AN INTEGRATED ARCHITECTURE FOR SECURITY AND KEY MANAGEMENT BASED ON BLOCKCHAIN

Mr.C.Jeevanantham M.E[1], Maria A Rexana B.Tech[2], G.Saravana Theepiga B.Tech[3], T.Nandhini B.Tech[4]

[1]Assistant Professor in Information Technology, Dr.Mahalingam College of Engineering And Technology, Pollachi-642003, Coimbatore, Tamil Nadu, India

[2,3,4]Student, Dr.Mahalingam College of Engineering and Technology, Pollachi-642003,Coimbatore, TamilNadu, India

ABSTRACT

One of the key wireless technologies now on the market to support LPWAN settings is Low-Power Wide-Area Network (LoRaWAN). This makes it possible for Internet of Things devices to communicate over great distances (IoT). The Join Server, a crucial part of the LoRaWAN architecture, is in charge of security operations including key management and authentication. Nevertheless, because all encryption keys are kept in one location, specifically one point of failure is the Join Server (SPOF). In order to improve LoRaWAN's security criteria, the research then offers a reliable and secure design. The Join Server has been changed and the smart contracts and a permissioned blockchain are used to overcome the SPOF problem. Open-source technologies were used to build a functioning prototype in order to assess the viability of the suggested architecture. It was also looked at how well a blockchain network performed on a cloud system with various workloads. The results show that performance and availability are compromised when figuring out the amount of blockchain peers in small settings. In huge instances when performance is strong, this pattern is inverted.

1. INTRODUCTION

1.1 THE BLOCKCHAIN

Blockchain is a networked, immutable record that simplifies tracking transactions and keeping track of assets inside a company network. An asset may be tangible (such a house, a vehicle, cash, or a piece of land) or amorphous (intellectual property, patents, copyrights, branding). A block chain technology allows for the tracking and sale of almost any item of interest, lowering risk and costs for all parties. The lifeblood of company is information. The faster and more accurate the response, the better. Since it provides real-time, transferable, and completely transparent data stored on a public blockchain that only authorised network users can access, blockchain is a fantastic technique for disseminating this kind of data. A blockchain technology can monitor transactions, finances, and production, among other things. Members have a shared concept of the truth, allowing you to see every aspect of transactions from start to finish. This boosts your confidence and creates new chances. A public blockchain, such as Bit coin, is one that everyone may join and participate in. It's possible that a lot of computational power, weak confidentiality, and little to no transactions privacy will all be needed. These issues are crucial for blockchain business use cases. Like a public blockchain, a private blockchain network is a global peer-to-peer network. One person or organisation controls the network, which also selects participants, manages the consensus process, and updates the shared ledger. Depending on the application, this may significantly boost participant confidence and trust. A private blockchain can even be housed on a company's property and managed behind a firewall.

1.2 INFORMATION INTEGRITY

Data integrity is the term for the consistency, completeness, and correctness of data. When addressing regulatory compliance, especially GDPR compliance, the term "data integrity" also implies the safety and security of data. It is kept current by a set of processes, standards, and specifications established during the design phase. Because there is so much talk about data integrity, it's easy to get the genuine picture jumbled. Data integrity and data protection are sometimes conflated, however the two concepts have different meanings. Data integrity also guarantees that data is safe from outside influences. The two types of data integrity are physical and logical data integrity. Both are a group of steps and methods for ensuring the reliability of the information in relational and hierarchical data. The protection of data completeness and precision during storage and retrieval is referred to as physical integrity. Physical integrity is at risk when power outages, natural disasters, or hacking attacks impair database operations. Data processing managers, device programmers, applications programmers, and internal auditors might not be able to collect accurate data because of human error, storage degradation, and several other issues.

1.3 HOMOMORPHIC ENCRYPTION

A kind of encryption known as homomorphic encryption enables users to compute on encrypted data without first having to decode it. These computations' results are then stored in encrypted form, which, when decoded, yields the identical results as if the operations had been carried out on plain data. This encryption can be used to ensure the privacy of hired storage and computing. This makes it possible to encrypt data before sending it to processing environments in business cloud services. Homomorphic encryption can be used for personal information, such as medical records, to allow for additional services by lowering privacy obstacles preventing data interchange or by enhancing the security of existing services. Healthcare predictive analytics, for example, due to privacy concerns with medical data, could be challenging to deploy through a third-party service provider; but, if the vendor of predictive analytics services can work with encrypted data, these privacy concerns can be addressed. Moreover, the data is secure even if the service lender's system is hacked. The capacity to compute over encrypted data without having access to the secret key is a feature of homomorphic encryption. The outcome of such a calculation is encrypted.

