SatChain: GEO Network Security Mechanism based on Blockchain and QKD Protocol

R.Bharathi[1],M.S.Maharahjan[2], K.Monika[3],M.Pavithra[4],C.Sivaraj[5],S.Thilipkumar[6]

[1]*Assistant Professor,Department of Computer Science and Engineering, Cheran College Of Engineering, Karur,Tamilnadu,India.*

[2]*Assistant Professor,Department of Computer Science And Engineering, GRT Institute of Engineering and Technology ,Tiruttani , ThriuvallurDist , Tamilnadu,India*

[3,4,5,6] *U.G.Student,Department of Computer Science And Engineering,Cheran College Of Engineering,Karur,Tamilnadu,India.*

[1]*bharathimkce@gmail.com*,[2]*maha84rajan@gmail.com*,[3]*kmonika2210@gmail.com*,[4]*pavithramaniraj001@gmail.com*,[5]*Sivakc63@gmail.com*,[6]*thilipkumarsaravanan14022001@gmail.com*

Abstract

With the convergence of terrestrial wireless and satellite communications, the sixth generation (6G) networks are projected to create a completely linked world. Data processing capacity is minimal, storage and security are constrained due to satellite physical limits in terms of available power and area, and the data may be exposed to alteration or contamination by intruders. Since satellite communication has become more crucial in the development of global communication networks, there have been worries regarding its security. It's difficult to keep a satellite network safe from unauthorised data access while still making efficient use of storage capacity. In this project, a satellite communication network is suggested using blockchain technology and the QKD protocol, which is based on authentication and privacy protection. An architecture comprising of both traditional and limited devices linked to the blockchain through a wireless heterogeneous network has been built to achieve this goal. Registration, authentication, and revocation are used to carry out the communication. The satellite will send the acquired data to the terrestrial base station, which will record all key parameters on the distributed blockchain and delete any rogue node certificates from the blockchain. The proposed satellite-based Blockchain and QKD system offers a high degree of security for future 6G and beyond networks, the Internet of Things, self-driving vehicles, and other rapidly evolving applications.

Keywords:6G Networks,QKD,Blockchain,Satellitecommunication,Wireless network

1. INTRODUCTION

A satellite is a spacecraft that circles another object. Natural and man-made satellites are the two sorts of satellites. The Earth and the Moon are examples of natural satellites [1]-[5]. The Earth revolves around the Sun, whereas the Moon revolves around it. A man-made satellite is a device that is sent into space and revolves around the body shown in Figure 1.1.

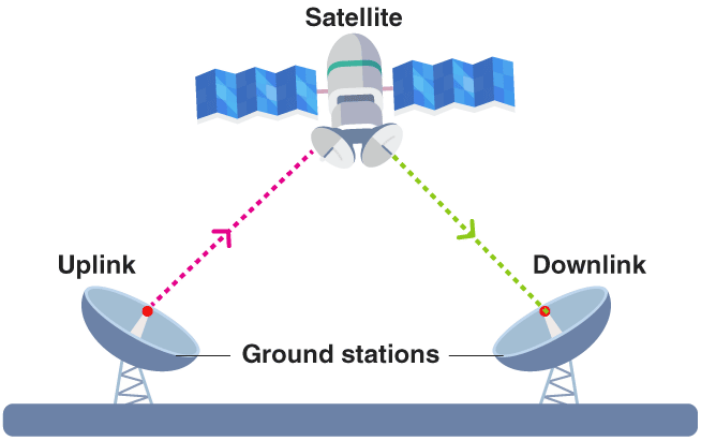

Figure 1.1.Satellite Communication

Low Earth Orbit (LEO)

LEO is located between 200 and 1200 kilometres above the earth's surface. This orbit has the benefit of a shorter signal travel time and a smaller chance of losing its course. On the other hand, since the satellite travels faster as the earth rotates, the coverage zone is fairly limited (in contrast to GEO) and the connection time from ground station to satellite is shorter. The growing interest in mobile communications through satellites in recent years has prompted a rise in LEO utilisation and research.

