Applied Artificial Intelligence and Computing Systems
https://www.scigate.org
Science Gate Academic
Vol. 1, No. 1, 2025

Article

Blockchain-Based Secure Video Data Protection Framework Enhanced with National Cryptographic Algorithms

Tilda Marwick
Eastern Washington University, Cheney, USA
tmarwick.220@ewu.edu

Abstract: *This paper proposes a blockchain-based security protection framework for video data, integrating the SM2, SM3, and SM4 algorithms to achieve high-level data integrity, privacy, and reliability. The framework addresses the vulnerabilities of traditional centralized storage, such as single-point failures and tampering risks, by employing a consortium blockchain architecture with distributed storage and multi-node consensus mechanisms. The SM4 algorithm is used for data encryption and storage, SM2 for identity authentication and digital signatures, and SM3 for hash computation and traceability. Through the integration of smart contracts, the system achieves fine-grained access control and end-to-end auditability, ensuring that only authorized entities can access or modify video data. Experimental implementation on a four-node consortium chain demonstrates secure data transmission, verifiable access records, and efficient consensus execution. The proposed framework significantly enhances the reliability, transparency, and security of video surveillance systems and shows broad potential for application in smart city management, public safety, and industrial monitoring.*

Keywords: *Blockchain security; video data protection; SM cryptographic algorithms; consortium blockchain; data integrity*

1. Introduction

Video surveillance systems, as critical infrastructure for public safety and operational efficiency enhancement, have gained ubiquitous deployment across diverse sectors including transportation, finance, education, and healthcare. The global market for public safety video surveillance applications demonstrates an irreversible growth trajectory. According to the latest market analysis from Wealth Business Monitor, this sector is projected to maintain a robust compound annual growth rate (CAGR) of 16.8% during the forecast period from 2022 to 2029[1]. However, this rapid market expansion, characterized by high market share concentration, substantial profit margins, increasingly complex system architectures, and diversified application scenarios, has concurrently amplified the security challenges confronting video systems. The primary security concerns can be categorized as follows:

(1)Data vulnerability exposure: Video data repositories contain substantial volumes of sensitive information, including but not limited to facial recognition data, vehicle license plate information, and behavioral patterns. Unauthorized access to such data could precipitate severe consequences ranging from personal privacy violations to corporate espionage. Conventional centralized storage architectures are particularly susceptible to targeted cyberattacks, resulting in recurrent data breach incidents.

(2)Data integrity compromise: Serving as crucial evidentiary material in judicial proceedings, the authenticity and integrity of video data are paramount. Nevertheless, traditional storage methodologies lack robust mechanisms to prevent malicious data manipulation or unauthorized deletion, thereby undermining the evidentiary value of such recordings.

(3)Storage infrastructure vulnerability: Centralized data storage systems are inherently susceptible to single-point-of-failure scenarios. Any disruption to the storage servers, whether through system failures or cyberattacks, could potentially lead to catastrophic data loss or service outages.

(4)Unauthorized system access: Networked video systems are particularly vulnerable to illicit access attempts. Cyber adversaries may exploit system vulnerabilities or weak authentication protocols to gain unauthorized access, potentially leading to data exfiltration or system compromise.

These security vulnerabilities pose significant threats that extend beyond mere system operational disruptions, potentially resulting in substantial societal repercussions and economic ramifications. While conventional security mechanisms, including firewalls and intrusion detection systems, have contributed to enhanced system protection, they exhibit inherent limitations in addressing contemporary security challenges. Specifically, the centralized storage paradigm fundamentally lacks the capability to ensure data integrity against sophisticated tampering attempts. Moreover, traditional cryptographic approaches may prove inadequate against emerging threats, particularly in the era of quantum computing advancements. Consequently, the imperative for developing innovative technological solutions has become increasingly urgent. Such solutions must adopt a holistic approach to fortify video system security, encompassing robust data protection mechanisms, resilient network security frameworks, and comprehensive application-level safeguards to address the multifaceted security requirements of modern video surveillance systems.

2. Key technology analysis

2.1 Blockchain Architecture

Blockchain technology, functioning as a distributed and tamper-resistant database, operates through a collaborative maintenance mechanism involving all participating nodes within the system. These nodes collectively establish an extensive Peer-to-Peer (P2P) network architecture. Within this decentralized, peer-to-peer framework, the creation of a new block by any node triggers a broadcast mechanism that disseminates the information to adjacent nodes. Subsequent to rigorous verification processes, these nodes propagate the validated data throughout the network. The block achieves official integration into the blockchain only upon successful verification by a majority consensus of nodes within the entire system.