2. RELATED WORKS

The literature is replete with publications that advocate LPWAN and blockchain integration. According to the authors of [4], a blockchain network's architecture would use LoRa gateways as its clients. The Ethereumblockchain and actual LoRa devices are used to achieve the suggested solution. The security characteristics of the suggested design are not, however, described by the authors. Additionally, There are no specifics regarding how the Application Server and blockchain nodes are integrated. [5] has a suggestion that is comparable but created for a pollution monitoring application. In the suggested infrastructure, several Servers establish a decentralised network and perform blockchain functions like hashing, transactional confirmation, and block chaining. The proposed approach can validate the legitimacy of network transactions. Nevertheless, the authors don't go into detail about the architecture's security features, and the suggested remedy wasn't put into practise.

It is advised to adopt a blockchain-based two-factor authentication method. The Ethereum blockchain was used by the authors to implement their suggested strategy. In order to assess the suggested solution in terms of latency and throughput a performance study was conducted.

Findings reveal that the Ethereum blockchain's frequent mining operations cause a significant amount of latency to be introduced during the initial Join step. Yet for the proposed approach to function, end-device firmware changes are necessary because the Join Server remains active in the LoRaWAN network.

For the LoRaWAN join process to increase availability and confidentiality, the authors of [10] propose a blockchain-based solution. They both function as endpoints of a permissioned blockchain, Join Server and Network Server share key exchange protocol. The authors of [11] also suggest a blockchain-based LoRaWANarchitecture to defend the joint operation from jamming and replay assaults. Blockchain nodes act as LoRAWAN Networks in the proposed structure. The Join Server manages join requests by reading/writing authentication data on the blockchain network using smart contracts. With this strategy, a secure access control system for LoRAWAN may be created. The authors use the Ethereum blockchain to develop their method and do simulations to verify it. The acquired results show that the suggested solution is efficient when a demand of 30 join sessions produced by 1000 endpoints simultaneously.

The Join Server was joined to a blockchain network in the earlier work [12] to provide high dependability and safe storage of information. In opposition to our prior study, the Join Server has been completely replaced in the current work with a contract that is performed by a variety of peers dispersed around the blockchain system. Additionally, by doing both security and performance testing in a cloud environment, this study enhances the analysis of the suggested architecture. The prototype's implementation also complies with the most recent LoRaWAN standard.

The technology's numerous configurations and versions provide a significant hurdle for architects creating blockchain-based applications. Because blockchain are still in their infancy, there is limited product data or credible technological evaluation to compare different blockchain. In order to aid in the design and evaluation of blockchain and block chain technology systems' effects on software architectures, we present a methodology for categorising and contrasting them in this paper. [2]

3. PROPOSED ARCHITECTURE

We describe the recommended LoRaWAN architecture in this section. The chaincode functionality and network topology are discussed first. The suggested architecture's message process is then described in detail. The parts that went into building a functioning prototype are then mentioned.

3.1 NETWORK TOPOLOGY

The suggested network design is shown here. Only two of the security and access control responsibilities that a chaincode currently performs in place of JS are handling the main encryption keys and the OTAA process. Private blockchain and NS are divided into GRP1 and GRP2, two separate groupings. To assure availability, the private blockchain is implemented in many GRP1 peers. As a client machine from GRP2, NS may interface with the chaincode. The chaincode must be started by the GRP1 administrator, who must also register any additional devices' encryption keys. The root credentials are always given in the transaction's temporary fields and kept in the PDC of GRP1 whenever registration or update activities are performed (As a result, NS cannot access the cryptographic keys directly). The Hyperledger Fabric generates digital certificates and verifies each node's identification using a Public Key Infrastructure (PKI). Using Transport Layer Security ensures the privacy of communications between trustworthy peers (TLS).

3.2 CHAINCODE DESCRIPTION

A user's authorization to utilise a particular function is determined by a set of rules for network access that are defined by the chaincode. This shows how the chaincode managed and kept track of the root data encryption using the DeviceKeys struct.

