https://doi.org/10.26599/IJCS.2024.9100031 International Journal of Crowd Science

Research on Blockchain-Based Intrinsic Security Mechanisms for Satellite Internet

Jiandong Liu[1] ✉, Hailong Kang[1], Feipeng Wu[2], Wenbo Wei[3], and Xichao Hou[3]

ABSTRACT

In the context of rapid globalization and the swift advancement of information technology, satellite internet has emerged as a critical infrastructure for global communication services, drawing unprecedented attention to its security challenges. Traditional security measures are increasingly inadequate, struggling to meet the high standards of security, transparency, and reliability required by modern communication networks. Blockchain technology, with its unique attributes such as decentralization, immutability, and smart contracts, presents a promising solution to these security concerns. This paper explores blockchain-based intrinsic security mechanisms for satellite internet, with a particular emphasis on key components such as trusted accounts, data encryption, and access control. The objective is to propose a robust set of strategies and provide technical support for the security management of satellite internet, ultimately aiming to enhance the security and reliability of satellite communication networks on a global scale.

KEYWORDS

blockchain; satellite communication; network security; security architecture; information security

Satellite internet plays a vital role in providing connectivity to remote and maritime regions. However, the evolution of network attack technologies has introduced significant security threats, including signal interception, data tampering, malicious control, and denial-of-service attacks. Traditional security measures are increasingly inadequate, highlighting the need for innovative solutions. Blockchain technology, with its inherent decentralization, data immutability, and transparency, offers promising possibilities for enhancing the security of satellite internet. By integrating blockchain, a more secure, reliable, and autonomous communication network can be established, leading to improved data transmission security, enhanced resistance to attacks, and strengthened device security and identity authentication.

This study investigates the application of blockchain technology in constructing intrinsic security mechanisms for satellite internet, aimed at addressing both current and emerging security challenges. By analyzing the core characteristics and security advantages of blockchain, the study demonstrates comprehensive security protection and validates the proposed solutions through detailed case studies.

This research holds significant theoretical and practical value in advancing satellite internet security, with far-reaching implications for future commercial applications and the broader process of social informatization.

1 Work Background and Review of Related Work

1.1 Overview of satellite internet and its impact on global communication

Satellite Internet is an advanced technology that leverages satellite communication to achieve global internet coverage. By deploying satellite networks in Earth's orbit, this large-scale system is able to provide broadband internet access to users on land, in the air, and at sea. As a vital supplement and extension of terrestrial networks, satellite internet helps to accelerate the narrowing of the digital divide between regions and further expands the coverage and service capabilities of ground-based networks[1].

The satellite internet system constructs a global communication network by utilizing satellites in Earth's orbit to transmit data and communication signals, especially in remote areas where terrestrial infrastructure is hard to reach. Typically, a satellite internet system consists of three components: the space segment, the ground segment, and the user segment[2].

The space segment is made up of satellite constellations that provide information relay services, ranging from a single satellite to thousands of satellites, operating in Geostationary Earth Orbit (GEO), Medium Earth Orbit (MEO), or Low Earth Orbit (LEO). The satellite system includes a space-based core network, which ensures global coverage through inter-satellite links, as well as a space-based access network. The ground segment, or ground-based core network, consists of ground stations that act as gateways connecting satellites to the internet. These include satellite control centers, system control centers, and gateway stations, responsible for managing satellite positions, trajectories, and network connectivity. The user segment comprises communication terminals, such as handheld devices, portable stations, and vehicle-mounted stations.

As illustrated in Fig. 1, those terminals connect to satellites through uplink and downlink channels, while inter-satellite links and feeder links connect the space segment with gateway stations. The impact of satellite internet on global communication is

1 China Satellite Network System Institute Co., Ltd., Beijing 100029, China
2 China Satellite Network Innovation Research Institute Co., Ltd., Beijing 100029, China
3 Beijing Weixin Perception Technology Co., Ltd., Beijing 100086, China
Address correspondence to Jiandong Liu, liujd@chinasatnet.com.cn

© The author(s) 2026. The articles published in this open access journal are distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/).

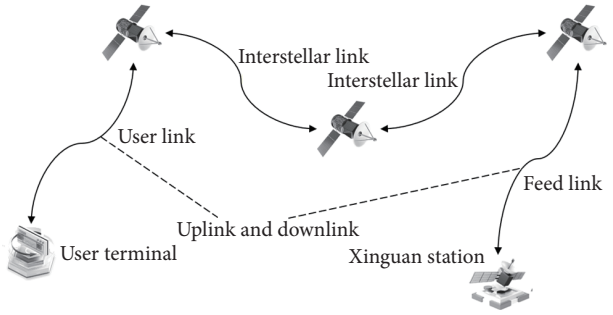


Fig. 1 Satellite internet.

profound. It not only provides full coverage in remote oceanic and polar regions, filling gaps in the global communication network, but also acts as a crucial backup during natural disasters or emergencies, ensuring reliable communication when terrestrial networks fail. Moreover, satellite internet supports mobile connectivity for aircraft and ships, which is essential for industries such as aviation and maritime transportation, while also fostering the development of emerging business models like the Internet of Things (IoTs) and Vehicle-to-Everything (V2X).