Medium Earth Orbit (MEO)

MEO is between 1200 and 35286 kilometres above the earth's surface. According to some sources, the Medium Earth Orbit is between 5000 and 13000 kilometres in height, or between two Van Allen belts [Walke00]. The Van Allen belts are two high-intensity radiation zones on Earth that are home to highly charged particles and high-energy neutrons. As a

result, the two belts are harmful to communication satellites. As a result, the satellite is not placed in the Van Allen belts zones.

Highly Elliptical Orbit (HEO)

The HEO's name comes from its elliptical shape, which allows for greater coverage of highly populated zones or otherwise inaccessible regions of the globe (such as the poles) without disrupting lower orbits.

Geostationary Orbit (GEO)

GEO is 35786 kilometres above the Earth's surface. The orbit is known as a geostationary orbit because the speed of satellites in this orbit is matched to the speed of the planet's rotation, ensuring that the satellite travels in lockstep with the earth. To put it another way, if one could view the satellite from the ground, the satellite would constantly remain at the same location in space from the perspective of the planet. The majority of communication satellites are stationed in GEO.[6]-[10]

2. RELATED WORK

The applications of satellite communication systems include the following.

- TV
- Telephone
- Monitoring of Weather Condition and Forecasting
- Military
- Navigations
- Amateur Radio
- TV broadcasting like DTH (Direct to Home)
- Radio Broadcasting
- Remote sensing applications
- Disaster Management
- Voice communications & Radio Broadcasting
- Internet Access
- Digital cinema
- Internet applications to provide the application of internet connection for GPS applications, data transfer, Internet surfing, and many more.

3. PROPOSED WORK

Geostationary earth orbit (GEO), medium earth orbit (MEO), and low earth orbit (LEO) are the three kinds of orbits characterised by satellite height (LEO). GEO satellites, for example, remain stationary in relation to the earth's surface, resulting in less doppler shift and a reduced likelihood of transmission outages than non-GEO satellites. GEO satellites operate at very high altitudes (35,786 km) and provide the most comprehensive coverage. GEO satellites are selected in our suggested protocol because to their low outage probability and vast coverage.

3.1.Quantum Cryptography

Quantum cryptography, also known as quantum encryption, uses quantum mechanics principles to encrypt communications such that they can never be read by anybody other than the intended receiver. It takes use of quantum's numerous states, as well as its "no change theory," which ensures that it cannot be disrupted unintentionally.

3.2Quantum key distribution:

The process of establishing a shared key between two trusted parties utilising quantum communication such that an untrusted eavesdropper cannot learn anything about the key. Quantum key distribution uses special purpose technology to produce and distribute cryptographic keying material based on the unique features of quantum mechanical systems.

Version 2 of the Internet Key Exchange: Quantum Key Generation (IKEv2) IKEv2 (Internet Key Exchange Version 2) is a protocol for establishing keys and security associations (SAs) for the purpose of establishing a secure Satellite Network (SN) connection that prevents data packets from being read or intercepted over a public Internet connection (see fig 3.1). This lets a distant computer on a public network to access resources while yet benefiting from the security of a private closed network.

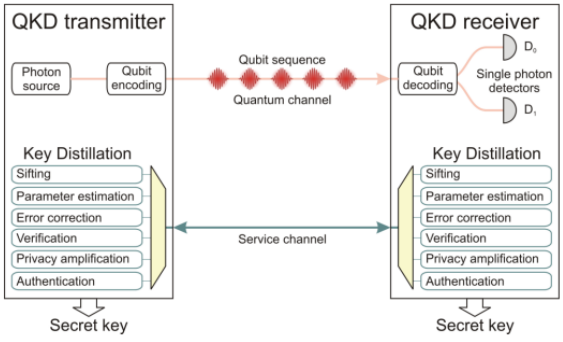

Figure 3.1. Quantum Key Distribution

3.3. SatChain

A consortium blockchain is presented to allow cooperative satellite constellations to share information. A novel idea called SatChain is suggested in this section. SatChains are a technique to tokenize space transactions as digital tokens that can be authenticated using a blockchain system. SDTs may be transmitted via a satellite constellation, which is a collection of satellite networks. As a result, blockchain may be used as an authenticator in this case for any communication patterns that may occur inside a single satellite constellation. As illustrated in fig. 3.2, SatChain is utilised to handle sensing data between satellites and DPC; as a result, blockchain may be used as a tracking system in this situation to identify predicted spacecollisions between satellites and DPC.

