Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 5): pp. 8422-8428
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.05.937

Secure Heterogeneous Communication Environment Using Blockchain

[1] Gajanan P. Arsalwad , [2]Dr. Sohel A. Bhura , [3]Dr. Suresh S. Asole

[1,2,3]Babasaheb Naik College of Engineering, Pusad, Maharashtra, India.

Abstract. The globalisation that has occurred in the contemporary world has had a significant impact on the communication networks. When it comes to communication, most of the time closed and centralised methods are used, which might sometimes lead to privacy issues. The related systems are not capable of meeting the requirements for the information security components of integrity and openness. "Community research applications" is one example of this kind of framework. Existing communication frameworks for community interactions rely on the credibility of intermediate organisations, such as a central authority server, in order to function well. It is thought to be vulnerable to an assault that targets a single point of failure. It is possible that things may become much worse, since the relevant authorities may not be aware of any internal unrest that may be occurring. As a result of this, it is strongly advised that a framework for community engagement that is based on blockchain technology be designed. In this study, we present a secure communication architecture for community interactions that is built on blockchain technology. The technique of blockchain was included into the framework that was suggested, and it was realised using a distributed ledger that was tamper-proof.

Keywords: Communication, Blockchain, Heterogenious, Application.

I. Introduction

The development of information and communications technology (ICT) has led to a rise in the need for participation in community activities. In addition to this, there cannot be a single authority in control, which necessitates privacy and security measures[1-5]. One of these communities is the research community, which requires high levels of integrity and privacy but should not be dependent on a centralised system with limited access to its software. These systems each contain a single weak spot, which is a sign of their overall inadequacy. Developing systems that are not just decentralised and transparent but also have an adequate level of security is necessary in order to overcome this problem. One example of such a decentralised method is the blockchain technology, which enables people to freely connect with one another and share their knowledge without having to place their faith in any one particular authority. Applications that are built on top of blockchain technology run on a peer-to-peer (P2P) network structure via the use of algorithms that are based on consensus [1–9]. We pre6ented a blockchain-based secure communication framework for community involvement in this piece of research. This framework made use of helpful cryptographic mechanisms including encryption/decryption and key management. The proposed framework may be used by researchers working in fields such as engineering sciences and medical sciences in order to facilitate safe community engagement within such fields. The proposed framework offers these researchers a secure and confidential environment in which to discuss the findings of their research, to pose questions, to receive responses, and to explore a variety of opportunities without the need to worry that their findings will be altered or disclosed to unauthorised parties[10-13]. An Android application has been constructed on the basis of the framework that has been presented. The audience may use this application to exchange articles about their existing study and to participate on the development of new research projects. For the purpose of ensuring that the suggested framework is functional, we make use of the flutter developer kit. This allows for a smooth user experience. For the purpose of ensuring security, we make use of the blockchain method.

II. Literature Survey:

In recent years, a large number of authentication and key management protocol methods have been devised for use in a variety of industries, including networks, healthcare, and other applications[14]. These mechanisms have been used in a variety of settings. The following paragraphs provide a summary of several pertinent schemes.

The use of blockchain technology to smart communities was analysed[15]. There are several different blockchain procedures that are used, such as the generation, verification, and consensus algorithmic processes. In addition to this, a comprehensive explanation is done using a variety of system models. They have built clusters to ensure data security with the assistance of blockchain technology by combining a variety of activities that are comparable to one another. In [16] developed a key management method for the smart grid environment that would ensure the safe communication of smart metres. Several issues with the structure of the smart grid, including key management and trustworthy mutual authentication, were the focus of attention. A keyless signature technique that was scalable, quick, and had a minimal computational cost was also offered, and it was built on the consortium blockchain. In [17] took into consideration the situation of IoMT and proposed a technique for authenticating different smart healthcare devices as well as key agreement. The suggested mechanism made available to a variety of organisations a simple communication system that was built on blockchain technology. A comparison with other other systems that are quite comparable was also carried out.