As Satellite Internet technology continues to advance, its role in global communication becomes increasingly prominent. Despite its wide coverage and diverse applications, this technology still faces numerous challenges, particularly in terms of network security. To ensure the stability and security of Satellite internet while delivering global communication services, innovative security mechanisms and strategies must be adopted.

1.2 Security challenges in satellite internet networks

As a crucial component of the global communication network the security of satellite internet is vital for ensuring the reliability and integrity of information transmission. With the rapid development of satellite internet technology, its importance in the global communication network is increasing. However, the accompanying security risks are also becoming more significant. Satellite communication systems are highly susceptible to cyberattacks, primarily including information eavesdropping, identity spoofing, and system control takeover[3].

The technical security risks of satellite internet primarily include the lack of unified security standards, risks of eavesdropping and spoofing, network attack risks, access authentication risks, and ground station security risks[4].

Lack of unified satellite network security standards: Different countries and regions adopt varying security strategies for satellite networks, leading to imbalanced global security protection. This disparity increases security risks and opportunities for cross-border attacks.

Risks of eavesdropping and spoofing: Satellite communications are susceptible to eavesdropping, where signals are intercepted to steal information, and spoofing, where forged signals interfere with or deceive satellites and ground stations.

Network attack risks: Satellite internet faces threats like viruses, trojans, and DoS attacks, which can disrupt operations, cause data leaks, or paralyze the network. Malicious software can infect satellite systems, and DoS attacks can overwhelm resources.

Access authentication risks: Incomplete access authentication mechanisms pose risks of unauthorized access. Unauthorized users may conduct illicit communications, steal sensitive information, or attack the network by forging identity information.

Ground station risks: Ground stations are critical nodes. If compromised, attackers can control the entire network, causing communication interruptions or destructive operations on satellites. Risks stem from both physical and network security aspects.

Satellite internet, despite its broad coverage, faces severe security risks like eavesdropping, spoofing, network attacks, and authentication issues. Strengthening protection through technical, managerial, and cooperative measures and developing comprehensive security standards is crucial for ensuring security and reliability. Additionally, challenges include physical facility threats, insufficient key management, and new issues from network integration.

Satellite communication systems consist of a ground segment and a space segment. The ground segment includes the main control center, monitoring center, and gateway stations. The space segment comprises satellite constellations, inter-satellite links, and satellite-to-ground links. The space segment, responsible for the transmission, forwarding, and exchange of data and signaling through microwave communication, is the core of the entire system and also the part most susceptible to security risks[5].

Satellite internet faces challenges in key management and legal monitoring mechanisms. Inadequate key management can result in decrypted communications and information leaks, while insufficient legal monitoring increases the risk of undetected illegal activities. Effective key management should encompass the entire lifecycle of keys, including generation, distribution, storage, and destruction. Robust legal monitoring mechanisms are essential for continuously overseeing network activities and ensuring secure operations.

The integration of satellite internet with ground networks introduces new security challenges, increasing the complexity of security management. Heightened data flow and interoperability issues raise the risk of data leaks and vulnerabilities. Ensuring network security requires comprehensive strategies, including multi-level protection, unified security standards, effective monitoring, and enhanced coordination between networks.

To address these challenges, it is necessary to develop comprehensive security management strategies, including multilevel security protection measures, unified security standards and regulations, and effective monitoring and response mechanisms. Additionally, strengthening coordination and cooperation between different networks to enhance overall network security protection capabilities is a crucial measure for addressing security challenges arising from integration.

1.3 Analysis of current security solutions

Satellite internet, as an advanced communication network architecture, integrates ground networks, aerial networks, and space satellite networks to form a seamless global communication system. However, this complex network system also faces multiple cybersecurity challenges, necessitating effective security measures to ensure the security and reliability of communication. The existing security solutions for satellite internet mainly involve the following aspects:

(1) Design and implementation of access authentication schemes: Given the highly dynamic topology of satellite internet and the diverse types of access users, corresponding access authentication schemes have been proposed to ensure the effective protection of the network's first line of defense.

(2) Network integration using SDN and VNF technologies: By utilizing Software-Defined Networking (SDN) and Virtual Network Function (VNF) technologies, effective integration of satellite and ground networks is achieved, thereby enhancing the

security and reliability of the network[6].

(3) Physical layer security solutions: Considering the unique nature of satellite internet information networks, security solutions that consider both the physical layer and its upper layers have been proposed, leveraging the advantages of Geostationary Earth Orbit (GEO) and Low Earth Orbit (LEO) satellites to enhance network security.

(4) Anti-jamming solutions for communication systems: The anti-jamming solution for communication systems is implemented through a three-tier protection mechanism. To achieve the switching of these three levels of protection, it is necessary to employ electromagnetic environment sensing, broadband dynamic spectrum management, comprehensive analysis and decision-making, and resource allocation assistance[7].

