management), Video Input Detection, and Object Detection. This meets the need for real-time video surveillance and event response systems for public safety.

Second, through data models, such as Camera Identity and Video Metadata, it is shown how blockchain technology ensures the integrity and traceability of video data. This is a key element for enhancing the transparency and reliability of video data management.

Third, the security and management mechanisms of the system, including Security Policy, Access Control, and Network Management, are highlighted. These can be used to address security threats and privacy concerns that the video management system of a smart city may face. Finally, by integrating the system modules with the previously mentioned policies and controls, we demonstrate how blockchain and surveillance cameras interact to achieve both efficiency and safety in the video management system. By detailing the structure and data of the proposed system, this study demonstrates how blockchain technology can direct the improvement of safety and services in smart cities' video management systems.

2. MATERIALS AND METHOD

Smart cities leverage a variety of advanced technologies, including IoT, artificial intelligence, and big data to improve the efficiency of infrastructure and operations. In this context, blockchain technology offers solutions for security, data integrity, privacy protection, data sharing, and collaboration in smart-city video surveillance systems. It also has the potential to be used for various purposes such as crime prevention, traffic management, and public safety maintenance in smart cities. However, traditional video-surveillance systems face several challenges.

Data Security: Data stored on central servers are vulnerable to hacking attacks.

Privacy Violation: Video data containing personal information may be misused.

Lack of System Integration: It difficult to share and collaborate data across heterogeneous systems.

Blockchain technology, based on distributed ledgers, encryption, and consensus algorithms, can provide a secure and transparent data management system to improve the security, privacy, and efficiency of video surveillance systems in smart city environments. Based on the latest research trends, the key topics and research for realizing blockchain-based video surveillance systems are as follows.

2.1. Decentralized Security

A major vulnerability of traditional video surveillance systems is their centralized data storage and management structure, which exposes a single point of attack that could compromise the entire system. Recent studies have proposed utilizing the distributed ledger characteristic of blockchain to eliminate centralized management servers and securely store video data and related metadata across multiple nodes in a blockchain network[5],[6],[8],[16],[17],[18].

2.2. Data Integrity and Authenticity

Data collected from video surveillance systems are susceptible to security threats and the risks of manipulation and tampering. Blockchain technology is gaining attention as a solution to these problems. Utilizing the immutability and data traceability features of blockchain, methods have been proposed to store the hash values of individual video frames on the blockchain, allowing for the immediate verification of any changes to the data and tracing of its origin in a manner similar to [6],[7],[8],[13],[16],[17]. Although not directly related to video surveillance systems, a method has been presented that uses blockchain to efficiently integrate spatiotemporal data in wireless sensor networks[10], which can be applied to securely and efficiently aggregate data collected across various locations and times within large-scale video surveillance systems.

2.3. Privacy Preservation

Concerns regarding the potential invasion of privacy due to video surveillance activities continue to be raised. Research on blockchain technology has necessitated the design of systems that meet the requirements for protecting personal information. Key technologies include secure Merkle trees and homomorphic encryption [7],[8],[9]. Additionally, methods for decentralizing privacy using blockchains to protect personal data have been proposed [11]. This concept can be applied to smart city video surveillance systems to effectively maintain surveillance efficacy while protecting the privacy of individuals captured in footage. Furthermore, the use of blockchain for secure surveillance data storage models[15],[20][21][22][23] can be discussed as a solution for the safe storage and management of surveillance data collected in smart-city environments.

2.4. Blockchain-Based Interoperability

The construction of video surveillance systems involves various processes, and blockchain can optimize these processes and enhance their efficiency[14]. In particular, they can provide a secure and efficient data-sharing environment that supports standardization, data compatibility, efficient data sharing, and collaboration, thereby strengthening collaboration among various institutions[12].

In addition, this paper introduces a blockchain-based smart-surveillance system combined with artificial intelligence. This research thoroughly explored how to build a powerful surveillance solution by integrating blockchain and artificial intelligence within a smart city environment[19].

3. RESULTS AND DISCUSSION

Blockchain technology can be utilized to enhance the security, privacy, and efficiency of video surveillance systems in smart-city environments. This study conducts an in-depth analysis of the core topics and research methodologies of blockchain-based video surveillance systems, and proposes their potential applications within the context of smart cities.

