International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

DATA SECURITY IN COMMUNICATION USING BLOCKCHAIN AND KEY BASED PROTOCOL

Mrs. B. DEEPIKA[1], M.E., PH.D.,

BOOMIKA M[2], DEVIKA P[2], JEEVA M[2], KAMESHWARI S[2]

[1]**Department of CSE, Assistant Professor, Dhanalakshmi Srinivasan Engineering college, Perambalur**

[2]**Department of CSE, UG Student, Dhanalakshmi Srinivasan Engineering college, Perambalur**

ABSTRACT: ***Satellite communications play an important role in the development of global communications networks. Recently, satellite networking has been receiving a lot of attention as a solution to alleviate the limitations of terrestrial networks due to low stability and coverage. It has many disadvantages, including low processing power, storage space, and limited data security. Illegal access has become a problem. Data processing power is minimal, storage space and data security are limited due to regional power availability and physical satellite limitations, and data can be modified or accessed by malicious users. As the importance of satellite communication increases in the development of global communication networks, concerns about the security of satellite communication are also growing. This project proposes a satellite communication network using blockchain technology and QKD protocol based on authentication and personal information protection. To achieve this goal, an architecture was built consisting of traditional and constrained devices connected to the blockchain over a wireless heterogeneous network. Communication uses registration, authentication, and cancellation. The satellite transmits the received data to a base station on the ground, which stores all key parameters in the decentralized blockchain and removes all invalid node certificates from the blockchain. The proposed blockchain and QKD satellite system provides a high level of security for future 6Gandbeyond networks, Internet of Things, autonomous vehicles and other rapidly developing applications.***

1. INTRODUCTION

This presentation covers the basic principles and applications of satellite communications. , historical developments, major components, and important roles in communications, broadcasting, meteorological observation, and remote sensing are discussed. Advances in satellite technology have spawned an entire satellite services industry that provides a variety of services to broadcasters, Internet Service Providers (ISPs), governments, the military, and other sectors. Satellite communications technology is often used during natural disasters or emergency situations when terrestrial communications services are disrupted. Emergency communication services can be provided in disaster areas using mobile satellite equipment.

Blockchain technology is at the forefront of the digital revolution, transforming trust, security, and transparency in information sharing. Blockchain is essentially a distributed ledger that records transactions on a computer network and provides immutability and consensus without the need for a central authority.

Quantum Key Distribution (QKD) is at the forefront of quantum cryptography, providing innovative solutions. We talk about the eternal problem of securing communication channels in the quantum computer era. When traditional encryption methods face the looming threat of quantum algorithms that can break traditional encryption, QKD becomes a beacon of quantum-resistant information security. The introduction reviews the innovative aspects of the QKD protocol and explores the quantum mechanical principles underlying its functionality. QKD leverages the unique properties of quantum particles, such as superposition and entanglement, to create an inherently secure method for exchanging cryptographic keys between parties.

2. LITERATURESURVEY

Cloud security that combines dynamic AES encryption and blockchain-based key management. As businesses increasingly rely on cloud services to store

and manage sensitive data, ensuring confidentiality and integrity has become paramount. This project provides dynamic AES encryption, where encryption keys are dynamically generated and updated based on various parameters such as time, user access, or data sensitivity. PUF is a hardware security primitive that uses internal changes in the physical properties of an electronic component to uniquely identify it.

This project aims to provide the ability to recover information using multidimensional CRPS protection (cryptographically secure PUF-based protection). CRPS adds an additional layer of security by using encryption technology to protect data exchanged between authenticated parties. Although sharing information between multiple users or organizations is common, ensuring the confidentiality and integrity of shared information remains difficult. This is a proxy public monitoring and reverse encryption system to solve these problems. Proxy re-encryption allows a trusted third party, called a proxy, to convert ciphertext encrypted with one user's public key into ciphertext that can be decrypted with another user's private key.

3. EXISTING SYSTEM

Satellite communications have many benefits and risks. Security solutions that minimize security risks and protect satellite networks must be developed using cryptographic algorithms. Since security is a key consideration for all communications, existing security methods include DES and Advanced Encryption Standard (AES). Elliptic Curve Cryptography (ECC), Triple-DES, Blowfish, hashing algorithms and (data encryption standards), etc. Encryption keys are dynamically generated and updated based on various parameters such as time, user access, or data sensitivity.