The blockchain's transactional integrity is maintained through cryptographic hash values recorded within each block, ensuring both data transparency and traceability. This distributed ledger technology exhibits several distinctive security-enhancing characteristics, including high redundancy storage, unforgeability, tamper resistance, efficient smart contract execution, and robust privacy protection mechanisms. The system's security is further reinforced by its inherent verification protocols: any unauthorized modification attempt on a block would be detected during the verification process by other nodes, rendering the altered data invalid across the network. The blockchain's sequential chain structure significantly increases the complexity of data tampering, as any attempt to legitimize altered data would

require control over more than 50% of the network's computational power and modification of all subsequent blocks[2], making such attempts economically infeasible due to the disproportionate cost-benefit ratio.

The blockchain platform architecture employs a sophisticated layered design paradigm, with each stratum dedicated to specific functional components[3]. As illustrated in Figure. 1, the fundamental architecture of blockchain technology comprises four primary layers.

The blockchain architecture comprises six fundamental layers, each serving distinct functions within the system:

(1)Data Layer: Serving as the foundational stratum, this layer employs a block-based data storage mechanism where all transactional information is encapsulated within interconnected data nodes. The primary function of this layer involves the structural organization of raw data into coherent blocks. Each block is characterized by specific metadata, including block size, header information, transaction count, and a comprehensive or partial record of recent transactions. This structural integrity ensures the chronological and cryptographic linkage of blocks within the chain.

(2)Network Layer: Functioning as the communication infrastructure, this layer facilitates decentralized information exchange among network participants. It incorporates three core components: P2P network protocols, data dissemination mechanisms, and verification processes. The P2P architecture ensures network resilience, as data transmission occurs through multiple independent nodes, maintaining system functionality even when individual nodes or network segments are compromised.

(3)Consensus Layer: This critical stratum enables distributed nodes within the P2P network to achieve agreement on block validity and determine the authoritative chain. Numerous consensus algorithms have been developed, with notable implementations including Proof of Work (PoW) [4], Proof of Stake (PoS) [5], and Delegated Proof of Stake (DPoS) [6]. These mechanisms ensure network integrity while addressing the Byzantine Generals Problem in distributed systems.

(4)Incentive Layer: Designed to promote network participation and security, this layer implements economic incentives for node operators. Through the consensus mechanism, nodes that successfully validate and add blocks receive compensation, typically comprising block generation rewards and transaction fees. This economic model, exemplified by Bitcoin and Ethereum networks, aligns participant incentives with network security objectives.

(5)Contract Layer: This programmable stratum encapsulates various scripts, algorithms, and contractual protocols, enabling automated execution of complex operations. Smart contracts, as self-executing protocols with predefined conditions, facilitate automated transactions and data operations. These contracts can autonomously read from and write to the blockchain, trigger subsequent contracts, and execute predefined logic, thereby reducing reliance on human arbitration and minimizing trust-related costs.

(6)Application Layer: Representing the highest abstraction level, this layer implements blockchain technology across diverse use cases. It encompasses three primary programmable domains: currency systems (e.g., cryptocurrencies), financial applications (e.g., decentralized finance), and societal applications (e.g., governance systems). This layer demonstrates the technology's versatility in addressing various real-world challenges through programmable solutions.

2.2 Consortium Blockchain

Based on the application of blockchain technology across various industries and the associated access control mechanisms, mainstream blockchain systems can be classified into two primary categories: Public Blockchain and Consortium Blockchain[7].

Public Blockchain represents a fully open and permissionless system where any global participant can access the network at any time to read data, submit verifiable transactions, and participate in the consensus process. These systems are characterized by complete decentralization, as no single entity or organization can control or manipulate data access and modification. The transparency and immutability of public blockchains are maintained through cryptographic mechanisms and distributed consensus protocols.

Consortium Blockchain, alternatively referred to as Federated Blockchain, operates within a more controlled environment, typically established among multiple pre-approved organizations with mutually verified identities. This architecture is particularly suitable for applications such as interbank payment settlements, enterprise supply chain management, and intergovernmental data sharing. Positioned between public and private blockchains, consortium chains exhibit partial decentralization characteristics. Access to the network is restricted to authorized members, with read, write, and consensus participation rights governed by predefined rules and permissions.