3.1. Overview of system architecture

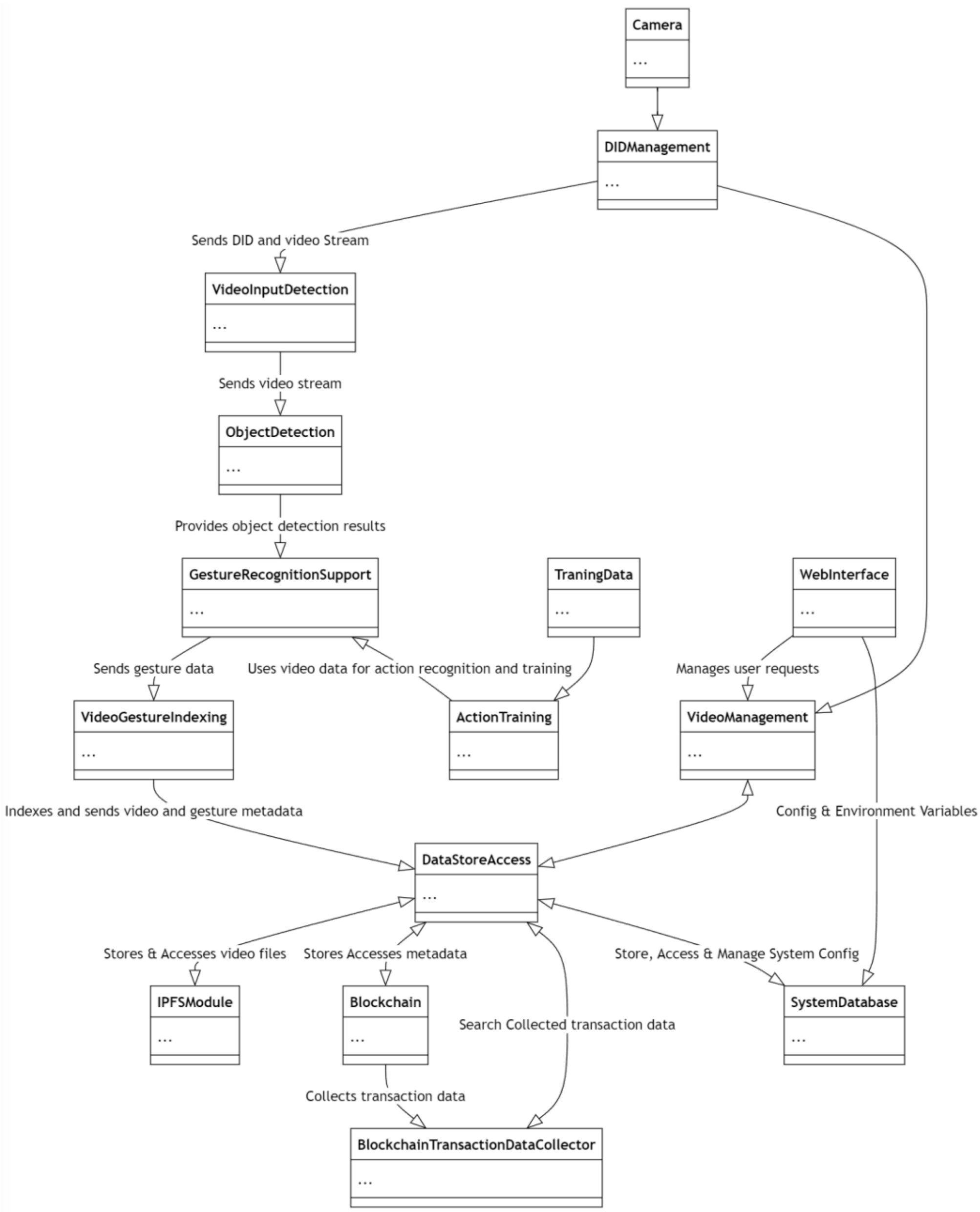

Figure 1. System Architecture

Figure 1 illustrates the overall structure of the video surveillance and data management system and explains the significance and role of each key module. This system integrates various technical elements to optimize the collection, processing, storage, and retrieval of video surveillance data and is defined as follows:

Table 1. Input/output data and interrelationships for each module

Module Name	Input Data	Output Data	Description
Video Input Detection	Real-time video stream from cameras	Video stream signals detected	Detects video stream signals from cameras.
Object Detection	Video stream	Object detection results	Identifies and classifies objects in videos.
Gesture Recognition Support	Object detection results	Gesture recognition results	Identifies and classifies behavior patterns.
Video & Gesture Indexing	Video stream, Gesture recognition results	Indexed video and gesture metadata	Combines video and gesture data for indexing.
Data Store & Access	Indexed data	Stored data and access rights	Manages secure data storage and access.
Blockchain	Metadata	Transaction data	Ensures data integrity with immutable records.
Blockchain Transaction Data Collector	Transaction data	Transaction collection data	Retrieves and collects blockchain transaction data.
IPFS	Video files	CID (Content Identifier), file name, size	Stores video files on a distributed filesystem.
Web Interface	User requests	Information provided to users	Serves information based on user requests.
Video Management	User requests	Managed and provided video data	Manages video data based on user requests.
Action & Training	Action labels and training data	Training results	Supplies data for improving the learning model.

① The Camera module serves as the primary input device for the system, providing real-time video streams. It is utilized as foundational data in the fields of computer vision and digital image processing, and is responsible for the initial steps in environmental monitoring and event detection.