PUF is a hardware security primitive that leverages intrinsic differences in the physical properties of electronic components for unique identification. This project aims to share recoverable data using multidimensional CRPS (cryptographically strong PUF-based protection). CRPS adds an additional layer of security by using encryption technology to protect data transmitted between authorized parties.

4. DRAWBACKS

- As the computer power of attackers and eavesdroppers increases, the security of encryption methods is weakening.
- Many of these systems use static authentication, which authenticates the user or device only once, at the beginning of each session. It does not prevent man-in-the-middle attacks, nor does it prevent collision attacks.
- It does not provide reverse or forward secrecy, as an attacker can obtain the device ID and then intercept other values from the current session to find previous and future secret keys.
- Initialization and computation costs are high.

5. PROPOSED SYSTEM

Data hackers can remotely disrupt, intercept, or modify wireless network systems, target flight crew equipment, and manipulate the direction and transmission of satellite communications antennas in satellite communications.

Space utilization in satellite communication can be developed separately to improve communication security according to satellite communication standards. The security requirements of satellite communications services cannot be met by a single security system. In this study, we assume that blockchain is used to evaluate the security of satellite communication networks in terms of personal information protection, access control, and security authentication.

Consortium blockchain was introduced to allow joint satellite constellations to exchange information. In this section, we propose a new idea called Sat Chain. Sat Chains are a way to tokenize spatial transactions in the form of digital tokens that can be authenticated using a blockchain system. SDT can be transmitted via a constellation of satellites, which is a collection of satellite networks. As a result, in this case blockchain can be used as an authenticator for all communication patterns that may occur within a single satellite constellation. Sat Chain is used to process sensing data between satellites and data centers. As a result, in these situations, blockchain can be used as a tracking system to identify expected spatial collisions between satellites and data centers.

Quantum encryption, also known as quantum cryptography, uses the principles of quantum mechanics to encrypt messages in a way that makes them unreadable to anyone but the intended recipient. This ensures that it cannot be damaged unintentionally. Quantum Key Distribution: The process of using quantum communication to establish a shared key between two trusted parties, so that an untrusted eavesdropper will know nothing about the key. Quantum key distribution uses special technologies to produce and distribute cryptographic key material based on the unique capabilities of quantum mechanical systems. Internet Key Exchange Version 2: Quantum

Key Generation (IKEv2) Internet Key Exchange Version 2 (IKEv2) is a protocol that generates keys and secure associations (SAs) to establish secure satellite network (SN) connections that prevent data transmission. Prevents packets from being read or intercepted over public Internet connections (see Figure 3.1). This allows remote computers on a public network to access resources while maintaining the security of a closed, private network.

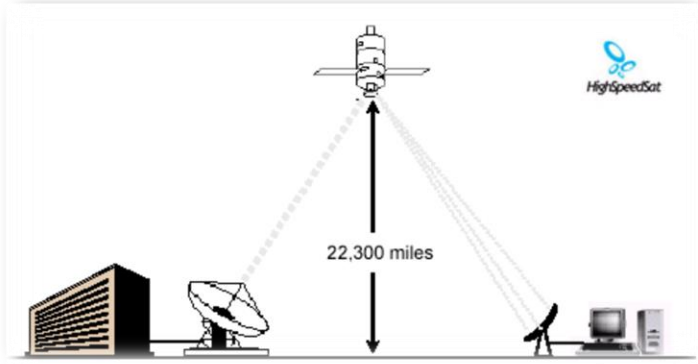
Data Processing Centre

The satellite network system architecture model described in this project is a complex framework designed to optimize the efficiency and reliability of satellite communications. This model consists of key components such as satellite, ground station, data center, and satellite controller.

Easy wireless network connection to facilitate data sharing and communication. One of the key steps in this model is the registration and initialization phase. This plays an important role in establishing a secure and reliable communication channel between the user terminal and the satellite network.