The consortium blockchain model is collaboratively maintained by institutional members, incorporating essential functionalities including member management, authentication, authorization protocols, monitoring systems, and auditing mechanisms. The system's strong controllability stems from its rigorous identity verification processes and permissioned node conFigureuration, where all participants are identifiable entities. To ensure robust security, each node implements multi-layered protection mechanisms. The architecture supports cross-chain interoperability through verified message authentication and effective identity verification protocols.

Data accessibility within consortium chains follows a need-to-know basis, with information visibility restricted to authorized internal organizations and their designated users. The limited number of participating nodes facilitates faster consensus achievement and enhanced transaction processing speeds compared to public blockchains. Consortium chains typically support multiple programming languages, simplifying deployment and execution processes. A prominent example of consortium blockchain implementation is the Hyperledger Fabric system[8], which has gained significant adoption in enterprise and institutional settings.

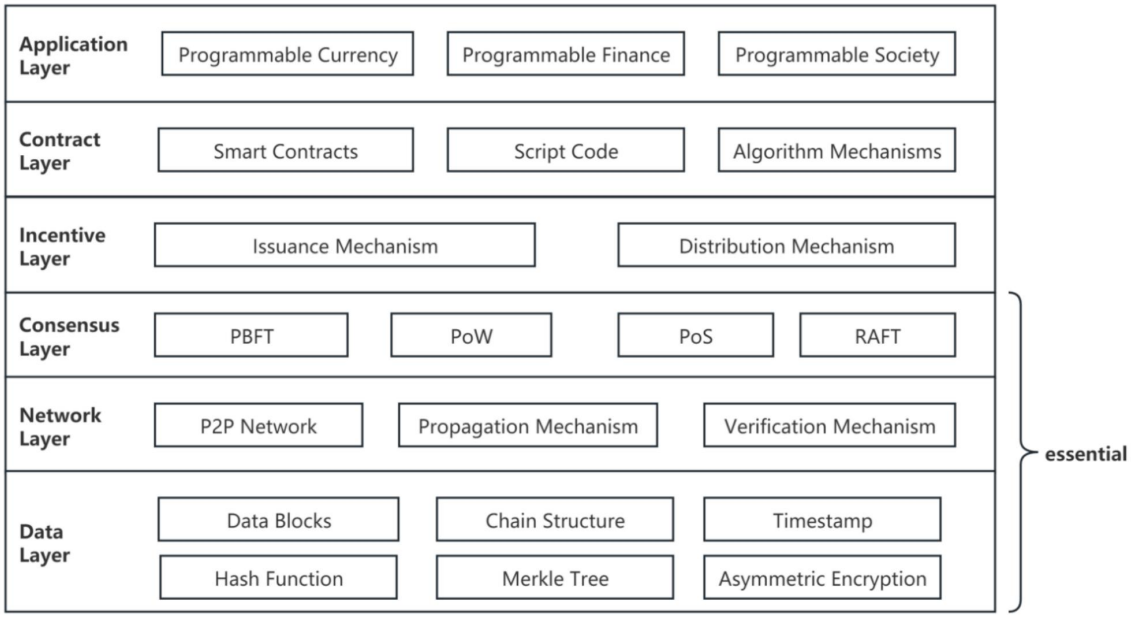

Figure 1. Common blockchains architecture

2.3 SM Algorithm

Cryptographic technology, serving as the foundational pillar of information security infrastructure, provides essential security features and reliability. As a critical strategic resource for national security, cryptographic technology has been extensively deployed across vital information infrastructure, national economic systems, and various sectors of social development. It represents the crucial safeguard for national political security, economic stability, national defense capabilities, and information protection. In recognition of its strategic importance, nations worldwide are actively developing proprietary encryption technologies. The SM cryptographic algorithm series, independently developed and innovated by China, encompasses a comprehensive suite of data encryption processing algorithms, including symmetric, asymmetric, and hash functions, designated as SM1 through SM4.