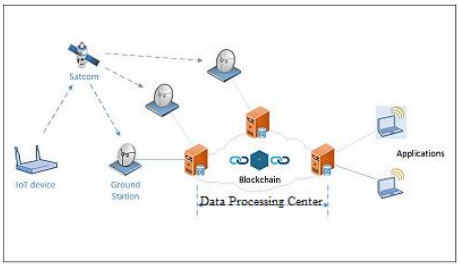

Figure 3.2.SatChain

3.4.Proof of Space Transactions (PoST)

Proof of Space Transactions (PoST) is a new blockchain protocol for verifying SEDs inside a satellite constellation and adding new blocks to the blockchain. Each satellite in a constellation is represented by a private key and a piece of cryptographic evidence for a satellite's private key that is cryptographically tied to a particular SED in the PoST approach. When a new SED is triggered between two satellites, the satellite that initiated the transaction communicates the transaction's cryptographic proof with the rest of the satellite constellation to certify the triggered SED's legitimacy. The receiving satellite also asks for the nonce code of the blockchain's latest block. A new block is added to the blockchain whenever the nonce code is validated by the receiving satellite.

4. RESULTS AND DISCUSSION

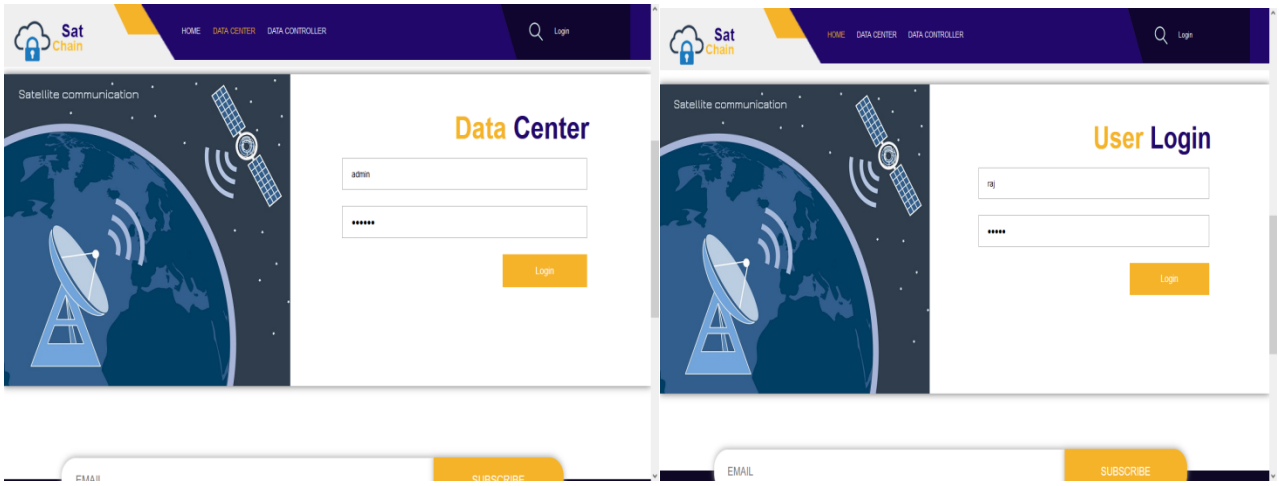

FIG NO.4.1 DATA CENTER AND USER LOGIN

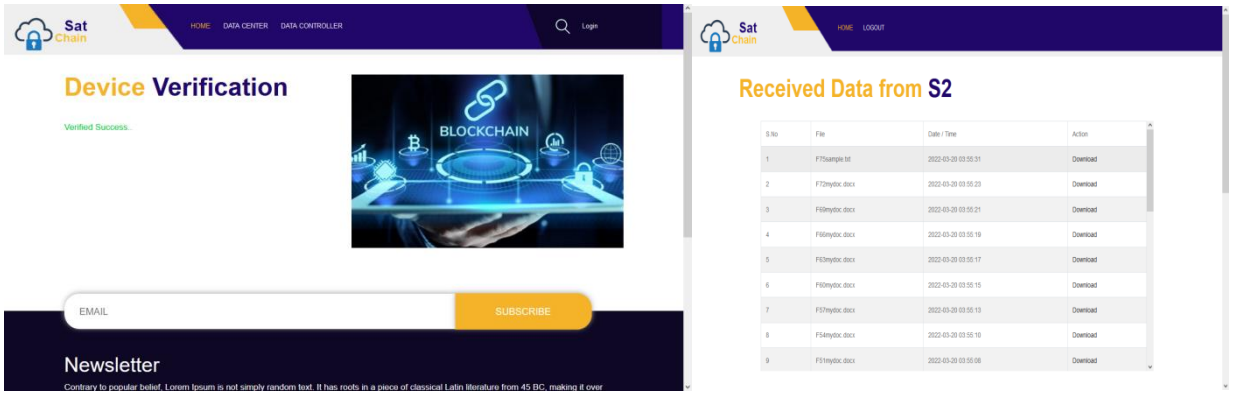

FIG NO 4.2 DEVICE VERIFICATION AND RECEIVED DATA

5. CONCLUSION

Not only is the satellite communication channel distinct from the common mobile channel, but it is also distinct from the ground station channel. The satellite communication channel combines the satellite and mobile communication channels into one. Hackers and external interference signals make satellite communication lines very susceptible. It may be difficult to keep satellite networks safe from unauthorised access and usage of data. Quantum Key Cryptography and block chain technology are used to investigate the security of satellite communication networks in terms of access control, secrecy, and security authentication in this research. The suggested approach is designed to address the security issue that arises when a centralised database is used in satellite communication. The simulation results suggest that the proposed strategy may greatly enhance satellite communications security and protection.

6. FUTURE WORK

The blockchain-satellite system will rely on cloud constellations in the future to manage data centres in orbit, where corporations may upload data and circumvent terrestrial networks; this strategy will aid governments and companies in obtaining information from many sources and orbits in space.