(5) Blockchain security solutions: Satellite networks and ground networks are heterogeneous, and satellite internet access poses security risks. The open channels and exposed nodes in satellite networks also pose security threats to resource management. Blockchain, as a decentralized technology, is very suitable for addressing the security and reliability issues of satellite internet. The blockchain-based security management architecture includes contract layers, consensus layers, and data layers[8].

Contract layer: The contract layer mainly includes smart contracts. Smart contracts run on the system in the form of script code through preset trigger conditions. Once these conditions are confirmed, they cannot be changed. When the set conditions are met, the smart contract automatically executes, thereby automating satellite network management[9].

Satellite internet, as an integrated communication network spanning ground, aerial, and space components, forms a highly sophisticated global communication system. While this network architecture provides seamless connectivity across diverse environments, it also introduces significant cybersecurity challenges that demand robust security measures. Current solutions focus on multiple aspects, including access authentication schemes tailored to the dynamic nature of satellite networks, the integration of Software-Defined Networking (SDN) and Virtual Network Function (VNF) technologies to strengthen the network's security, and physical layer security measures to protect critical infrastructure. Anti-jamming mechanisms and blockchain-based solutions have also been introduced to mitigate risks associated with signal interference and resource management vulnerabilities.

However, despite these advancements, traditional security measures tend to address specific vulnerabilities in isolation, without offering a holistic solution to the increasingly sophisticated threats posed by cyberattacks. This highlights the importance of endogenous security—a security paradigm that embeds protection mechanisms directly into the core architecture of satellite internet systems. By shifting from reactive measures to proactive, built-in security frameworks, endogenous security can enhance the system's resilience against emerging threats, ensuring the long-term reliability and integrity of satellite communication networks.

2 Design of Intrinsic Security Mechanisms for Satellite Internet

2.1 Application of blockchain architecture in intrinsic security mechanisms

Intrinsic security is an advanced methodology that embeds security measures at every stage of system design, development, and operation. The core principle of this approach is to enhance overall system security and reliability by integrating security as a fundamental component of system architecture, rather than treating it as an additional feature. The realization of intrinsic security involves multiple critical areas, from hardware to software levels, from initial design to daily maintenance, each being indispensable. Endogenous security involves system-level security considerations at the initial design stage, enabling the system to possess inherent immunity. This approach not only allows the system to passively resist malicious attacks but also actively eliminate various security risks[11].

Key characteristics of intrinsic security include:

Prevention focus: Intrinsic security strategies emphasize preventive measures, reducing security vulnerabilities through design before issues arise.

Lifecycle coverage: Security measures span the entire system lifecycle, from requirement analysis, design, implementation, deployment, maintenance, to decommissioning.

Comprehensive protection: Not only addressing external attacks but also internal threats, system misuse, and operational errors.

Blockchain technology inherently integrates multiple intrinsic security mechanisms from its inception, forming the cornerstone of its core security architecture. In constructing intrinsic security mechanisms for satellite internet, the security architecture of blockchain offers an innovative solution, effectively overcoming numerous challenges in traditional security systems. This design not only enhances data protection capabilities but also improves the overall security and reliability of the system. Blockchain technology can provide comprehensive information security protection for satellite internet, ensuring secure network access and trusted resource management. Through cryptographic methods, blockchain guarantees the immutability of data blocks, thereby enhancing the security of satellite networks. As a distributed ledger technology, blockchain can be applied within satellite networks, using a blockchain-like data structure to verify and store data, providing robust information security protection for satellite internet[2].

Smart contracts can automatically execute preset protocols and conditions, achieving automated security management. For example, smart contracts can automatically manage access permissions, ensuring that only verified users can access specific satellite data or control commands. Additionally, smart contracts can be used to automatically update security protocols, promptly responding to new threats and vulnerabilities, thereby improving the system's dynamic defense capabilities[12].

The core elements of intrinsic security mechanisms include:

(1) Decentralized architecture and encryption technologies: Leveraging the decentralized nature of blockchain and satellite communication networks, combined with encryption mechanisms, effectively mitigates single points of failure and ensures the security of data transmission.

(2) Permission management and risk assessment: Fine-grained access control is achieved through permission models, while real-time threat assessment is conducted via risk models, significantly enhancing the system's security defense capabilities.

(3) Dynamic authorization and risk monitoring: Smart contracts enable dynamic management of authorizations, and real-time risk detection services ensure rapid response to security incidents.

(4) Operational transparency and auditability: The dashboard provides real-time monitoring of system status, while logging

services record operational processes to ensure transparency and traceability.

(5) Identity verification and data integrity: Accounts authenticate identities and blockchain technology ensures data immutability, enhancing the security and reliability of the data.

(6) Full lifecycle security coverage: Security measures are integrated throughout the system's design, development, and operational stages, providing comprehensive security protection across the entire lifecycle, ensuring system stability and reliability.

(7) Privacy protection in data circulation: Multi-party secure computation and encryption technologies safeguard the privacy and security of data during cross-domain transmission.