This paper also presents an improved method sha 256 block chain, which combines the basic scheme with a data filtering technique to reduce DoS effect while maintaining perfect data security resilience. A group of suggested work on Multi cloud storage Key Generation centers can produce the keys utilized in each subgroup in concurrently. Although the keys for the members of the same subgroup are created by various KGCs, they can all calculate the same subgroup key. This is a desirable characteristic, particularly for large-scale network systems, because it reduces the problem of concentrating effort on a single entity.

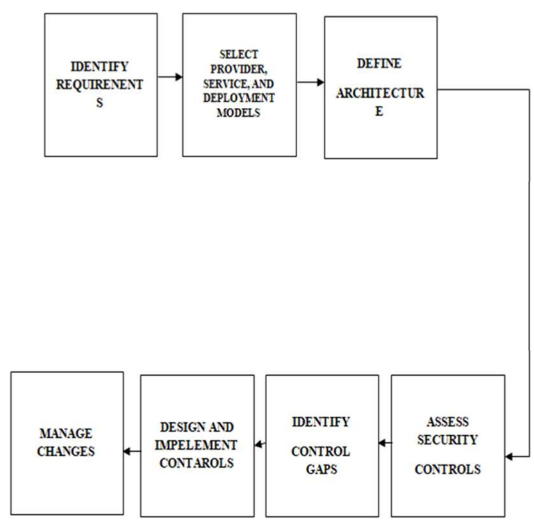


Figure 1: Flow diagram

4. BLOCKCHAIN KEY MANAGEMENT PHASE

For any cryptographic system, efficient and safe key management is a difficulty. If the hacker is successful in locating the keys by any means—such as brute force, side channel attack, physical system access, poor encryption, replay attack, etc.—he or she will be able to access the system. So, one of the most important aspects of the cryptographic system is key managementIf the keys are not maintained safe, no architecture is secure. The IoT devices are authenticated by PKI on the blockchain infrastructure, and the integrity of the infrastructure depends on the reliability of the third party. This section covers PKI for blockchains and access control for Bitcoin wallets.

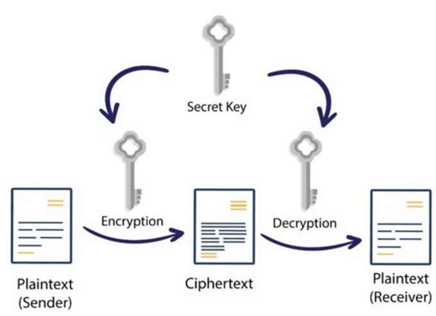


Figure 2: key encryption

5. RESULT ANALYSIS

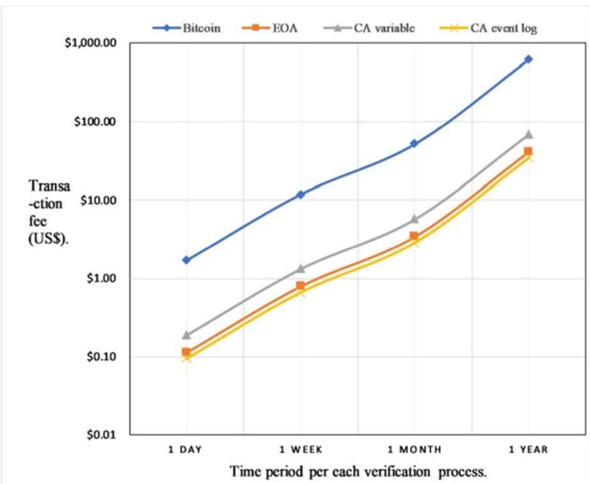
In a cloud environment, the functioning prototype's performance was assessed. The findings from efficiency and safety trials conducted in various settings are presented in this section. The preliminary security analysis of the suggested architecture completes this section.

5.1 SECURITY ANALYSIS

A secure and stable architecture exhibits a number of key characteristics, such as secrecy, integrity, and availability. One goal of the suggested design is to offer a safe, permissioned blockchain environment where a smart contract may be executed. The key management and OTAA method carried out by a regular JS are implemented by this smart contract. Although [33] offers a formal security analysis, this research does not address the integrity of the other LoRaWAN systems (such as gateways and AS). The following points outline how the suggested approach satisfies security requirements.