The Data Processing Centre has four sub modules,

- Registration And Initialization Steps
- Certification And Approval
- Composition Negotiation
- Secure Key Exchange

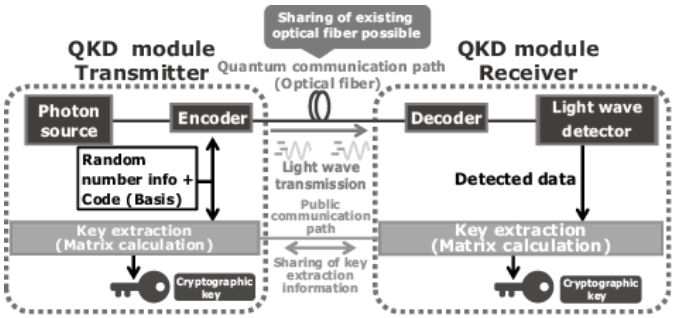


Data Processing Centre

Quantum Key Generation and Distribution

Quantum Key Distribution (QKD) is at the forefront of modern cryptography and uses the principles of quantum mechanics to provide unprecedented security. The essence of QKD is to use quantum communication to establish a shared encryption key between two trusted parties, while providing immunity to eavesdropping attempts by untrusted attackers. QKD uses its expertise to change the paradigm of cryptographic protocols, providing reliable protection against increasingly sophisticated cyber threats.

Through the process of quantum entanglement, particles can be correlated in such a way that a modification or measurement of one particle immediately affects the entangled counterpart, detecting eavesdropping attempts. This phenomenon is at the core of the QKD protocol.



Quantum Key Generation and Distribution

Successful implementation of QKD relies on special techniques suited to exploit the unique properties of quantum systems. Quantum key distribution systems typically involve the use of quantum cryptography devices, quantum key generators, and quantum relays, each designed to manipulate and transmit quantum states accurately and reliably.

Sat Chain

The consortium's blockchain represents a significant advance in information sharing and collaboration between joint satellite constellations. The introduction of this innovative approach opens a new era in space technology, enabling seamless communication and data exchange within satellite networks. At the heart of this initiative is an innovative concept known as Sat Chain. Sat Chains provides a new framework for tokenizing spatial transactions, turning them into digital tokens that can be processed securely using blockchain protocols. Using blockchain technology, Sat Chains provides a reliable authentication and verification mechanism for space transactions, ensuring transparency, immutability, and integrity throughout the entire process.

Sat Chains transforms the way space transactions are conducted and recorded by enabling the creation and distribution of space-based digital tokens (SDTs) within satellite constellations. These digital tokens serve as cryptographic representations of space

assets, resources, or services, facilitating the seamless exchange of value within satellite networks. The decentralized nature of blockchain technology allows SDT to be securely broadcast and verified across the many satellites that make up the satellite constellation. This decentralized approach eliminates the need for centralized intermediaries or institutions and creates a peer-to-peer network where space transactions can be completed autonomously and in trust. The introduction of satellite networks and SDT represents a paradigm shift in the space industry, opening up new opportunities for cooperation, trade and exploration in outer space. Sat Chains tokenize space transactions and leverage blockchain protocols to provide a distributed and immutable ledger for recording and verifying space activities.