② The DIDManagement module enhances digital identity management and secures access control by generating, assigning, and managing Distributed Identifiers (DID) for each camera. This plays a crucial role in digital identity and access control.

③ The VideoInputDetection module detects the camera DID within the video streams and recognizes the video stream signals, managing the camera location and anomaly information. This process is based on pattern recognition and machine-learning technologies.

④ The ObjectDetection module identifies and analyzes objects within a video stream and detects suspicious activities and potential risks. This core technology, in the field of computer vision, significantly improves the efficiency of security systems.

⑤ The GestureRecognitionSupport module identifies and classifies behavioral patterns based on the results of object detection.

⑥ The VideoGestureIndexing module indexes video and gesture metadata, creating thumbnails and timestamps to ensure the searchability and accessibility of the data. This process is a key element in enhancing the efficiency of information retrieval systems.

⑦ The ActionTraining module provides action labels and training data for training the gesture recognition and behavior analysis models. This is important to improve the learning capabilities of models in the fields of machine learning and artificial intelligence.

⑧ The VideoManagement module is responsible for the search, control, and monitoring of video streams. Multimedia database management and information retrieval technologies enable efficient video-data management.

⑨ The DataStoreAccess module manages the distributed storage and secure access to data by storing video files on the IPFS and metadata on the blockchain. This plays a vital role in ensuring the security, integrity, and accessibility of data.

⑩ The Blockchain and IPFSModule modules are responsible for ensuring integrity, immutability, and secure storage through a distributed file system of data. They provide a technical foundation for enhancing the reliability and security of data-management systems.

⑪ The blockchainTransactionDataCollector module collects and caches transaction data from the blockchain, providing users with fast search results. This enhances the efficient use of blockchain technology and improves data accessibility.

⑫ The WebInterface and SystemDatabase modules manage the user interface, the system's environmental variables, and configuration information. They ensure the convenience of users and stable operation of the system.

Table 2. Data model fields of main modules

Module Name	Field	Type	Description
DIDManagement	did	string	Digital Identifier for the camera.
	generateTimestamp	dateTime	Timestamp when the DID was generated.
	assignTo	string	Identifier for the entity the DID is assigned to.
	status	string	Status of the DID (e.g., active, inactive).
VideoInputDetection	cameraDID	string	DID of the camera that detected the video input.
	videoStreamSignal	string	Signal or identifier for the video stream.
	cameraLocation	string	Location information of the camera.
	anomalyInformation	string	Information about any anomalies detected.
ObjectDetection	detectedObjects	array	List of objects detected in the video.
	suspiciousActivities	boolean	Indicates whether any suspicious activities were detected.
	potentialHazards	boolean	Indicates whether any potential

			hazards were detected.
GestureRecognitionSupport	behaviorPatterns	array	List of identified behavior patterns.
	actionRecognitionData	string	Data related to gesture and action recognition.
VideoManagement	searchAndControl-VideoInformation	function	Allows searching and controlling video information.
	monitorVideoStreams	function	Monitors video streams for any specified criteria.
VideoGestureIndexing	indexVideoAnd-GestureMetadata	function	Indexes video and gesture metadata for easy retrieval.
	generateThumbnailsAnd-Timestamps	function	Generates thumbnails and timestamps for video segments.
DataStoreAccess	storeVideoFilesInIPFS	function	Stores video files in the InterPlanetary File System (IPFS).
	storeMetadataInBlockchain	function	Stores video metadata in a blockchain for integrity and traceability.
BlockchainTransaction-DataCollector	collectAnd-CacheTransactionData	function	Collects and caches transaction

			data for quick access.
IPFSModule	usePrivate-DistributedFileSystem	function	Utilizes a private distributed file system for secure storage.
Blockchain	maintainData-IntegrityAndImmutability	function	Ensures the integrity and immutability of stored data.