2.2 System architecture design for intrinsic security mechanisms in satellite internet

As shown in Fig. 2, this architecture diagram presents a comprehensive intrinsic security system that integrates satellite communication and blockchain technologies, encompassing everything from foundational communication and blockchain support to data management, permission control, and risk management. Each layer has specific functions that work closely together to ensure the security, flexibility, and efficiency of the system.

2.2.1 Network layer

The network layer serves as the foundation of the system, providing core communication and data processing capabilities. It incorporates satellite communication networks and blockchain infrastructure. This layer enables efficient communication across space and ground using satellite networks, while blockchain technology ensures data transmission is transparent, immutable, and secure, forming a robust foundation for the entire system.

(1) Satellite communication network

Geostationary Earth Orbit (GEO): Satellites are positioned approximately 36 000 km from Earth, providing continuous coverage over a fixed region. Suitable for broadcasting and global communications.

Medium Earth Orbit (MEO): Satellites positioned between 2000 and 20 000 km above Earth provide broader coverage, commonly used for global navigation systems like GPS.

Low Earth Orbit (LEO): Satellites positioned between 500 and 2000 km above Earth offer lower latency, making them ideal for real-time applications such as satellite internet.

(2) Blockchain infrastructure

Peer-to-Peer (P2P) network: A decentralized network architecture where each participant, or node, acts as both a client and a server, enabling decentralized communication between nodes and ensuring secure data transmission across the network.

Virtual machines: A software-based simulation of physical computers that provide the runtime environment for blockchain, enabling the execution of smart contracts and transaction processing.

Consensus algorithms: A mechanism that ensures all participants (nodes) in a distributed network reach agreement on the information added to the blockchain. It maintains data consistency, integrity, and security across the system, even when some nodes are unreliable or malicious. These protocols are essential for achieving consensus among distributed nodes, thereby safeguarding the overall security and reliability of the blockchain system.

Smart contracts: Automated programs stored on the blockchain that execute predefined actions once specific conditions are met. They function similarly to traditional contracts, but their execution is entirely controlled by computer code, without the need for human intervention. For example, when a certain amount of cryptocurrency is received, a smart contract can automatically release the corresponding service or resource.

Trusted accounts: Trusted accounts are digital accounts certified by authoritative institutions and generated using public-private key encryption technology. They are categorized into individual trusted accounts, corporate trusted accounts, and device trusted accounts. The trusted account mechanism ensures the security of user identity verification through the pairing of public and private keys. The public key can be openly shared and is used for encrypting information, while the private key, which is exclusively held by the user, is employed for decryption. Only individuals possessing the private key can unlock the corresponding encrypted information. This mechanism guarantees the security of the account and ensures the immutability of the data.

2.2.2 Model layer

As the logical core of the system, the model layer defines the

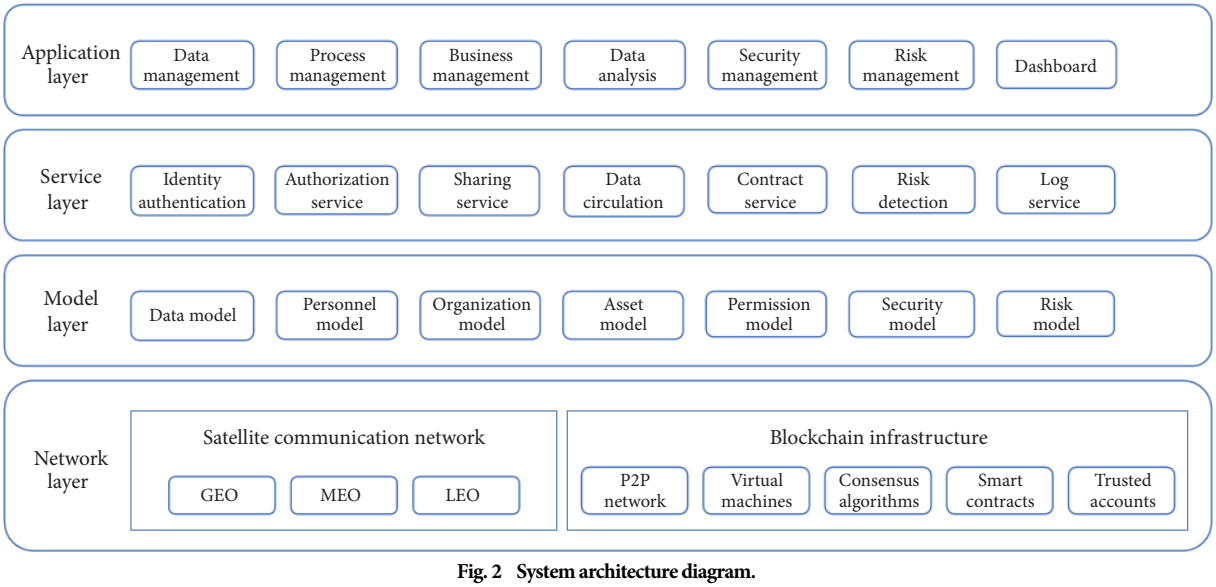


Fig. 2 System architecture diagram.

system's data, permission, and security mechanisms. Through various models, this layer manages data, users, permissions, and risks comprehensively, covering data management, permission control, organizational structure management, and security analysis. The introduction of the risk model enhances the system's risk assessment and early warning capabilities, providing a crucial safeguard for stable system operation.

