WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# SatChain: GEO Network Security Mechanism based on Block chain and QKD Protocol

***Chitra .S[1], Gayathri .K[2], Nithiya .V[3], Prof Ambika .S[4]***

*[1]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
*E-Mail: subashkavi64@gmail.com*
*[2]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
*E-Mail: gayathrikaliyaperumal07@gmail.com*
*[3]EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
*E-Mail: nithyarajan071@gmail.com*
*[4]Assistant professor, EGS Pillay Engineering College (Autonomous), Nagapattinam, Tamilnadu, India*
*E-Mail: ranjani@egs.org*

A B S T R A C T

In satellite correspondence frameworks, satellite power and handling limits are restricted, and that implies that capacity and security are likewise compelled. Satellite correspondence station very defenseless against programmer sand outside impedance signals. Shielding satellite organizations from unlawful in line access and utilize can very challenge. In this paper, architecture composed of satellite and ground equipment is developed that integrates communication network authentication an privacy protection structures. In the proposed plot, the correspondence, enrollment, confirmation, and disavowal of data are accomplished through stages to further develop correspondence security. The satellite advances the gathered data to a ground base station, which has serious areas of strength for a handling limit. The ground base station records all the key parameters in the distributed block chain, and all malicious node certificates are removed from the system. To additional improve information transmission security, the key is moved utilizing an awry encryption calculation. To gauge the vigor of utilizing the proposed network design, under a similar assault condition, an immunity investigation is performed. In the wake of leading reproduction explores, the outcomes show that the proposed plot enormously further develops correspondence security and assurance.

Keywords: Satellite communication system, communication network authentication, privacy protection scheme, ground base station.

## 1. INTRODUCTION

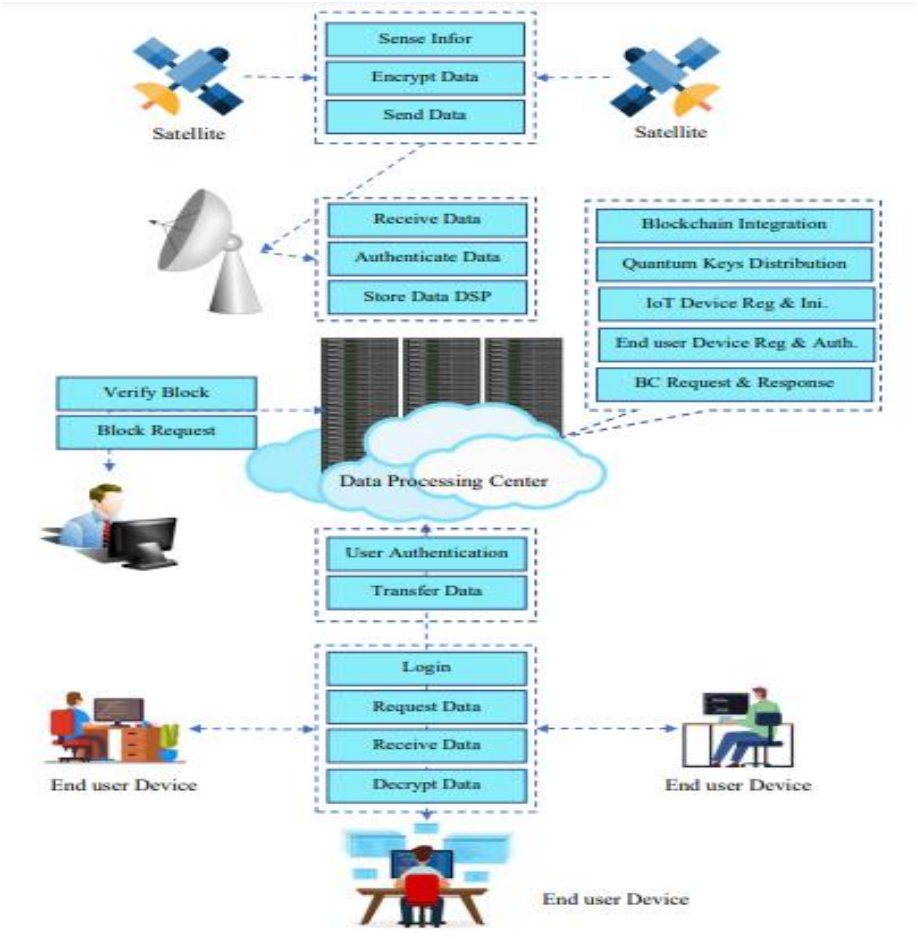
With the fast improvement of PC organisations and correspondence innovation, satellite correspondence has become one of the most significant and promising exchange information technologies, given its intrinsic advantages of long-range mobile communication, the cost-effectiveness of multicast and broadcast systems, wide coverage area, and high flexibility. Satellite correspondence frameworks empower the sending and getting of data around the world, offering web access, TV, phone, radio, and other regular citizen and military tasks, through the satellite organisation correspondence system. The advent of HTS (high-throughput satellite) systems has greatly enhanced technical capabilities and offered wideband services at lower costs. Significant upgrades are normal on the impending super groups of stars in low Earth circles that will convey an enormous number of satellites, giving full earth incorporation to restricted deferments despite wide information move limit. The use of satellites, given these characteristics, can increase efficiency in providing large sets of services and applications that are security-sensitive, for example, telemedicine, banking, search and salvage, sensor organizations, and content conveyance network feeds, which create around 90% of the total traffic. Nonetheless, much of the time, the security of satellite correspondence has been truly compromised, bringing about secretive risks. In satellite correspondences (and, surprisingly, in earthbound frameworks), programmers can meddle, capture, or modify wireless network frameworks from a distance, assault the hardware of flight teams, and control the situating and transmission of satellite correspondence radio wires. As per satellite correspondence conventions, the utilisation of room in satellite correspondence