The SM2 algorithm[9], a prominent member of this cryptographic suite, represents an advanced asymmetric cryptographic algorithm based on the computational complexity of solving discrete logarithm problems. This algorithm demonstrates superior performance in several critical aspects, including plaintext encoding efficiency, decryption accuracy verification, encrypted data length management, and computational efficiency during encryption processes. In practical implementations, the SM2 algorithm exhibits notable characteristics of high-speed processing and minimal computational overhead. As an implementation of Elliptic Curve Cryptography (ECC), SM2 outperforms traditional RSA algorithms in both signature generation speed and key generation efficiency. The comparative analysis between SM2 and RSA algorithms is presented in Table 1, highlighting the performance advantages of the SM2 implementation.

Table 1. Comparison between SM2 algorithm and RSA algorithm

	RSA algorithm	SM2 algorithm
Computing structure	Provide special reversible modular exponentiation operations	Elliptic Curve
Computational complexity	Sub exponential level	security exponential level
The required number of public key bits under the same security	-	-
performance	more	less
Key generation speed	Slow	More than 100 times faster than RSA algorithm
Decryption and encryption speed	average	fast
security	The difficult problem based on decomposing large integers	Based on discrete logarithm and fcdlp problems

The SM3 algorithm[10], a cryptographic hash function , serves critical functions in digital security applications. This algorithm is primarily employed for message authentication code generation and verification, digital signature creation and validation, and secure random number generation. As an enhanced implementation derived from the SHA-256 framework, the SM3 algorithm incorporates several technical improvements while maintaining the fundamental Merkle-Damgard structure. The algorithm processes message blocks of 512 bits and generates a 256-bit hash value, ensuring robust cryptographic strength and computational efficiency. The technical specifications and performance characteristics of the SM3 algorithm, particularly in comparison with SHA-256, are systematically presented in Table 2, highlighting its enhanced features and operational advantages within the Chinese SM cryptographic framework.

The SM4 algorithm, a symmetric block cipher, represents a significant advancement in data encryption technology. As an openly available cryptographic standard, SM4 employs a sophisticated 32-round nonlinear iterative structure in both its encryption and key expansion processes. The algorithm's core operations encompass multiple cryptographic primitives, including exclusive OR (XOR) operations, composite permutations, nonlinear transformations, inverse operations, cyclic shifts, and S-box substitutions. A distinctive feature of SM4 is its symmetric mathematical architecture, where the encryption and decryption processes share identical operational rules and structures, with decryption achieved simply by applying the round keys in reverse order.

The SM4 algorithm has found primary application in ensuring the security and confidentiality of wireless local area network (WLAN) products, providing robust protection for data transmission in wireless environments. The technical specifications and performance metrics of SM4, particularly when compared with the Triple Data Encryption Standard (3DES), are systematically presented in Table 3. This comparison highlights SM4's enhanced security features and computational efficiency, demonstrating its advantages in modern cryptographic applications.

Table 2. Comparison between SM3 algorithm and SHA-256

	SHA-256	SM3 algorithm
Computing structure	fundamental data structure	Merkle-Damgard
Digests length	256	256
Key generation speed	average	fast
Decryption and encryption speed	average	fast
security	High	higher

Through comprehensive comparative analysis between SM cryptographic algorithms and their international counterparts, empirical evidence demonstrates the superior performance characteristics of China's indigenous cryptographic solutions. The SM encryption algorithms exhibit enhanced security properties and improved encryption/decryption processing speeds compared to established international standards. This performance advantage signifies that China's independently developed cryptographic system offers greater practical utility in critical areas of data security protection and cryptographic processing efficiency. The technical superiority of these algorithms manifests in multiple dimensions, including but not limited to computational efficiency, resistance to cryptanalytic attacks, and implementation flexibility, positioning them as competitive alternatives in the global cryptographic landscape.

3. Transforming Blockchain with SM Algorithm

3.1 Transforming Method

The integration of SM algorithms into blockchain systems significantly enhances their security and autonomous controllability. This transformation can be systematically implemented through the following technical modifications:

(1)Cryptographic Algorithm Replacement:

a)Consensus Mechanism Enhancement:

Substitute SHA-256 in Proof-of-Work (PoW) mechanisms with the SM3 hash algorithm. Replace ECDSA signature algorithms in Proof-of-Stake (PoS) and other consensus mechanisms with SM2.

b)Network Communication Security:

Implement SM2 for node identity authentication and key agreement protocols.