7. REFERENCES

[1]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.

[2]H. Yang, Y. Liang, Q. Yao, S. Guo, A. Yu, and J. Zhang, ``Blockchain- based secure distributed control for software defined optical networking,'' China Commun., vol. 16, no. 6, pp. 42- 54, Jun. 2019.

[3]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.

[4] J. D Parsons. The Mobile Radio Propagation Channel, second edition. John Wiley and Sons Ltd., © 2000. Online ISBN 0-470-84152-4.

[5] Ray E. Sherriff and Y. Fun Hu. Mobile Satellite Communication Networks. John Wiley and Sons Ltd., © 2000. Online ISBN 0-470-84555-2.

[6] A. Mehrnia and H. Hashemi. Mobile Satellite Propagation Channel, Part I – A comparative evaluation of current models. Proceedings of VTC'1999-Fall Conference, Amsterdam, September 19-22, 1999.

[7] E. Lutz. Land Mobile Satellite Channel – recording and modeling. Proceedings of the 4th International Conference on Satellite Systems for Mobile Communications and Navigation, London, October 1988, pp. 15 – 19.

[8] C. Loo. A statistical model for land mobile satellite link. IEEE Transactions on Vehicular Technology, vol. 34. no. 3, pp. 122-127, August 1985.

[9] H. Suzuki. A Statistical Model for Urban Radio Propagation. IEEE Transactions on Vehicular Technology, Vol. Com-25. No. 7, pp. 673-680, July 1977.

[10] E. Lutz, D. Cygan, M. Dippold, F. Dolainsky and W. Papke. The Land Mobile Satellite Communication Channel – Recording, Statistics and Channel Model. IEEE Transactions on Vehicular Technology, vol. 40. no. 2, pp. 375-386, May 1991

[11] R.Bharathi, T.Abirami," Energy efficient compressive sensing with predictive model for IoT based medical data transmission", Journal of Ambient Intelligence and Humanized Computing, November 2020, https://doi.org/10.1007/s12652-020-02670-z

[12] R.Bharathi, T.Abirami," Energy Efficient Clustering with Disease Diagnosis Model for IoT based Sustainable Healthcare Systems", Sustainable Computing: Informatics and Systems, 23 September 2020, https://doi.org/10.1016/j.suscom.2020.100453