End User and Device Registration

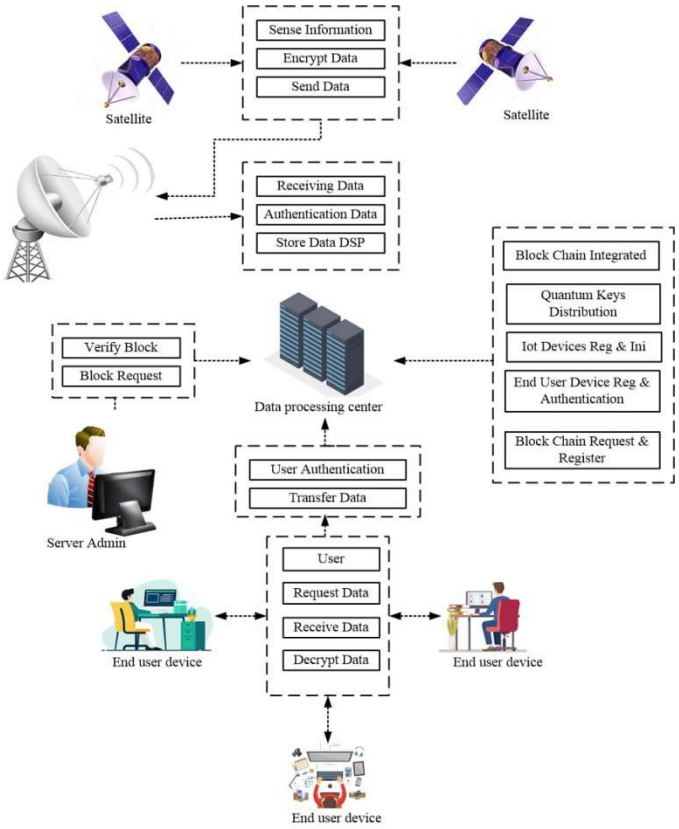
End user registration serves as the foundational step in granting individuals access to a network while upholding security and authentication standards. This process entails the collection of pertinent information from users, including personal details such as their name, address, contact information, and credentials. The primary objective of gathering this data is twofold: first, to verify the user's identity and second, to ascertain them authorization status for accessing the network.

By obtaining comprehensive information, network administrators can establish reliable systems for identifying and authenticating users, reducing the risks associated with unauthorized access or fraudulent activity. When you submit your registration information, the information you provide goes through a rigorous verification process to ensure its accuracy and reliability. This verification process involves cross-referencing the data you provide with existing records or databases to verify your identity and verify your authorization status. You can also implement additional measures such as email verification, phone verification, or multi-factor authentication to increase security and prevent unauthorized access.

ADVANTAGES

- Provides improved stability
- Integration of blockchain and quantum key distribution (QKD)
- Reliable security.
- Vulnerability to unauthorized access in terrestrial networks. QKD provides an additional layer of security through authentication and privacy.
- Registration, authentication, and revocation mechanisms enhance the overall security of the network.

6. SYSTEM ARCHITECTURE



7. CONCLUSION

A privacy-preserving authentication method based on data storage in blockchain can effectively provide a security protection mechanism for satellite communications. Initially, the registration and authentication process of all satellite sensor nodes is performed at the base station to ensure the reliability of sensor nodes. Once the authentication process is complete, all key parameter information is stored in the Universal Key Mechanism (UKM) in the data center.

GBS transmits key boundary data to satellite sensor centers, which use inter-satellite blockchain technology to record key parameters at the point, improving the immutability and transparency of the received data. The simulation results show that the proposed method significantly improves the safety and security of satellite communication.

8. FUTURE ENHANCEMENT

The concept of a satellite blockchain system involves using satellites in orbit to support blockchain technology to ensure secure transmission and storage of data in space. The system is expected to develop further by relying on cloud constellations, networks of interconnected satellites that act as data centers in orbit. These cloud constellations allow companies to upload and manage data directly from space, bypassing terrestrial networks.

Governments and businesses can use cloud constellations to access vast amounts of data from a variety of sources and from space orbit. This approach offers a variety of advantages over traditional terrestrial networks, including increased data security, reduced latency, and improved reliability. Additionally, satellite blockchain systems can provide greater resilience to ground-based disruptions and cyber threats by decentralizing data storage and processing capabilities in space.

REFERENCES

[1] S. Liu, Z. Gao, Y. Wu, D. W. K. Ng, X. Gao, K.-K. Wong, et al., "LEO satellite constellations for 5G and beyond: How will they reshape vertical domains?", IEEE Commun. Mag., vol. 59, no. 7, pp. 30-36, Jul. 2021.

[2] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6G era: Challenges and opportunities", IEEE Netw., vol. 35, no. 2, pp. 244-251, Mar. 2021.

[3] B. Al Homssi, A. Al-Hourani, K. Wang, P. Conder, S. Kandeepan, J. Choi, et al., "Next generation mega satellite networks for access equality: Opportunities challenges and performance", IEEE Commun. Mag., vol. 60, no. 4, pp. 18-24, Apr. 2022.