Data model: Define the data structure within the system, ensuring data consistency and availability.

Personnel model: Manage user identities and permissions, including staff, devices, and other entities within the system.

Organization model: Manage hierarchical structures and internal permissions to support complex organizational architectures.

Asset model: Track and manage the system's resources and assets, ensuring effective utilization.

Permission model: Control access to system resources, ensuring only authorized users or devices can access specific resources.

Security model: Define the system's security strategies and mechanisms to protect against external threats and attacks.

Risk model: Assess potential risks within the system, providing early warnings and solutions.

2.2.3 Service layer

The service layer provides essential foundational services for the application layer, implementing core functionalities based on the logic defined in the model layer. Risk detection services leverage the risk model in the model layer to monitor the system's operational status in real-time and trigger alerts when necessary. Log services record all operations, ensuring operational transparency and traceability, facilitating auditing and tracking. Integrated with blockchain, log services record operations, transactions, and authorization changes in an immutable manner, ensuring transparency and traceability. Contract services enable automated risk management; when a certain risk threshold is detected, smart contracts automatically trigger predefined responses, such as limiting permissions, freezing accounts, or adjusting system settings, allowing for swift responses to potential threats.

Identity authentication: Ensure that all users and devices are authenticated, preventing unauthorized access.

Authorization service: Manage access permissions for users and devices, ensuring secure resource usage.

Sharing service: Facilitate the sharing and distribution of data or resources, ensuring smooth collaboration among multiple parties.

Data circulation: Manage the flow of data within the system, ensuring secure transmission between nodes.

Contract Service: Deploy and execute smart contracts, ensuring automated contract logic execution.

Risk detection: Monitor potential risk behaviors within the system, issuing alerts to prevent potential threats.

Log service: Record all operations to ensure operational transparency and traceability, supporting audits and tracking.

2.2.4 Application layer

As the core interface between users and the system, the application layer provides comprehensive business functions and operational interfaces, directly addressing users' business needs. This layer integrates various operational functions, including a risk management module for effective monitoring and response to potential risks. Real-time alert functions are integrated into the dashboard, allowing administrators to observe risk variations across different layers in real-time and take appropriate action based on the alert information.

Data management: Provide data storage, processing, and query functionalities, supporting data operations in business applications.

Process management: Manage the execution of business processes, ensuring automation and efficient operations.

Business management: Support daily business operations for enterprises or organizations, providing monitoring and optimization functions.

Data analysis: Analyze collected system data to generate reports, providing insights for business decisions.

Security management: Monitor system security, managing user permissions, detecting abnormal behavior, and taking necessary security measures.

Risk management: Assess and respond to potential risks within the system, ensuring system stability and security.

Dashboard: Provide a real-time system monitoring interface, displaying system status, key indicators, and alert information to help administrators quickly understand the system's status.

Compared to traditional database architectures and network security frameworks, trusted accounts offer significant advantages by providing account-level data security. First, they address the risk in traditional architectures where database administrators have excessive privileges, granting them access to all database data. Trusted accounts introduce fine-grained access control, ensuring that even administrators can only access data within their authorized scope, thus reducing the risk of data breaches. Additionally, the trusted account system overcomes the limitations of traditional network security architectures, which often focus on external threats while neglecting internal vulnerabilities. This system effectively prevents unauthorized access by internal users or devices, thereby enhancing the overall security of the system.

Compared to zero-trust security architectures, traditional zero-trust models focus primarily on trusted identity authentication but fall short of implementing a comprehensive trusted account system. As a result, their data security continues to rely heavily on network-level protection. In contrast, a trusted account system strengthens overall data security by establishing security mechanisms directly at the account level, providing more granular control and protection over sensitive information[13].

2.3 Key advantages of blockchain-integrated intrinsic security architecture

Traditional security frameworks rely on centralized control, leading to issues such as single points of failure, lack of transparency, and susceptibility to internal attacks. The blockchain-integrated intrinsic security architecture eliminates single points of failure through decentralization, enhancing system resilience. Its encryption and distributed ledger ensure data immutability, effectively preventing data tampering and internal threats.

Zero trust architecture relies on strict identity verification but still depends on centralized authentication. The blockchain-integrated intrinsic security architecture uses public-private key pairs and trusted accounts to achieve decentralized identity verification, ensuring the transparency and traceability of identity information while mitigating the risks of relying on a single authentication authority.

SDN and VNF improve network resource management through virtualization but depend on centralized operations, which may lack transparency. The blockchain-integrated intrinsic security architecture ensures transparency and automates network management through distributed ledgers and smart contracts,

reducing the reliance on manual configurations.