3.2. Data Model

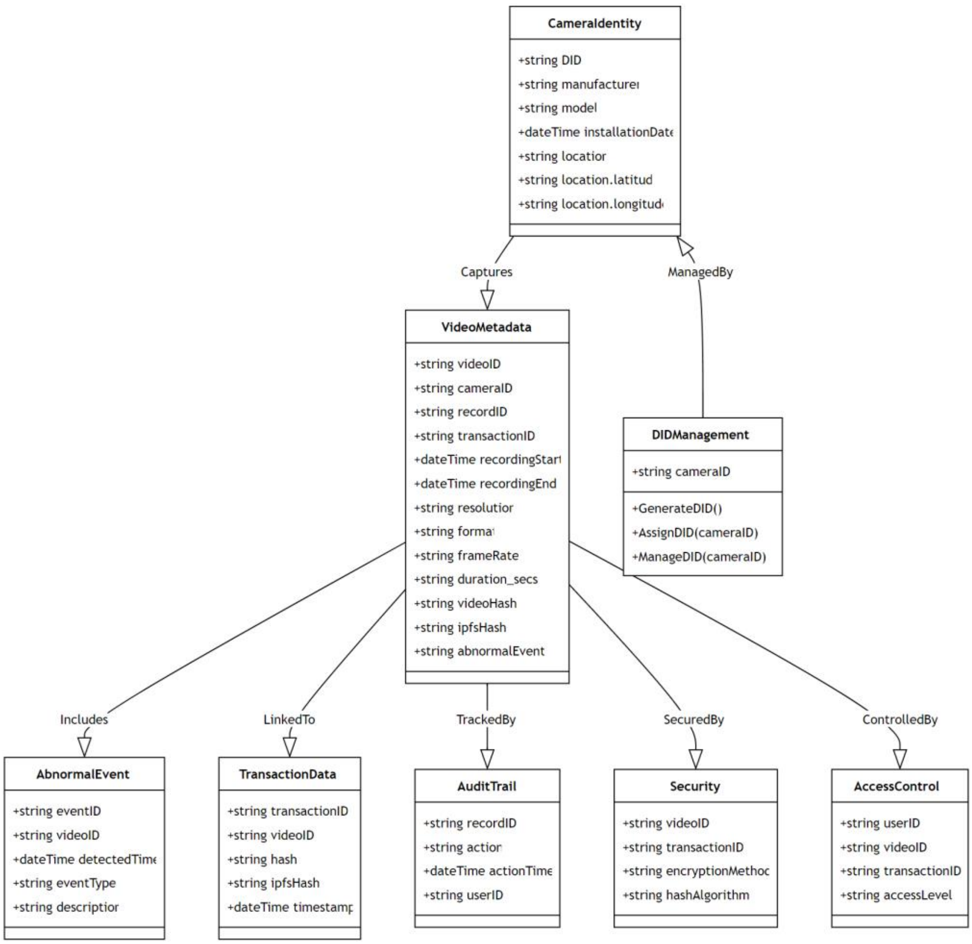

Figure 2. Data Model

Data models and configurations are crucial components of video surveillance and data management systems. Each data model performs a specific role within the system, and its interactions define the data flow and processing procedures of the system. The effective design and management of data models are critical factors that determine a system's efficiency, security, and scalability.

Table 3. Interrelationship between data types

Data Type	Description	Interaction
Video Data	Raw footage captured by surveillance cameras.	Served as input for object detection, stored on IPFS, and indexed for retrieval.
Metadata	Data providing information about video files.	Used for indexing, searching, and blockchain transactions to ensure integrity.
Blockchain Transaction Data	Records of blockchain transactions for video files.	Ensures video data integrity and facilitates secure access control.
Object Detection Data	Results from analyzing video for specific objects.	Input for gesture recognition, action detection, and triggers alerts or actions.
Gesture Recognition Data	Identified gestures or actions within video footage.	Used for enhanced indexing, alerting, and specific search functionalities.
User Data	Information on system users and access rights.	Determines access levels and rights for viewing or managing video data.
IPFS References	Links to video files stored on IPFS.	Facilitates decentralized storage and retrieval of video data without compromising integrity.

Figure 2 presents a data model diagram that outlines the structure of data management and security within a video surveillance system. Each class represents a core component of the system, and their relationships define the flow and processing of the data as follows:

① The CameraIdentity class contains unique identification information for surveillance cameras, including the Digital Identifier (DID) of the camera, manufacturer, model, installation date, and location (including latitude and longitude). This class is essential for uniquely identifying each camera and tracking its location and characteristics within a system.

② The DIDManagement class is responsible for generating, assigning, and managing Digital Identifiers (DID) for the cameras. It is linked to the CameraIdentity class, and assigns and manages a unique identifier for each camera.

③ The VideoMetadata class manages metadata for video recordings, including video ID, camera ID, recording start and end times, resolution, format, frame rate, video length (in seconds), video hash, IPFS hash, and abnormal events. This class defines the characteristics and storage locations of video files, and enables the recording of abnormal events.

④ The AbnormalEvent class includes details of abnormal events detected within the video, comprising the event ID, video ID, time detected, event type, and description. It is used to record and analyze significant incidents in security-monitoring systems.

⑤ The TransactionData class manages blockchain transaction data related to video data, including transaction ID, video ID, hash, IPFS hash, and timestamp. It is crucial to ensure the integrity and traceability of video data.

⑥ The AuditTrail class manages audit trail records of all actions performed within the system, including the record ID, action performed, time of action, and user ID. Thus, it is essential to enhance the security and transparency of the system.

⑦ The Security class contains security-related information for video data, including the video ID, transaction ID, encryption methods, and hash algorithms. They play a vital role in maintaining the security of video data and ensuring data integrity.

⑧ The AccessControl class manages access control information for video data, including the user ID, video ID, transaction ID, and access level. It is used to define access permissions for users and manage secure access to data.