can be increased autonomously to improve correspondence security. Proposals have been made to increase the solidarity and similarity of correspondence conventions for space. A solitary security instrument is deficient to meet the security necessities for satellite correspondence administrations. In this paper, block tie advancement is familiar with analysing the security of satellite correspondence networks to the extent of entrance control, confidentiality, and security affirmation.

## METHODOLOGY

Assuming organization security frameworks are planned utilizing ad hoc and capricious techniques, their trustworthiness will be in uncertainty and the change to the data age will be risked. Subsequently, a reliable and clear arrangement procedure for network security is seriously required. The issue has gotten little consideration. This can perhaps be explained by the relative immaturity of the underlying technology. Ward and Mellor see that many designing disciplines advance through unsurprising stages. In the primary stage, advances for taking care of issues start to arise. Engineering is dominated by attempts to fit the problems to the few available solutions. In the subsequent stage, power-52 November 1990-IEEE Communications Magazine As full elective advances become accessible, there is less need to compel fit issues into arrangements. Subsequently, a reliable and clear arrangement procedure for network security is seriously required focused, with a focus on characteristics such as cost and flexibility rather than the solubility of problems.It is our perspective that the discipline of affiliation security is in the last 50% of stage two. The progress to the third stage should be joined by an experienced philosophy that demands an issue focused approach. Current programming rehearses give a valuable similarity. The practically widespread acknowledgment of a proper necessities examination stage is an encapsulation of the issue focused approach. Software has benefited from gains in quality, development time, and maintainability. There is not a great explanation to accept that such gains couldn't be accomplished in that frame of mind of organization security. We have had the option to find just a single paper tending to, in a critical way, the issue of organization security strategy. These authors mention but do not develop a treatment of design, instead concentrating on the surrounding issues: threat analyses, operational system assessment, review, and certification.