Utilize SM4 for encrypting network transmission data to ensure secure communication channels.

c)Data Storage Management:

Apply SM3 for hashing block and transaction data to maintain data integrity. Employ SM4 for encrypting sensitive data storage to prevent unauthorized access. (2)Protocol Layer Transformation:

a)Node Discovery Protocol:

Implement SM2 for node identity verification to prevent infiltration of malicious nodes.

b)Data Transmission Protocol:

Integrate SM2 and SM4 for data encryption and digital signatures.

Ensure secure and reliable data transmission through cryptographic protection.

c)Smart Contract Integration:

Embed SM cryptographic algorithms into smart contract functionality.

Enable advanced features including data encryption and signature verification. (3)Application Layer Transformation:

a)Wallet Security Enhancement:

Implement SM2 for private key generation and management. Utilize SM3 for secure address generation.

b)Exchange Security Upgrade:

Apply SM cryptographic algorithms for user asset protection. Encrypt trading data using standardized cryptographic protocols.

c)Decentralized Application (DApp) Integration:

Incorporate SM cryptographic algorithms into DApp architecture.

Enable secure data storage and robust identity authentication mechanisms.

This comprehensive transformation approach ensures the systematic integration of SM cryptographic standards throughout the blockchain ecosystem, enhancing both security and regulatory compliance while maintaining system performance and functionality.

3.2 Architecture

The architectural framework of the consortium blockchains supporting SM algorithms through a layered design approach comprises several core components, each serving distinct functions within the system. As illustrated in Figureure 2, this architecture demonstrates a hierarchical structure that integrates cryptographic security at multiple levels.

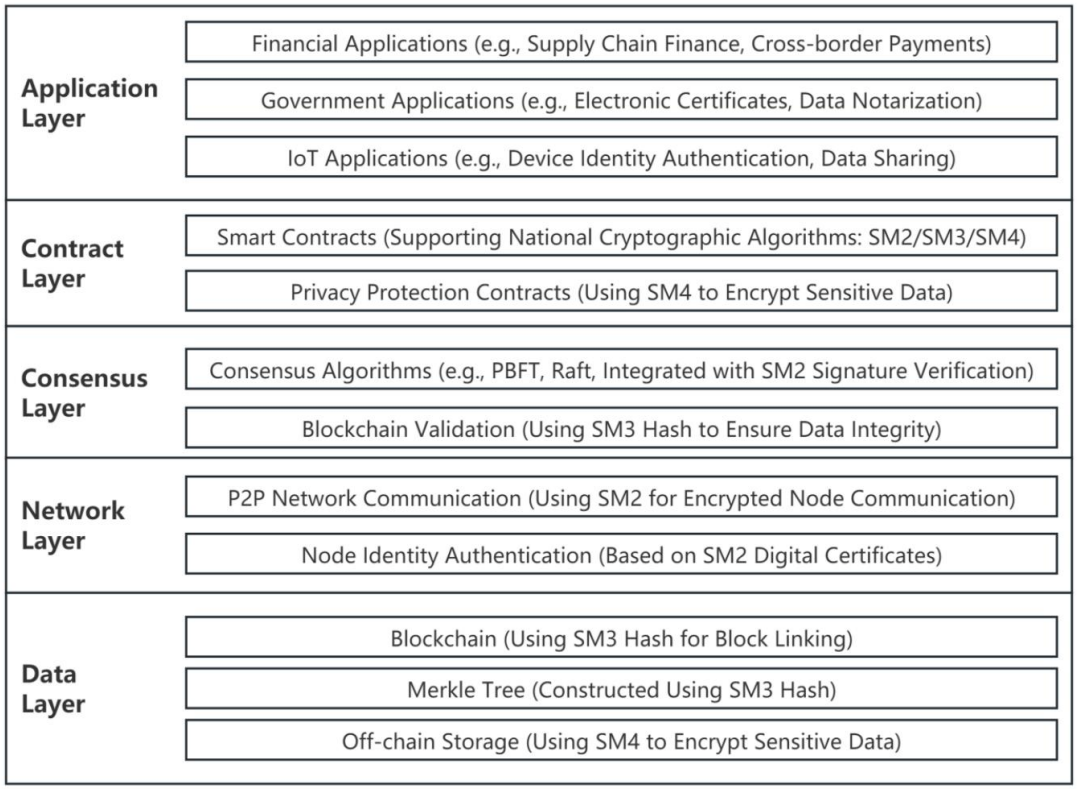

Figure 2. Consortium Blockchains Architecture Supporting SM Algorithms

3.3 Transaction Signature Verification Process

The transaction signature verification process within the SM cryptographic algorithm- enhanced blockchain system can be delineated through the following comprehensive workflow:

(1)Node Registration Phase:

a)Generate cryptographic key pair for Node A using SM2 algorithm: Private key: dA

Public key: pA

b)Compute user identifier hash value ZA using SM3

c)Securely store dA and ZA using local encryption mechanisms (2)Transaction Signature Phase:

a)Preprocess transaction data D to obtain normalized data D1

b)Generate cryptographic hash of D1 using SM3 algorithm:

Hash value: e = SM3(D1)

c)Create digital signature using SM2 signature algorithm:

Signature: SIGT = SM2-Sign(e, dA) d)Construct signed transaction package:

TA1 = {TA, pA, SIGT}

e)Broadcast TA1 to the network through P2P propagation (3)Transaction Verification Phase:

a)Designated block-generating nodes (consortium chain master nodes) collect unverified transactions

b)Validate transaction integrity through SM2 signature verification:

Verify SIGT using pA and e

c)Upon successful verification:

Mark TA as valid

Include in new block creation Propagate updated blockchain state

The system architecture provides modular transaction consensus through custom interfaces, enabling flexible consensus algorithm implementation. The protocol architecture is divided into two primary modules:

(1)Transaction Processing Module:

a)Transaction Pool: Implements caching mechanism for pending transactions

b)Thread Management:

c)Initialization: Starts transaction processing threads d)Synchronization: Blocks threads during consensus confirmation

e)Consensus Interface: Provides transaction-specific consensus implementation (2)Consensus Module:

a)Transaction Lifecycle Management:

Creation: Generates new transactions Propagation: Implements network broadcasting Finalization: Manages blockchain update process b)Consensus Mechanism:

Coordinates transaction validation Manages block creation

Handles chain synchronization

This architecture ensures secure transaction processing through SM algorithms while maintaining system flexibility and performance. The modular design facilitates customization and scalability of consensus mechanisms, supporting various application requirements within the consortium chain environment.

4. Security protection scheme based on Transforming Blockchain with SM Algorithm

4.1 Scheme Design

As a critical component of intelligent security systems, video data plays a pivotal role in key areas such as criminal investigations, civil litigation, public safety, and social research. However, with the rapid advancement of network technology, malicious actors frequently exploit cyber- attack methods to engage in illegal activities such as data fraud. Concurrently, traditional video data storage solutions face the risk of permanent data loss due to single points of failure, leading to potentially immeasurable economic losses.

To address the challenges of video data loss from local single-point servers and the susceptibility to attacks and tampering when stored in the cloud, this project proposes a security protection framework for video data based on an "Alliance Chain" architecture enhanced with SM algorithms. Specifically, the framework encompasses the following aspects:

(1)Data Encryption and Storage: The SM4 algorithm is employed to encrypt video data, ensuring its security during both transmission and storage. The encrypted data is then stored on blockchain nodes, leveraging the immutable nature of blockchain technology to prevent data tampering.

(2)Identity Authentication and Access Control: Utilizing the SM2 algorithm, the framework implements mutual authentication between devices and users to prevent unauthorized access by

illegitimate devices or users. Additionally, by integrating blockchain smart contracts, fine-grained access control is achieved, ensuring that only authorized users can access the video data.

(3)Data Traceability and Auditing: By harnessing the traceability features of blockchain, the framework records and audits the entire lifecycle of video data, including its generation, transmission, and access. This facilitates traceability and accountability in the event of a security incident.

4.2 Algorithm Design

(1)SM2

In the consortium chain, the SM2 algorithm is applied to the signing and verification of transactions. Transactions are a fundamental component of the consortium chain system, and all other system components are designed to ensure that transactions can be generated, propagated, validated, and ultimately added to the global ledger of the network. A transaction is essentially a data structure comprising three main parts: the transaction hash, transaction data, and transaction signature. The transaction hash, consisting of 32 bytes, serves as a unique identifier for the transaction. The transaction data, composed of mutable bytes, is used to store on-chain information. The transaction signature, generated using the SM2 algorithm, is 64 bytes in length and ensures the authenticity and integrity of the transaction.