This data model systematically addresses the collection, storage, management, and security of data within a video-surveillance system. Each class and its relationship clearly define the system's data flow and processing methods. This structure maximizes the system's efficiency and security, supporting various functions such as the identification and processing of abnormal events, ensuring data integrity, and managing user access control.

3.3. Control and policy model

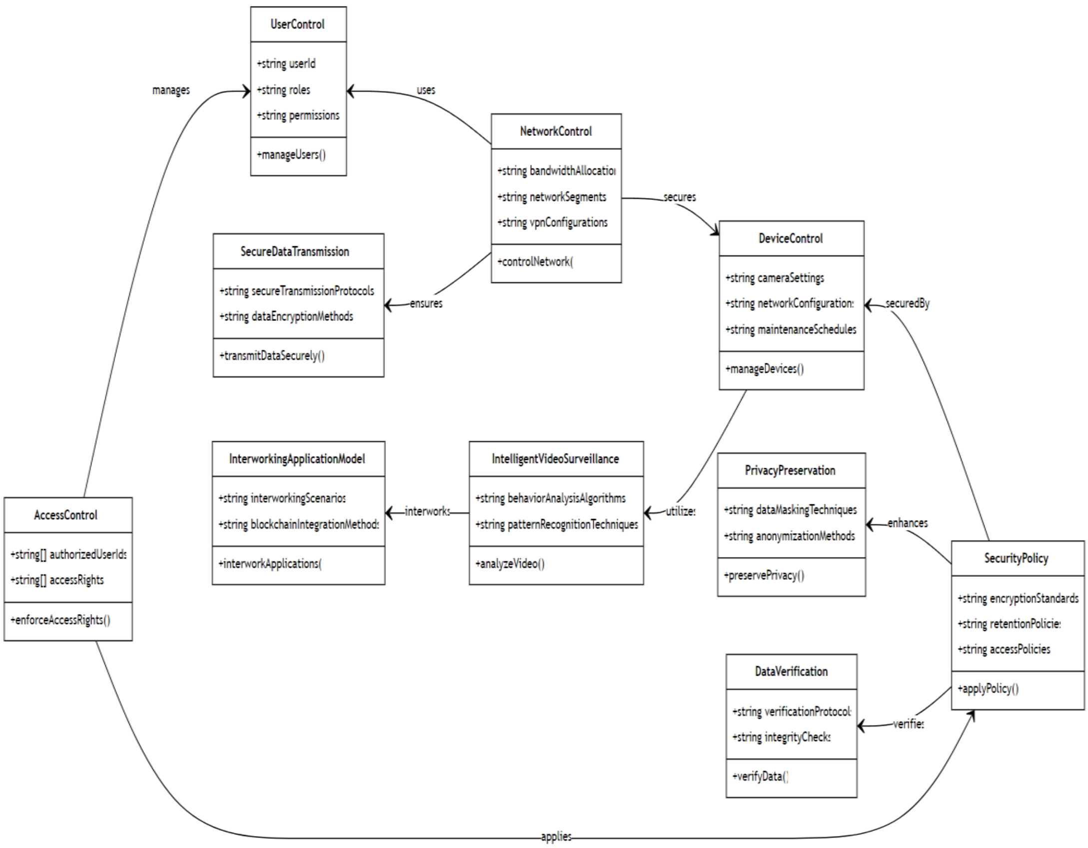

Figure 3. Control and policy data model

Figure 3 illustrates the operation of the control and security-policy models. The system is composed of multiple modules, each performing specific functions to enhance the overall security and efficiency of the system, and operating as follows:

① Access Control manages user access permissions within the system. It defines the allowed actions and data access rights for each user, and enforces these permissions. User management is conducted using the UserControl module, granting access rights based on the identity and role of the user.

② Security policies define and apply the security policies of a system. This includes encryption standards, data retention policies, and access policies, which strengthen the security of the system's data and communication. It is enforced by the AccessControl module to ensure consistent management of security policies across the system.

③ Device Control is responsible for managing device settings, network configurations, and maintenance schedules. Network security is enhanced through the NetworkControl module, with security policies defined by SecurityPolicy applied to devices.

④ Network Control controls the network through bandwidth allocation, network-segment configuration, and VPN settings. It is connected to the DeviceControl and SecureDataTransmission modules to ensure the security of data transmission over the network.

⑤ Privacy Preservation enhances the protection of personal information through data-masking and anonymization methods. Privacy is protected according to the security policies defined by SecurityPolicy.

⑥ The integrity and accuracy of the data were verified. The reliability of the data is ensured through verification protocols and integrity checks set by SecurityPolicy.

⑦ Intelligent Video Surveillance analyzes video data using behavioral analysis and pattern recognition technologies. It processes data collected from cameras managed by the DeviceControl module and shares analysis results with other systems through the InterworkingApplicationModel.

⑧ Secure Data Transmission is responsible for ensuring data security during transmission. It manages encryption methods and security protocols applied during data transmission, in conjunction with network security settings defined by the NetworkControl module.