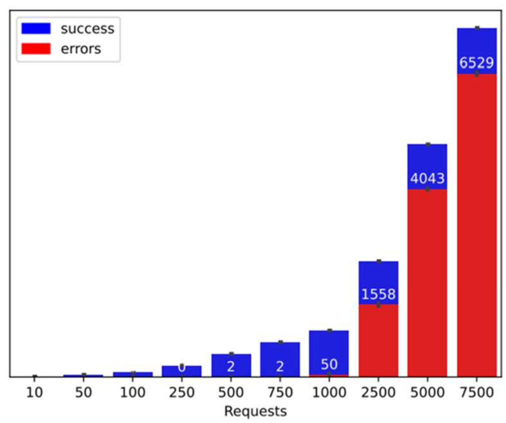
• **Availability:** Clients need access to services and data at all timesIn blockchain systems, availability is ensured by keeping copies of the record across many peers. Several endorsing peers can deploy chaincodes using Hyperledger Fabric [34]. As a result, the recommended design guarantees high availability for consumers and is resistant to DoS attacks.

Transaction fee Total cost in	Master hash every			
	30 Min	One hour	Half day	One day
One day	$4.32	$2.16	$0.18	$0.09
One week	$30.24	$15.12	$1.26	$0.63
One month	$131.4	$65.7	$5.475	$2.738
One year	$1576.8	$788.4	$65.7	$32.85



develop a permissioned blockchain network. Several tests were conducted to assess the suggested design. Second, a cloud environment efficiency analysis was carried out using a variety of authorised peers and tasks. The findings demonstrate that, in modest settings, while deciding on the number of approving peers, efficiency and accessibility are trade-offs.

Error message analysis during OTAA process



6. CONCLUSION

In order to enhance access control in LoRaWAN networks, this study provides a safe and fault-tolerant design. The suggested approach uses a permissioned blockchain and smart contract in place of JavaScript to eliminate the possibility of a single source of failure. To verify the suggested architecture, a functional prototype was created with accessible software. Hyperledger Fabric was used to

The performance of bigger sets of approving peers, however, shines out under situations with a high volume of transactions, reversing this tendency. Hence, we draw the conclusion that many endorsing peers work best in real-world LPWAN contexts. The effectiveness of the Hyperledger environment may be tested further in the future with different ordering service implementations and different ordering node counts. Further testing of the Hyperledger environment's performance with various ordering service implementations and ordering node counts is possible.

REFERENCES

[1] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, ‘‘Blockchain’s adoption in IoT: The challenges, and a way forward,’’ J. Netw. Comput. Appl., vol. 125, pp. 251–279, Jan. 2019.

[2] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, ‘‘Blockchain technology: A survey on applications and security privacy challenges,’’ Internet Things, vol. 8, Dec. 2019, Art. no. 100107.

[3] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, ‘‘Securing IoTs in distributed blockchain: Analysis, requirements and open issues,’’ Future Gener. Comput. Syst., vol. 100, pp. 325–343, Nov. 2019.

[4] K. R. Özyílmaz and A. Yurdakul, ‘‘Work-in-progress: Integrating lowpowerIoT devices to a blockchain-based infrastructure,’’ in Proc. Int. Conf. Embedded Softw. (EMSOFT), Oct. 2017, pp. 1–2.

[5] S. R. Niya, S. S. Jha, T. Bocek, and B. Stiller, ‘‘Design and implementation of an automated and decentralized pollution monitoring system with blockchains, smart contracts, and LoRaWAN,’’ in Proc. IEEE/IFIP Netw. Oper. Manage. Symp. (NOMS), Apr. 2018, pp. 1–4. [6] J. Lin, Z. Shen, C. Miao, and S. Liu, ‘‘Using blockchain to build trusted LoRaWANsharing server,’’ Int. J. Crowd Sci., vol. 1, no. 3, pp. 270–280, 2017.

[7] J. Lin, Z. Shen, and C. Miao, ‘‘Usingblockchain technology to build trust in sharing

LoRaWANIoT,’’ in Proc. 2nd Int. Conf. Crowd Sci. Eng. (ICCSE), New York, NY, USA, 2017, pp. 38–43.

[8] H. Liu, D. Han, and D. Li, ‘‘Fabric-IoT: A blockchain-based access control system in IoT,’’ IEEE Access, vol. 8, pp. 18207–18218, 2020.

[9] S. M. Danish, M. Lestas, W. Asif, H. K. Qureshi, and M. Rajarajan, ‘‘A lightweight blockchain based two factor authentication mechanism for LoRaWAN join procedure,’’ in Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), May 2019, pp. 1–6.