The blockchain-integrated intrinsic security architecture provides significant advantages in decentralization, immutability, and transparency, though challenges persist regarding processing efficiency and resource consumption. Combining this architecture with other security frameworks, such as Zero Trust and SDN/VNF, can result in more comprehensive and efficient security solutions.

This architecture addresses traditional security challenges while offering improved protection and operational efficiency. By embedding security measures throughout every layer of the system and utilizing decentralized blockchain technology, it ensures end-to-end security, from data transmission to risk management. The key advantages outlined below highlight why this architecture is a robust solution for modern, complex environments:

(1) Decentralization and high availability

The architecture leverages the decentralized nature of blockchain technology, effectively eliminating single points of failure. By distributing data and control information across multiple nodes, the system maintains high availability, ensuring stable operation even if some nodes fail or are attacked.

(2) Account-level data security

The trusted account mechanism provides account-level data security, ensuring that only authorized users and devices can access sensitive data. Even if data are transmitted over an unencrypted channel, unauthorized users cannot interpret the information, thereby enhancing data security—particularly well-suited for bandwidth-constrained environments such as satellite communication.

(3) Fine-grained access control

By combining the permission model with trusted accounts, the system implements fine-grained access control, ensuring that each user or device can only access the resources for which they are authorized. This reduces the risk of unauthorized access from both internal and external sources, thereby improving overall security.

(4) Intrinsic risk assessment and dynamic defense

The inclusion of a risk model enables real-time risk assessment, allowing the system to detect and provide early warnings for potential threats. Coupled with smart contracts, the system can automatically execute predefined security responses, such as adjusting permissions or restricting access, ensuring dynamic defense capabilities.

(5) Operational transparency and traceability

Through the combination of log services and blockchain technology, the architecture ensures operational transparency and immutability. All operations are traceable, providing the system with comprehensive auditing capabilities, enhancing operational transparency and trustworthiness.

(6) Full lifecycle security coverage

Security mechanisms are embedded throughout the system's design, development, deployment, and operation phases, ensuring security coverage across the entire lifecycle. This full-lifecycle security approach increases system stability and resilience against potential threats.

(7) Efficient data circulation and privacy protection

Using multi-party secure computation and encryption technologies, the system enables secure cross-domain data circulation while protecting data privacy. Even during data transmission between different nodes or networks, the system ensures data integrity and security.

(8) Smart contract automation and security management

The use of smart contracts in this architecture allows many operations to be automated, particularly in security management and risk control. Smart contracts not only improve efficiency but also ensure timely responses and execution of security measures, reducing the risk of human error.

By integrating blockchain and intrinsic security mechanisms, this system architecture offers multiple advantages, including decentralized high availability, fine-grained access control, dynamic risk defense, and operational transparency. These features ensure the security, flexibility, and reliability of the system in complex environments.

3 A Case Study on the Intrinsic Security Mechanism of Satellite Internet

A satellite internet project is currently under implementation, aimed at delivering high-speed and reliable internet connectivity to remote and underserved areas. As the satellite network continues to expand, the project team has observed a significant escalation in security challenges, driven by the increasing number of users and the growing complexity of the system. Issues such as unauthorized access, data breaches, and malicious attacks present severe risks to the network's integrity. In response, the project team opted to implement an intrinsic security framework focused on trusted accounts, authorization mechanisms, and trusted data to ensure the secure and reliable operation of the system.

The implementation of the intrinsic security system, as reflected in the system architecture, involved a combination of key modules: trusted accounts, an authorization system, and trusted data mechanisms, which together provided a comprehensive and adaptive security solution for satellite internet.

Network layer: The network layer, incorporating satellite communication and blockchain infrastructure, ensured reliable and secure communication between satellite nodes and ground systems. The decentralized blockchain network eliminated single points of failure and enhanced data integrity during transmission.

Model layer: The model layer played a pivotal role in defining the system's security policies, data structures, and risk management strategies. Trusted accounts, categorized into individual, organizational, and device types, ensured the authenticity and security of all identities within the system. The permission model enforced strict access control measures, while the risk model provided continuous risk assessments, identifying potential threats before they could impact system operations.

Service layer: The service layer provided critical services such as identity authentication, authorization, data circulation, and log services. These services ensured that only authenticated and authorized users and devices could access network resources, significantly reducing the system's vulnerability to unauthorized access. The log service, integrated with blockchain technology, offered immutable and traceable records of all operations, providing robust auditability and operational transparency.

Application layer: At the user interaction level, the data management and risk management functions allowed for seamless handling of business operations, data processing, and risk monitoring. The dashboard provided real-time system status updates and visualized alerts, ensuring that administrators could react promptly to potential security threats. This ensured the continuous monitoring and timely response to any suspicious activities or system anomalies, thereby safeguarding the integrity and availability of the satellite network.

By leveraging the capabilities of each system layer, the project team successfully established a fine-grained authorization system,

combining the principle of least privilege with multi-party secure computation. This minimized the risk of privilege abuse and unauthorized access, ensuring that data sharing occurred under strictly controlled conditions. Smart contracts automated access control enforcement, providing dynamic responses to changing security conditions in real-time.