(2)SM3

In a blockchain system based on SM cryptographic algorithms, the SM3 algorithm is utilized for computing hash values and Merkle roots. The block header contains three sets of metadata. The first set includes the hash value of the previous block, which links the current block to its predecessor in the blockchain. The second set comprises the Merkle tree root, which encapsulates the transaction information of the current block. The Merkle root in the block header is derived by recursively hashing pairs of transaction hashes until a single root hash is obtained. This root hash serves as a unique identifier for all transactions within the block and is stored in the block header. By applying the SM3 algorithm to perform a secondary hash calculation on the block header data, a 32-byte block hash value is generated, uniquely identifying the block.

Compared to traditional blockchain architectures, the consortium chain architecture enhances the scalability of consensus algorithms, reduces time and memory overhead in signature verification, and enables flexible application of consensus mechanisms. By adopting the SM3 algorithm as the digest algorithm for the blockchain, the resulting block hash values are securely stored and utilized.

(3)Communication Protocol

In the SM cryptographic algorithm-based blockchain, the communication protocol between nodes and clients relies on OpenSSL. The cryptographic suite, which replaces RSA and AES with SM2 and SM3 algorithms, facilitates the transmission of transactions from clients to nodes and ensures consensus among nodes. SSL connections between nodes are established using the ECC key exchange algorithm, specifically the ECDHE_SM3_with_SM4 cryptographic suite, which provides forward secrecy and enhanced security.

4.3 System Design and Implementation

Build a 4-node consortium chain locally and conFigureure all four nodes to belong to the same group. Deploy the consortium chain based on SM cryptographic algorithms, using the IP addresses and ports of the nodes as conFigureuration parameters. Establish SSL-secured communication channels to enable secure information exchange among the four nodes. This conFigureuration includes specifying the absolute path of certificate files, the relative path of node private keys, and the relative path of certificates.

Deploy smart contracts on the consortium chain to facilitate the acquisition of monitoring videos. To enhance video access efficiency, compute and generate hash values using the SM3 algorithm. Store these video hash values on the consortium chain to ensure data integrity and tamper resistance.The system adopts B/S architecture, as shown in Figureure 3.

Users can access video data, including hash values, node information, and other related metadata, directly from the consortium chain. The system features a graphical interface for data visualization, which simplifies usability for management personnel and provides an intuitive and visually engaging representation of the platform's functionalities. When users navigate to the "Video Surveillance" page on the web interface, the front-end sends a query request to the backend server. The server processes the request, retrieves the video's on-chain address, and queries the corresponding hash value. Once the data is acquired, it is stored in an array and transmitted to the front-end. The front-end then populates the data into the appropriate sections of the page for rendering, presenting the information to the user. This process facilitates seamless interaction between the front-end and back-end systems, culminating in the final rendered output.