⑨ The Interworking Application Model defines the interaction between systems and methods for blockchain integration. It enables integration with various applications by utilizing analysis results from the IntelligentVideoSurveillance module.

Table 4. Data model fields of control and policies

Control Name	Field	Type	Description
AccessControl	authorizedUserIds	string[]	List of User IDs authorized to access the system.
	accessRights	string[]	List of access rights assigned to authorized users.
DeviceControl	cameraSettings	string	Configuration settings for cameras.
	networkConfigurations	string	Network configuration settings.
NetworkControl	bandwidthAllocation	string	Allocation of bandwidth for network resources.
	networkSegments	string	Segmentation of the network for better management and security.
UserControl	userId	string	Identifier for the user.

	roles	string[]	Roles assigned to the user.

(a)

Policy Name	Field	Type	Description
SecurityPolicy	encryptionStandards	string	Encryption standards applied to protect data.
	retentionPolicies	string	Policies regarding the retention period of data.
PrivacyPreservation	dataMaskingTechniques	string	Techniques used to mask data to preserve privacy.
	anonymizationMethods	string	Methods used to anonymize data.
DataVerification	verificationProtocols	string	Protocols used to verify the integrity and authenticity of data.
IntelligentVideoSurveillance	behaviorAnalysisAlgorithms	string	Algorithms used for analyzing behavior patterns in video data.
SecureDataTransmission	secureTransmissionProtocols	string	Protocols used to ensure the secure transmission of data.

(b)