[10] M. Tan, D. Sun, and X. Li, ‘‘A secure and efficient blockchain-based key management scheme for LoRaWAN,’’ in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Mar. 2021, pp. 1–7.

[11] S. M. Danish, M. Lestas, H. K. Qureshi, K. Zhang, W. Asif, and M. Rajarajan, ‘‘Securing the LoRaWAN join procedure using blockchains,’’ Cluster Comput., vol. 23, no. 3, pp. 2123–2138, Sep. 2020.

[12] V. Ribeiro, R. Holanda, A. Ramos, and J. J. P. C. Rodrigues, ‘‘Enhancing key management in LoRaWAN with permissioned blockchain,’’ Sensors, vol. 20, no. 11, p. 3068, May 2020. [13] B. Buurman, J. Kamruzzaman, G. Karmakar, and S. Islam, ‘‘Low-power wide-area networks: Design goals, architecture, suitability to use cases and research challenges,’’ IEEE Access, vol. 8, pp. 17179–17220, 2020.

[14] U. Raza, P. Kulkarni, and M. Sooriyabandara, ‘‘Low power wide area networks: An overview,’’ IEEE Commun. Surveys Tuts., vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.

[15] C. Goursaud and J. M. Gorce, ‘‘Dedicated networks for IoT: PHY/MAC state of the art and challenges,’’ EAI Endorsed Trans. Internet Things, vol. 1, no. 1, Oct. 2015, Art. no. 150597.

[16] J. D. C. Silva, J. J. Rodrigues, A. M. Alberti, P. Solic, and A. A. L. Aquino, ‘‘LoRaWAN—A low power WAN protocol for Internet of Things: A review and opportunities,’’ in Proc. 2nd Int. Multidisciplinary Conf. Comput. Energy Sci. (SpliTech), 2017, pp. 1–6.

[17] L. Oliveira, ‘‘Performance assessment of LoRa and Sigfox protocols in mobility scenarios,’’ Nat. Inst. Telecommun., Minas Gerais, Brazil, Tech. Rep., 2018.

[18] LoRa Alliance. (2018). LoRaWAN Specification V1.1 | LoRa Alliance. Accessed: Jun. 14, 2021. [Online]. Available: https://loraalliance.org/resource-hub/lorawanr-specification-v11

[19] LoRa Alliance. LoRaWAN Back-End Interfaces V1.0 | LoRa Alliance. Accessed: Jun. 14, 2021. [Online]. Available: https://loraalliance.org/resource-hub/lorawan-back-end-interfaces-v1-0/

[20] R. Miller, ‘‘LoRa security: Building a secure LoRa solution,’’ MWR Labs, Basingstoke, U.K., White Paper 1, 2016.

[21] K. A. Nuaimi, N. Mohamed, M. A. Nuaimi, and J. Al-Jaroodi, ‘‘A survey of load balancing in cloud computing: Challenges and algorithms,’’ in Proc. 2nd Symp. Netw. Cloud Comput. Appl., Dec. 2012, pp. 137–142.

[22] E. J. Ghomi, A. M. Rahmani, and N. N. Qader, ‘‘Load-balancing algorithms in cloud computing: A survey,’’ J. Netw. Comput. Appl., vol. 88, pp. 50–71, Jun. 2017.

[23] E. Vargas and S. BluePrints, ‘‘High availability fundamentals,’’ Sun Blueprints Ser., pp. 1–7, Nov. 2000.

[24] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, ‘‘Blockchain challenges and opportunities: A survey,’’ Int. J. Web Grid Services, vol. 14, no. 4, pp. 352–375, 2018 network,’’ Sci. Technol. Libraries, vol. 37, no. 3, pp. 235–245, Jul. 2018

[25] M. Kuzlu, M. Pipattanasomporn, L. Gurses, and S. Rahman, ‘‘Performance analysis of a hyperledger fabric blockchain framework: Throughput, latency and scalability,’’ in Proc. IEEE Int. Conf.

Blockchain (Blockchain), Jul. 2019, pp. 536–540.

[26] C. Melo, F. Oliveira, J. Dantas, J. Araujo, P. Pereira, R. Maciel, and P. Maciel, ‘‘Performance and availability evaluation of the blockchain platform hyperledger fabric,’’ J. Supercomput., vol. 78, pp. 1–23, Mar. 2022.

[27] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, ‘‘Performance analysis of private blockchain platforms in varying workloads,’’ in Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN), Jul. 2017, pp. 1–6.