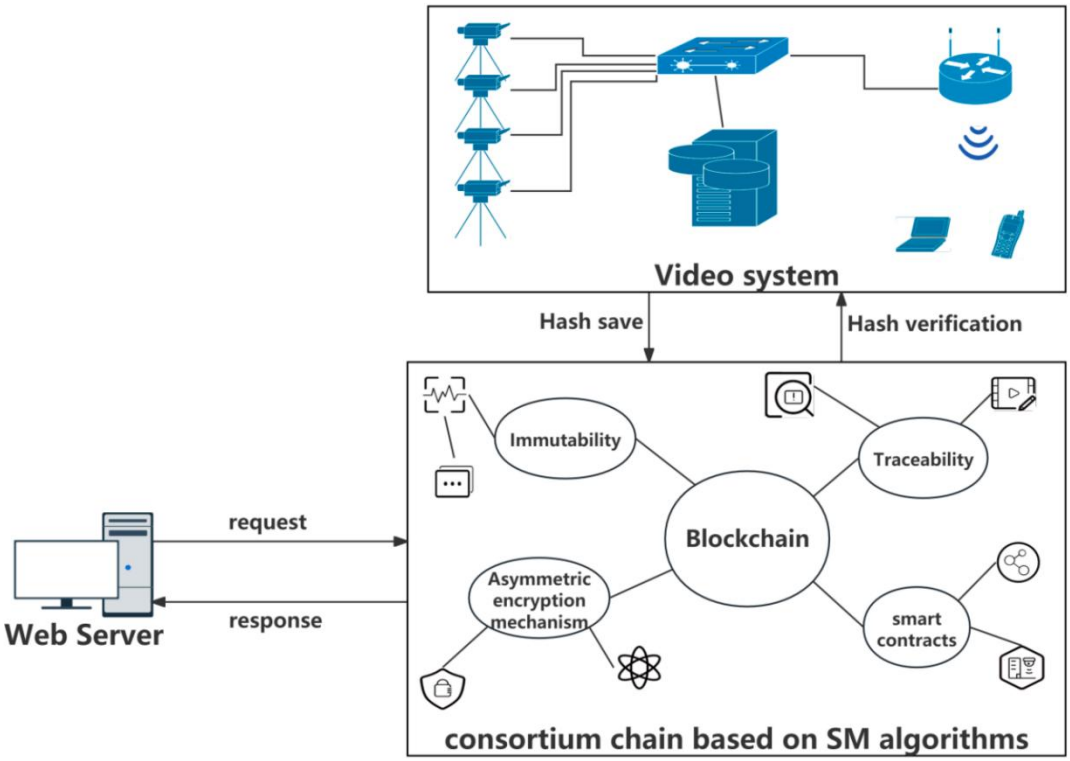

Figure 3. System architecture

5. Conclusion

This solution offers significant advantages over traditional video security protection methods:

(1)The decentralized storage architecture mitigates the risk of single points of failure, enhancing system reliability and resilience against attacks.

(2)The tamper-proof nature of blockchain ensures the authenticity and integrity of video data, providing a reliable foundation for judicial evidence collection.

(3)The application of SM algorithms strengthens data encryption, effectively countering emerging attack methods.

(4)The use of smart contracts enables fine-grained access control, better safeguarding user privacy.

This solution holds broad application potential in fields such as smart city development, public safety, and industrial monitoring. For instance, in smart city management, it can facilitate the creation of a cross-departmental and cross-regional video data sharing platform, improving urban governance efficiency. In public safety, it can provide reliable video evidence for criminal investigations. In industrial production, it enables comprehensive monitoring and quality traceability throughout the production process. As the technology continues to mature and application scenarios expand, the video data security protection solution based on SM algorithm-enhanced blockchain will play an increasingly vital role across diverse domains.

References

[1] Cheng Le. Layout and Optimization of China's Public Safety Video Surveillance System [J]. People's Forum, 2024 (23).

[2] Sayeed S, Marco-Gisbert H. Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack [J]. Applied Sciences, 2019, 9(9):1788. DOI:10.3390/app9091788.

[3] Shen Xin, Pei Qingqi, Liu Xuefeng. Overview of Blockchain Technology [J]. Journal of Network and Information Security, 2016, 2 (11): 11-20.

[4] Gervais A, Karame G O, Karl Wüst, et al. On the Security and Performance of Proof of Work Blockchains [J]. ACM, 2016. DOI:10.1145/2976749.2978341.

[5] Tang D, He P, Fan Z, et al. Pool competition and centralization in PoS blockchain network [J]. 2024.

[6] Xin W. Improvement of DPoS Consensus Algorithm Based on Blockchain [J]. Computer Science and Application, 2022. DOI:10.12677/csa.2022.1211255.

[7] Meng T, Zhao Y, Wolter K, et al. On Consortium Blockchain Consistency: A Queueing Network Model Approach [J]. IEEE Transactions on Parallel and Distributed Systems, 2021, PP(99):1-1. DOI:10.1109/TPDS.2021.3049915.

[8] Androulaki E, Manevich Y, Muralidharan S, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains [J]. 2018. DOI:10.1145/3190508.3190538.

[9] Wang Chaohui, Zhang Zhenfeng. Overview of SM2 elliptic curve public key cryptography algorithm [J]. Information Security Research, 2016, 2 (11): 972-982.

[10] Wang Xiaoyun, Yu Hongbo. SM3 Password Hash Algorithm [J]. Information Security Research, 2016, 2 (11): 983-994.

[11] Lv Shuwang, Su Bozhan, Wang Peng, et al. Overview of SM4 Block Cipher Algorithm [J]. Information Security Research, 2016, 2 (11): 995-1007.