3.4. Integration of system architect and data model

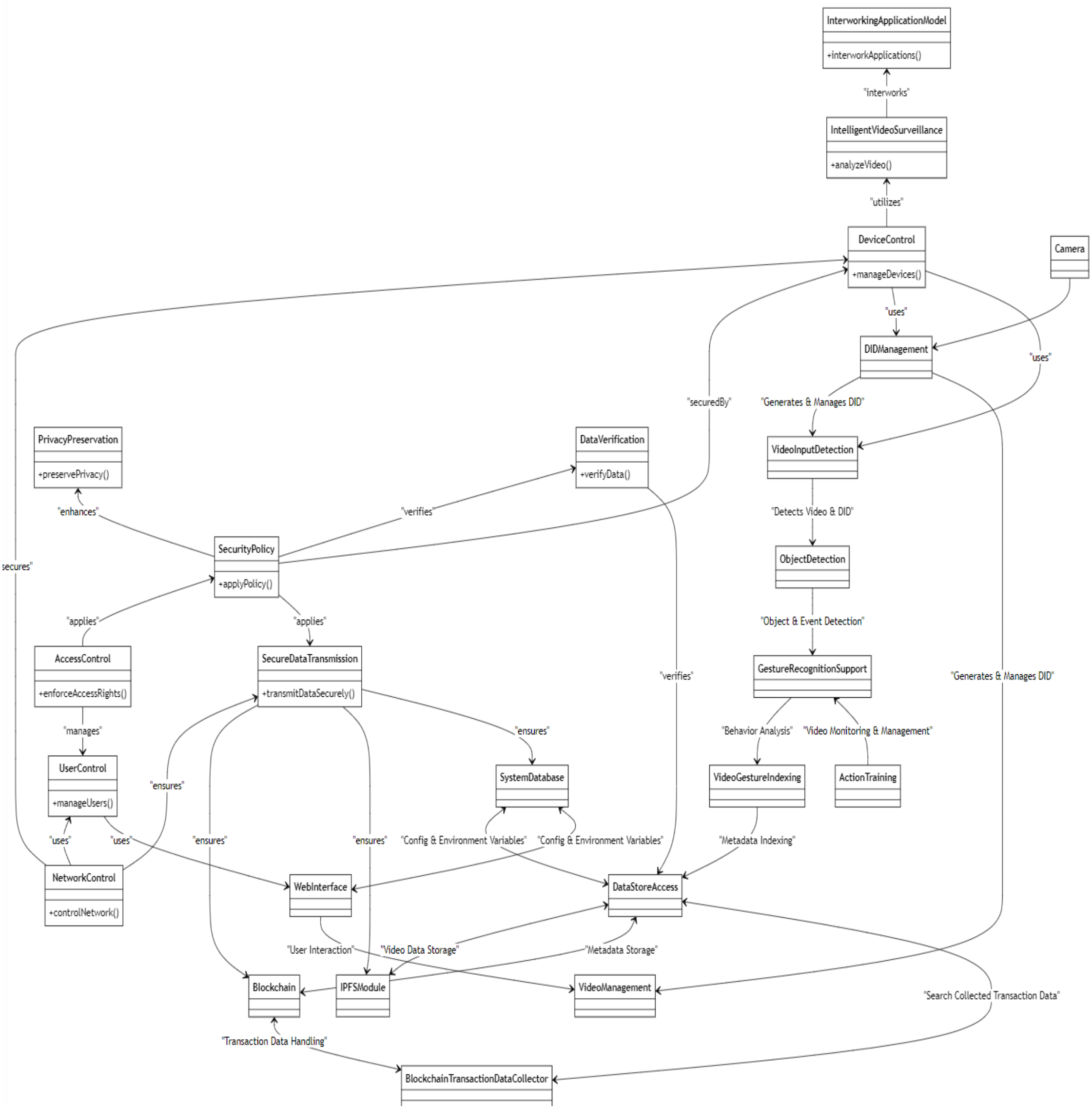

Figure 4. Integrated system and data model

Figure 4 shows the structure of the video surveillance and data management system in detail, showing how the user and device management control, core functional modules, and the policy model manage various aspects of the system. It particularly focuses on the significance of the data model, which serves as the central axis that enables the execution of core functions and security policies. The primary roles of the data model are as follows.

① DIDManagement provides a data model that forms a link between cameras and video data. By generating and managing the Digital Identifier (DID) of the cameras, it clearly identifies which video stream comes from which camera. This is essential for verifying the source of the data and ensuring traceability within the system.

② VideoMetadata is a data model that records the attributes of video files, including basic information such as recording start and end times, resolution, format, along with video hash and IPFS hash to support data integrity and accessibility. It facilitates the management and search of video data and enhances the data-processing efficiency of the system.

③ AbnormalEvent and TransactionData models manage the records of video analysis results and data transactions. Recording the details of detected events and the hash values of data transactions supports the security auditing and data verification tasks of the system.

④ DataStoreAccess, Blockchain, IPFSModule provide data storage and security. They offer secure storage of video files and metadata, ensuring data integrity, immutability, and accessibility. Specifically, the utilization of blockchain and IPFS technologies presents an innovative approach for data security and distributed storage.

⑤ As shown in Figure 4, data models play a crucial role beyond merely storing data; they are essential for managing, verifying, and protecting the system's data. Identifying the source of data, recording the attributes of videos, managing abnormal events, and ensuring secure storage and access to data, data models support various functions of the system.

In summary, it is evident that vital data models are for the efficient operation and security management of video surveillance and data management systems. The design and management of data models play a key role in optimizing system performance and ensuring the safety and accessibility of data. This reminds system designers and developers of the importance of data-centric system design and management and provides insights into system development.

4. CONCLUSION

The structure and data model of the video surveillance and data management system presented in this study have the potential to contribute in various ways. By detailing a complex structure that includes user and device management, core functional modules, and the policy model, we demonstrate how the interaction between each component and the data model can maximize the system's efficiency, security, and scalability. Specifically, the design and management of data models act as a key element supporting various functions within the system, such as identifying the source of data, recording video attributes, managing abnormal events, and ensuring the safe storage and access to data, with details as follows:

First, the importance of data models and data-centric approaches play a crucial role in system design and management, offering a direction for design that considers data security, processing efficiency, and system scalability. This approach is essential for future-oriented system development, ensuring data safety and accessibility, and optimizing the system performance.

Second, understanding the interactions and data flow within a complex system can contribute to the development of more efficient and secure system-design methodologies. The interconnected tasks between each component ensure the stability and performance of the system, thereby providing important guidelines for system designers and developers.

Understanding these interactions is crucial for developing methods for enhancing system security and optimizing data processing.

Third, by utilizing the presented diagrams to consider design directions that account for data security, processing efficiency, and system scalability, flexibility can be applied to the system to respond to future technological advancements and changing system requirements. This can make significant contributions to both academic research and industrial applications, facilitating the integration of new technologies and the development of design principles and methodologies.

In summary, this study emphasizes the complex structure of the video surveillance and data management system and the importance of interactions and data models within it. These elements are essential for the efficient operation and security management of systems and highlight the importance of data-centric system design and management. This provides valuable guidance for current and future system development projects, making significant contributions to the development of design directions that consider data security, processing efficiency, and system scalability.

ACKNOWLEDGMENT

This study was supported by the Professor Education Research Promotion Project at the Korea University of Technology and Education in 2024.