In the context of satellite internet, the system demonstrated exceptional resilience. Blockchain-based trusted data mechanisms ensured the immutability of transmitted and stored data, while continuous monitoring and real-time risk detection enhanced security for critical satellite operations, including control commands and confidential data exchanges. As a result, the satellite internet infrastructure remained secure and reliable, maintaining high levels of data protection even in bandwidth-limited and remote environments.

The deployment of the intrinsic security system, integrating trusted accounts, authorization systems, and trusted data mechanisms, effectively safeguarded the satellite internet network from a wide range of security threats. This architecture serves as a robust model for future satellite communication projects, emphasizing the importance of decentralized security frameworks and real-time risk management to ensure the integrity, availability, and confidentiality of satellite communications.

At the outset of the satellite internet project, users included government agencies, enterprises, individual users, and various terminal devices. The project team identified the need to guarantee the authenticity and security of every user and device, recognizing that traditional single-factor authentication methods were insufficient for a satellite internet environment characterized by extensive geographic distribution and diverse access methods.

To address these challenges, a trusted account system was implemented, categorizing accounts into individual, organizational, and device types. Each trusted account, authenticated by an authoritative institution, generated a unique digital identity using public-private key encryption. To strengthen security further, Multi-Factor Authentication (MFA) was introduced, requiring multiple verification methods such as passwords, biometrics, and physical tokens. Blockchain technology, with its immutable properties, was integrated into the authentication process, ensuring that user authentication data could be securely recorded and enabling cross-network and cross-platform identity verification. This significantly improved transparency and security in account management.

As the satellite internet system expanded, the need for complex access control mechanisms became apparent. For example, government entities required access to sensitive military communications, while enterprises needed access to commercial data. To prevent unauthorized access and privilege abuse, the project team designed a fine-grained authorization system based on trusted accounts. This system comprised:

(1) A trusted account circulation mechanism to ensure the reliability of identity authentication and secure data transmission.

(2) A data domain control-based circulation mechanism to manage permissions and rules for cross-domain data transfers, ensuring sensitive data was not misused across different domains.

(3) A secure multi-party computation-based data circulation mechanism, allowing data to be shared and processed confidentially.

Smart contracts were used to automatically enforce authorization rules, ensuring that only authorized users and devices could access specific satellite data or perform critical operations. This authorization system improved access control efficiency while minimizing the attack surface by adhering to the principle of least privilege.

In satellite internet, the security of data transmission and storage is paramount. Given the risks of data interception, tampering, or loss during satellite-to-ground communication, the project team implemented multi-layered data protection measures:

- Instruction data protection: System operation instructions, such as satellite control commands, were protected with encryption and digital signatures to prevent tampering or forgery, ensuring mission-critical operations remained secure from malicious attacks.

- Business data protection: Sensitive business data, such as user information and transaction records, was stored on the blockchain, ensuring immutability and auditability while enabling secure tracking of changes.

The system also deployed continuous monitoring and real-time analysis tools to monitor data flows across the satellite network and detect any anomalies. This allowed the system to promptly respond to security threats, maintaining data integrity and reliability throughout its operation.

By integrating trusted accounts, authorization systems, and trusted data mechanisms, the project team established a highly secure, reliable, and adaptive intrinsic security system for satellite internet. Trusted accounts ensured the authenticity of users and devices, the authorization system enabled fine-grained access control, and trusted data mechanisms guaranteed data integrity and security during transmission and storage.

During operational phases, the system consistently demonstrated exceptional security and stability, preventing unauthorized access and internal misuse. Blockchain-based trusted data management safeguarded critical data during satellite communications. Automated monitoring and real-time response mechanisms allowed the system to detect and mitigate security threats rapidly, ensuring the continuity of satellite internet services.

This successful implementation showcases the effectiveness of the intrinsic security architecture in satellite internet applications and provides a valuable reference for future satellite communication projects. It underscores the importance of trusted accounts, authorization systems, and trusted data in constructing robust and resilient security mechanisms for satellite internet networks on a global scale.

4 Conclusion and Future Work

Despite the critical role that intrinsic security mechanisms play in enhancing the security and reliability of satellite internet systems, several challenges remain in practical applications:

Addressing diverse threats: Satellite internet systems operate within a highly complex communication environment, encompassing multiple nodes such as ground stations, satellites, and user terminals. These systems are exposed to a wide array of threats originating from the physical, network, and application layers. Developing comprehensive defense strategies in such a multi-layered environment remains a formidable challenge. Current security mechanisms require further refinement to effectively counter sophisticated and evolving network attacks.

Balancing real-time response and system performance: In satellite internet systems, maintaining the ability to respond to security threats in real-time is essential. However, this must be achieved without compromising the system's data processing and transmission efficiency. Ensuring the real-time effectiveness of security mechanisms while upholding high system performance is

a significant challenge, particularly in the context of dynamically adjusting access controls and monitoring data in real-time. This underscores the need for continued technological advancements to meet these dual requirements.