The open-access blockchain platform [18] created and offered as an enterprise solution was based on the blockchain technology. The peer-to-peer file-sharing technology known as the Inter Planetary File System (IPFS) served as the foundation for this system. The purpose of the proposed platform was to provide a service that would promote the widespread sharing of knowledge, provide access to publications on the platform that were not owned by a third party, and further promote the credit system that was earned by engaging in interactions that were self-motivated. In [19] provided a comprehensive analysis of the blockchain technology, focusing on the ways in which it may actively contribute to the promotion of open research (unrestrained science).

They found the trustworthiness, cooperation, organisation, identity, credibility, and transparency offered by the blockchain to be very appealing, and it was for these reasons that they decided to use it. They have provided an insight into the themes of open-science, including the obstacles and research opportunities related with it, in their review. In [20] demonstrated the 'Dust app,' which was a messaging service that was powered by blockchain technology. It was built on Ethereum and used a technology that was known as "Mercury." This talking application was able to attain a level of efficiency and speed that was suitable for a messaging application by making use of Ethereum's messaging token. Because Dust saves all communications in memory (RAM), it is far more difficult for a hostile actor to obtain access to the messages. The difficulty increases by many orders of magnitude.

In [21] examined the XRP ledger algorithm to determine how to reach consensus without requiring the agreement of every single node in the network. In addition to this, the validation of the ledger over the current state of the network was carried out. In addition, [26] suggested a payment mechanism that uses blockchain technology to keep users' anonymity intact inside the payment system. In [23] carried out an in-depth investigation on the development of blockchain and the algorithm that governs its consensus. They analysed the blockchain technology over multiple layers, including the application layer, the platform layer, and the distributed computing layers, along with additional analysis and comparison of consensus algorithms, so that they could meet the demand for cost-efficient blockchain frameworks for ecosystems like smart cities.

III. Security Layers

The architecture of the system that has been presented is layered, and it is composed of three layers: the device layer, the controller layer, and the storage layer. In the Internet of Things applications, the physical devices that detect data and exchange it with other IoT devices made up what was known as the device layer. The controller layer comes next, and it's the one that the cluster head is in charge of managing. The controller layer is in charge of the development of secret keys, as well as the authentication of devices, the construction of blocks, and the formation of clusters.

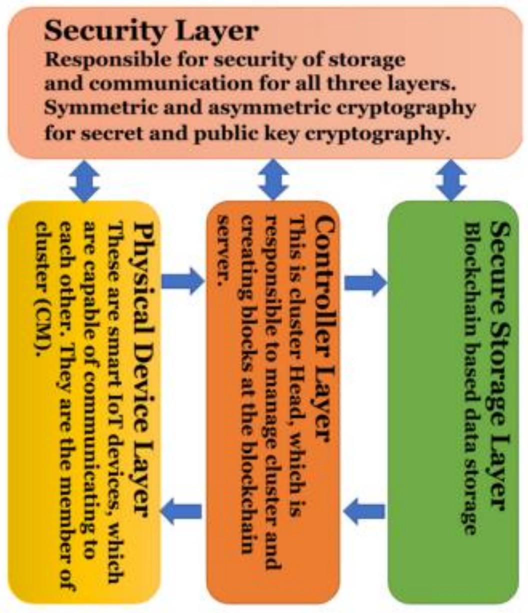
Security Layer
Responsible for security of storage and communication for all three layers. Symmetric and asymmetric cryptography for secret and public key cryptography.
Physical Device Layer
These are smart IoT devices, which are capable of communicating to each other. They are the member of cluster (CM).
Controller Layer
This is cluster Head, which is responsible to manage cluster and creating blocks at the blockchain server.
Secure Storage Layer
Blockchain based data storage

Figure1. Security Layers

IV. Secure Communication Model Using Blockchain

Figure 2 illustrates the network architecture that will be used by the proposed framework. It includes a variety of various sorts of entities, such as users (researchers), who, with the assistance of the suggested framework, are able to communicate with one another.