References

1. Gao Y, Li Y, Jia Y. Video computing across trust domains based on blockchain. In: Proceedings of the ACM Turing Celebration Conference-China. 2019. https://doi.org/10.1145/3321408.3326693
2. Moolikagedara K, et al. Video Blockchain: A Decentralized Approach for Secure and Sustainable Networks with Distributed Video Footage from Vehicle-Mounted Cameras in Smart Cities. Electronics. 2023;12(17):3621. https://doi.org/10.3390/electronics12173621
3. Brandão A, São Mamede H, Gonçalves R. A smart city's model secured by blockchain. In: Trends and Applications in Software Engineering: Proceedings of the 7th International Conference on Software Process Improvement (CIMPS 2018). Springer International Publishing; 2019. https://doi.org/10.1007/978-3-030-01171-0_23
4. Gallo P, Pongnumkul S, Nguyen UQ. BlockSee: Blockchain for IoT video surveillance in smart cities. In: 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe). IEEE; 2018. https://doi.org/10.1109/EEEIC.2018.8493895
5. Lee BK, Ahn M, Han SJ. Intelligent BlockChain-based P2P Energy Trading Service Research about the Platform. The Journal of Innovation Industry Technology. 2023;1(3):107-113. https://doi.org/10.60032/JIIT.2023.1.3.107
6. Zhang M, et al. Blockchain-based collaborative edge intelligence for trustworthy and real-time video surveillance. IEEE Transactions on Industrial Informatics. 2022;19(2):1623-1633. https://doi.org/10.1109/TII.2022.3203397
7. Vanin FNS, et al. A Blockchain-Based End-to-End Data Protection Model for Personal Health Records Sharing: A Fully Homomorphic Encryption Approach. Sensors. 2022;23(1):14. https://doi.org/10.3390/s23010014
8. Lee D, Park N. Blockchain based privacy preserving multimedia intelligent video

surveillance using secure Merkle tree. Multimedia Tools and Applications. 2021;80:34517-34534. doi:10.1007/s11042-020-08776-y
9. Peyrone N, Wichadakul D. A formal model for blockchain-based consent management in data sharing. Journal of Logical and Algebraic Methods in Programming. 2023;134:100886. https://doi.org/10.1016/j.jlamp.2023.100886
10. Li G, et al. Blockchain-enhanced spatiotemporal data aggregation for UAV-assisted wireless sensor networks. IEEE Transactions on Industrial Informatics. 2021;18(7):4520-4530. https://doi.org/10.1109/TII.2021.3120973
11. Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops. IEEE; 2015. https://doi.org/10.1109/SPW.2015.27
12. Manogaran G, et al. Blockchain assisted secure data sharing model for Internet of Things based smart industries. IEEE Transactions on Reliability. 2021;71(1):348-358. https://doi.org/10.1109/TR.2020.3047833
13. Zhao J, et al. Research on medical data storage and sharing model based on blockchain. High-Confidence Computing. 2023;100133. https://doi.org/10.1016/j.hcc.2023.100133
14. Post R, Kas S, Smit K. The role of modeling in blockchain process design. In: Business Process Management: Blockchain and Robotic Process Automation Forum: BPM 2020 Blockchain and RPA Forum, Seville, Spain, September 13–18, 2020, Proceedings. Springer International Publishing; 2020. https://doi.org/10.1007/978-3-030-58779-6_4
15. Soujanya D, Ramana KV. Secured Surveillance Storage Model Using Blockchain. In: Evolving Technologies for Computing, Communication and Smart World: Proceedings of ETCCS 2020. Springer Singapore; 2021. https://doi.org/10.1007/978-981-15-7804-5_19
16. Jingwen L, Xiaoou L, Jun Z, Wei L, Lening G. Application Model of Video Surveillance System Interworking Based on Blockchain. In: 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC). Vol. 4. IEEE; 2021. https://doi.org/10.1109/IMCEC51613.2021.9482064
17. Li J, et al. Application Model of Video Surveillance System Interworking Based on Blockchain. 2021 IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC). IEEE; 2021. https://doi.org/10.1109/IMCEC51613.2021.9482064
18. Xin Q, Yu K, Wen Z, Hlaing Myint S, Katsuyama Y, Sato T, Tokuda K, Sato T. Blockchain-based Content-oriented Surveillance Network. In: 2020. https://doi.org/10.1109/VTC2020-Spring48590.2020.9128532
19. Jain P, Dwivedi S, Alharbi AR, Sureshbabu R, Singh DP, Jamal SS, Krah D. Blockchain-Enabled Smart Surveillance System with Artificial Intelligence. Wireless Communications and Mobile Computing. 2022. https://doi.org/10.1155/2022/2792639
20. Jeong Y, Hwang D, Kim K-H. Blockchain-based management of video surveillance systems. In: 2019 International Conference on Information Networking (ICOIN). IEEE; 2019. https://doi.org/10.1109/ICOIN.2019.8718126
21. Maltare, N. N., Sharma, D., Patel, S. (2023). An Exploration and Prediction of Rainfall and Groundwater Level for the District of Banaskantha, Gujrat, India. International Journal of Environmental Sciences, 9 (1), 1-17 https://www.theaspd.com/resources/v9-1-1-Nilesh%20N.%20Maltare.pdf
22. Min, P.K., Mito, K. and Kim, T.H. (2024). The Evolving Landscape of Artificial Intelligence Applications in Animal Health. Indian Journal of Animal Research. https://doi.org/10.18805/IJAR.BF-1742
23. Kim, T. H. and AlZubi, A.A. (2024). AI Enhanced Precision Irrigation in Legume Farming: Optimizing Water Use Efficiency. Legume Research. https://doi.org/10.18805/LRF-791