Cross-domain collaboration and standardization: Satellite internet systems often involve cross-border and cross-platform collaboration, where security standards and protocols may vary significantly between countries and organizations. Achieving standardization and interoperability of security mechanisms across diverse regions and platforms presents a major obstacle. The development of unified security standards and protocols is therefore critical to facilitating seamless collaboration and ensuring global security interoperability.

Data privacy and compliance: The increased mobility of data within satellite internet systems has amplified concerns around data privacy and regulatory compliance. Ensuring data security while adhering to national regulations, particularly during cross-border data transmissions, remains a complex issue that requires urgent attention and resolution.

To address these challenges, future research efforts should focus on the following key areas:

Strengthening comprehensive defense systems: Research should continue to explore the development of multi-layered and comprehensive defense systems within the complex satellite internet environment. By integrating physical, network, and application-level security, more intelligent and automated defense technologies can be devised, thereby enhancing the system's capability to respond effectively to diverse threats.

Optimizing real-time response and system performance: Further optimization of both the real-time effectiveness of security mechanisms and overall system performance is essential. Future research could investigate more efficient encryption algorithms, flexible smart contract frameworks, and advanced threat detection technologies to strike an optimal balance between robust security and system efficiency.

Promoting the development of security standards and cross-domain collaboration: In the context of globalization, advancing the development and adoption of unified security standards for satellite internet is of paramount importance. Future work should prioritize the establishment of international cooperation frameworks, the formulation of standardized security protocols, and fostering collaboration among nations and organizations to ensure cross-domain security interoperability.

Enhancing data privacy protection and compliance: Further exploration is required to enhance data privacy protection in satellite internet systems while maintaining compliance with national laws and regulations. Special emphasis should be placed on safeguarding data during cross-border transmissions and ensuring adherence to the privacy requirements of different jurisdictions.

Exploring the application of emerging technologies: Future efforts should consider the integration of emerging technologies such as quantum encryption, distributed ledger technologies, and artificial intelligence into satellite internet security frameworks. These technologies hold the potential to significantly improve the system's security, efficiency, and flexibility, allowing for better responses to evolving security threats.

By focusing on these areas, the security and reliability of satellite internet systems can be significantly strengthened, providing a more secure, trustworthy, and stable communication environment. These advancements will not only safeguard critical infrastructure from potential attacks but also lay a solid foundation for the future development of satellite internet networks.

Dates

Received: 5 September 2024; Revised: 5 September 2024; Accepted: 13 September 2024

References

[1] C. Jiang, Q. Li, Y. Wang, D. Zhao, D. Zhao, Y. Jiang, and M. Xu, Survey on key technologies in space-ground integrated network, *J. Softw.*, vol. 35, no. 1, pp. 1–36, 2024.

[2] R. Zhu, Y. Zhang, Y. Wei, and C. Xi, Security management technology of multilayer satellite internet based on blockchain, *Space-Integr. -Ground Inf. Netw.*, vol. 3, no. 1, pp. 79–86, 2022.

[3] H. Guan, P. Yi, M. Yu, and J. Li, Overview of security technologies for satellite communication systems, *Telecommun. Sci.*, vol. 29, no. 7, pp. 96–102, 2013.

[4] A. Chen, Satellite communication system security protection, *Netw. Secur. Technol. Appl.*, no. 9, pp. 95–97, 2019.

[5] L. Chang, Security situation analysis of satellite internet under 'new infrastructure', *China Inf. Secur.*, no. 7, pp. 47–48, 2020.

[6] Z. Su, L. Liu, Z. Guo, J. Zhang, and T. Zhou, Research and simulation of satellite-ground channel characteristics for LEO satellites, *Radio Commun. Technol.*, vol. 49, no. 5, pp. 866–874, 2023.

[7] H. Chen, K. Qiao, and H. Yang, Research on security protection architecture of broadband satellite communication system, *Mod. Navig.*, no. 1, pp. 51–56, 2022.

[8] K. Christidis and M. Devetsikiotis, Blockchains and smart contracts for the Internet of Things, *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[9] X. Ji, K. Huang, J. Wu, Y. Chen, and W. You, Endogenous security technology of 6G space-ground integrated information network, *Space-Integr. -Ground Inf. Netw.*, vol. 4, no. 2, pp. 2–12, 2023.

[10] C. Li, B. Lei, C. Xie, and Y. Li, Trusted network based on blockchain technology, *Telecommun. Sci.*, vol. 35, no. 10, pp. 60–68, 2019.

[11] K. Nie, B. Cao, and M. Peng, 6G endogenous security: Blockchain technology, *Telecommun. Sci.*, vol. 36, no. 1, pp. 21–27, 2020.

[12] C. Shan, L. Lü, and S. Ye, Cross-domain data scheduling design of LEO satellite internet based on blockchain, *Cybersecur. Data Gov.*, vol. 43, no. 2, pp. 90–96, 2024.

[13] Y. Song, W. Zhou, J. Liu, and X. Li, Research on satellite internet security protection based on zero trust, *Space-Integr. -Ground Inf. Netw.*, vol. 2, no. 3, pp. 15–23, 2021.