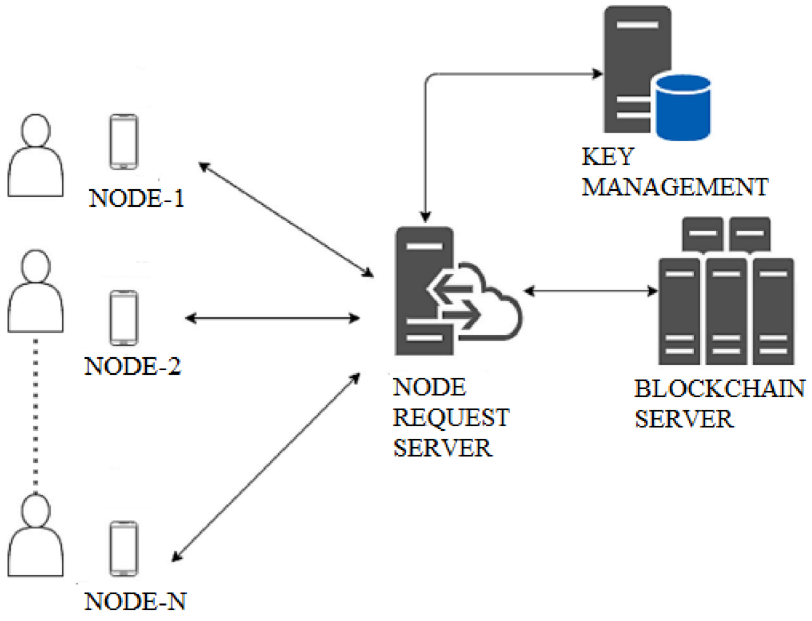

Figure2. Secure Communication Model Using Blockchain

A client request handler, often known as a server, is responsible for processing user requests. A connection has been established between the request handler server and an RAFT server that is hosted in the cloud. Within the architecture that we have presented, we also include a private blockchain server farm. This farm is responsible for storing user data in the form of a private blockchain. We employ an encryption and decryption technique based on AES, together with a key management approach that is described of the document titled "Proposed Technique." This allows for safe communication between the various organisations involved. For the purpose of carrying out the consensus procedure throughout the Key vault farm, the blockchain based consensus is used. Because of its high fault tolerance, simplicity of installation, and performance, was selected as the best option. It is within the scope of what we have in mind. Other algorithms, like as Paxos, ripple, and proof of work, have performance problems on computers with limited processing capacity, which in turn increases the computational overhead. These problems make it more difficult to mine cryptocurrencies. In addition, in the scenario that we took into consideration, it proved to be an excellent choice because it is ideally suited for the kinds of applications that require quick and effective processing at a low cost of implementation and is simple to put into action in order to achieve higher levels of communication efficiency.

The proposed framework becomes more dependable and secure as a result of the addition of a private blockchain server farm. This is because there is no single point reliance, and the blockchain mechanism helps to avoid the various forms of data leakage and data modification attacks.

V. Conclusion:

We provided a platform for secure communication based on the blockchain that may be used for community participation. The given system made advantage of the blockchain's underlying technology, and we implemented that method with a distributed ledger that was tamper-proof. We also created a firmware as an extra layer of security using the secure method in which a key management system is deployed to handle the keys in a safe manner. This was done in order to complement the other layers of security. An Android application (app) has been constructed, using the suggested framework as its foundation, in order to test the app's usability in a real-time setting. The android application that was built may be used to assure the consistency and security of the private data that is required for the engagement of the research community.

The security analysis that was supplied demonstrated that the suggested framework was safe from the many different kinds of attacks that may be launched against it. When we compare the performance of the proposed framework to the performance of other techniques that are comparable, we find that the suggested framework performs better.

Refernces:

[1] S. Wan, M. Li, G. Liu, C. Wang, Recent advances in consensus protocols for blockchain: a survey, Wirel. Netw. (2019).

[2] K. Valtanen, J. Backman, S. Yrjölä, Blockchain-powered value creation in the 5G and smart grid use cases, IEEE Access 7 (2019) 25690–25707.

[3] S. Baskar, S. Periyanayagi, P.M. Shakeel, V.S. Dhulipala, An energy persistent range-dependent regulated transmission communication model for vehicular network applications, Comput. Netw. 152 (2019) 144–153.

[4] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, M. Imran, Securing IoTs in distributed blockchain: Analysis, requirements and open issues, Future Gener. Comput. Syst. 100 (2019) 325–343.

[5] W. Feng, Z. Yan, MCS-Chain: Decentralized and trustworthy mobile crowdsourcing based on blockchain, Future Gener. Comput. Syst. 95 (2019) 649–666.