## MODELING AND ANALYSIS

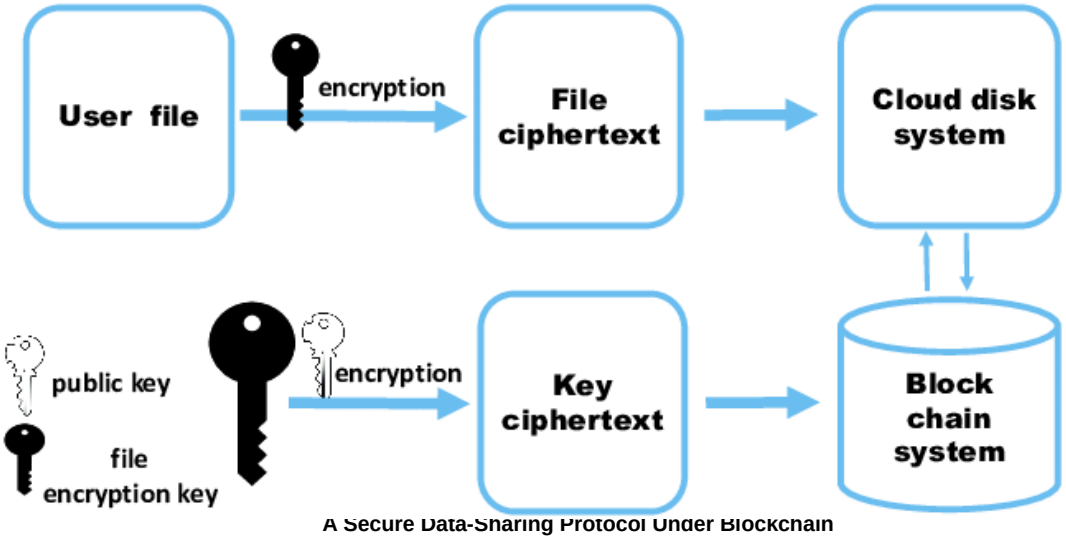


***Objective***

1. Design an algorithm for performing the security-related transformation.
2. Produce the restricted intel to be utilized with the calculation.
3. Develop methods for the distribution and sharing of secret information.
4. Determine a convention to be utilized by the two directors that utilize the security calculation and the privileged data to accomplish a specific security administration.

## RESULTS AND DISCUSSION

Developing new quantum-secured consensus protocols to enhance the blockchain security in optical networks is a challenging problem for future research. In addition to this, different quantum-secured signature schemes have to be designed for the signing phase in quantum secured blockchain for authentication. Moreover, to check validity of the transaction, participants in quantum-secured blockchain have to performed a verification test. Hence, various verification schemes are needed to be proposed, which make quantum blockchain more secure and reliable for quantum-secured blockchain participants. Furthermore, one of the most critical challenges in the quantum secured blockchain optical networks is resilience against node/link failure. Therefore, survivability needs to be addressed in such optical communication networks. Since blockchain technology is used in variety of applications such as but not limited to Internet of Things (IoT), wireless communication networks, healthcare networks, financial systems, supply chain, and voting systems. Hence, for security improvement, the quantum-secured blockchain can be deployed for such applications in the future.




A Secure Data-Sharing Protocol Under Blockchain

## CONCLUSION

The privacy protection authentication scheme based on blockchain data storage can effectively provide a security protection mechanism for satellite communications. Initially, the registration and certification processes for all satellite sensor nodes are carried out by the base station, ensuring the authenticity of the sensor nodes. After completing the authentication process, all key parameter information is stored in the DPC's immutable key mechanism (UKM). The GBS sends key boundary data to the satellite sensor hubs, which then, at that point, record the key parameters on inter-satellite blockchain technology to improve the invariance and transparency of the acquired data. The simulation results show that the proposed method was able to significantly improve security and protection for satellite communications.

REFERENCES

[1] 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.
[2] 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.
[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] 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.
[5] 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.
[6] 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.
[7] 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.
[8] Y.-H. Zhao, Z.-L. Wang, J.-Z. Xu, and X.-J. Guo, ''Realization algorithm of satellite network attack graph based on performance state space,'' J. Shenyang Univ. Technol., vol. 33, no. 2, pp. 202–207, Apr. 2011.
[9] Y. Wu, W.-C. Jiao, Y.-H. Pan, and H. Li, ''Analysis of cipher security and cipher attack modeling in satellite network,'' Comput. Technol. Develop., vol. 21, no. 6, pp. 140–144, Jun. 2011.
[10] 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.
[11] 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.
[12] 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.