[4] X. Lin, S. Cioni, G. Charbit, N. Chuberre, S. Hellsten and J. Boutillon, "On the path to 6G: Embracing the next wave of low Earth orbit satellite access", IEEE Commun. Mag., vol. 59, no. 12, pp. 36-42, Dec. 2021.

[5] X. Zhu and C. Jiang, "Integrated satellite-terrestrial networks toward 6G: Architectures applications and challenges", IEEE Internet Things J., vol. 9, no. 1, pp. 437-461, Jan. 2022.

[6] M. M. Azari, S. Solanki, S. Chatzinotas, O. Kodheli, H. Sallouha, A. Colpaert, et al., "Evolution of non-terrestrial networks from 5G to 6G: A survey", IEEE Commun. Surveys Tuts., vol. 24, no. 4, pp. 2633-2672, 4th Quart. 2022.

[7] X. Hou, J. Wang, Z. Fang, Y. Ren, K.-C. Chen and L. Hanzo, "Edge intelligence for mission-critical 6G services in space-air-ground integrated networks", IEEE Netw., vol. 36, no. 2, pp. 181-189, Mar. 2022.

[8] Y. Zhang, C. Chen, L. Liu, D. Lan, H. Jiang and S. Wan, "Aerial edge computing on orbit: A task offloading and allocation scheme", IEEE Trans. Netw. Sci. Eng., vol. 10, no. 1, pp. 275-285, Jan. 2023.

[9] F. Feng and M. Kowalski, ‘‘Underdetermined reverberant blind source separation: Sparse approaches for multiplicative and convolutive narrowband approximation,’’ IEEE/ACM Trans. Audio, Speech, Lang. Process., vol. 27, no. 2, pp. 442–456, Feb. 2019.

[10] S. Rathore, Y. Pan, and J. H. Park, ‘‘BlockDeepNet: A blockchain-based secure deep learning for IoT network,’’ Sustainability, vol. 11, no. 14, p. 3974, Jul. 2019.

[11] C. Li, L. Zhu, Z. Luo, and Z. Zhang, ‘‘Solutions to data reception with improve blind source separation in satellite communications,’’ in Proc. IEEE Int. Symp. Netw., Comput. Commun. (ISNCC), Montreal, QC, Canada, Oct. 2020, pp. 1–5

[12] Y. Chen, W. Wang, Z. Wang, and B. Xia, ‘‘A source counting method using acoustic vector sensor based on sparse modeling of DOA histogram,’’ IEEE Signal Process. Lett., vol. 26, no. 1, pp. 69–73, Jan. 2019

[13] M. E. Sudip, A. Mukherjee, A. Roy, N. Saurabh, Y. Rahulamathavan, and M. Rajarajan, ‘‘Blockchain at the edge: Performance of resourceconstrained IoT networks,’’ IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 1, pp. 174–183, Jan. 2021.

[14] S. Fu, J. Gao, and L. Zhao, ‘‘Integrated resource management for terrestrial-satellite systems,’’ IEEE Trans. Veh. Technol., vol. 69, no. 3, pp. 3256–3266, Mar. 2020

[15] R. Goyat, G. Kumar, R. Saha, M. Conti, M. K. Rai, R. Thomas, M. Alazab, and T. Hoon-Kim, ‘‘‘Blockchain-based data storage with privacy and authentication in Internet-of-Things,’’ IEEE Internet Things J., early access, Aug. 24, 2020, doi:

10.1109/JIOT.2020.3019074

[16] J. Yang, S. He, Y. Xu, L. Chen, and J. Ren, ‘‘A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks,’’ Sensors, vol. 19, no. 4, pp. 1–19, 2019

[17] L. Xu and F. Wu, ‘‘A lightweight authentication scheme for multi-gateway wireless sensor networks under IoT conception,’’ Arabian J. Sci. Eng., vol. 44, no. 4, pp. 3977–3993, Apr. 2019.

[18] H. Yang, Y. Liang, Q. Yao, S. Guo, A. Yu, and J. Zhang, ‘‘Blockchainbased secure distributed control for software defined optical networking,’’ China Commun., vol. 16, no. 6, pp. 42–54, Jun. 2019.