[6] P.F. Sheron, K.P. Sridhar, S. Baskar, P.M. Shakeel, A decentralized scalable security framework for end-to-end authentication of future IoT communication, Trans. Emerg. Telecommun. Technol. (2019) e3815.

[7] L. Huo, D. Jiang, S. Qi, L. Miao, A blockchain-based security traffic measurement approach to software defined networking, Mob. Netw. Appl. (2020).

[8] C. Lin, D. He, S. Zeadally, N. Kumar, K.-K.R. Choo, SecBCS: a secure and privacypreserving blockchain-based crowdsourcing system, Sci. China Inf. Sci. 63 (3) (2020).

[9] B. Putz, F. Menges, G. Pernul, A secure and auditable logging infrastructure based on a permissioned blockchain, Comput. Secur. 87 (2019) 101602.

[10] D. Yan, F. Liu, Y. Zhang, K. Jia, Dynamical model for individual defence against cyber epidemic attacks, IET Inf. Secur. 13 (6) (2019) 541–551.

[11] G. Da, M. Xu, P. Zhao, Modeling network systems under simultaneous cyber-attacks, IEEE Trans. Reliab. 68 (3) (2019) 971–984.

[12] M. Semerci, A.T. Cemgil, B. Sankur, An intelligent cyber security system against DDoS attacks in SIP networks, Comput. Netw. 136 (2018) 137–154.

[13] C. Liaskos, S. Nie, A. Tsioliaridou, A. Pitsillides, S. Ioannidis, I. Akyildiz, A novel communication paradigm for high capacity and security via programmable indoor wireless environments in next generation wireless systems, Ad Hoc Netw. 87 (2019) 1–16.

[14] H. Peng, Z. Kan, D. Zhao, J. Han, Security assessment for interdependent heterogeneous cyber physical systems, Mob. Netw. Appl. (2019).

[15] D.P. Zegzhda, E.Y. Pavlenko, Cyber-sustainability of software-defined networks based on situational management, Autom. Control Comput. Sci. 52 (8) (2018) 984–992.

[16] A.H. Celdrán, M.G. Pérez, F.J.G. Clemente, G.M. Pérez, Towards the autonomous provision of self-protection capabilities in 5G networks, J. Ambient Intell. Hum. Comput. 10 (12) (2018) 4707–4720.

[17] M.A. Mirza, M. Ahmad, M.A. Habib, N. Mahmood, C.M.N. Faisal, U. Ahmad, CDCSS: cluster-based distributed cooperative spectrum sensing model against primary user emulation (PUE) cyber attacks, J. Supercomput. 74 (10) (2018) 5082–5098.

[18] D.P. Zegzhda, D.A. Moskvin, A.V. Myasnikov, Assurance of cyber resistance of the distributed data storage systems using the blockchain technology, Autom. Control Comput. Sci. 52 (8) (2018) 1111–1116.

[19] J. Guan, Z. Wei, I. You, GRBC-based network security functions placement scheme in SDS for 5G security, J. Netw. Comput. Appl. 114 (2018) 48–56.

[20] M. Keshk, N. Moustafa, E. Sitnikova, B. Turnbull, Privacy-preserving big data analytics for cyber-physical systems, Wirel. Netw. (2018).

[21] L.F. Maimó, A.H. Celdrán, M.G. Pérez, F.J.G. Clemente, G.M. Pérez, Dynamic management of a deep learning-based anomaly detection system for 5G networks, J. Ambient Intell. Hum. Comput. 10 (8) (2018) 3083–3097.

[22] P. Rengaraju, S. S. Kumar, and C.-H. Lung, "Investigation of security and qos on sdn firewall using mac filtering," in 2017 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2017, pp. 1–5.

[23] D. P. Mishra, P. P. Satapathy, and B. Mishra, "Designing a secure network interface by thwarting mac spoofing attacks," in Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. ACM, 2016, p. 102.

[24] C. Aggarwal and K. Srivastava, "Securing iot devices using sdn and edge computing," in 2016 2nd International Conference on Next Generation Computing Technologies (NGCT). IEEE, 2016, pp. 877–882.

[25] M. Steichen, S. Hommes, and R. State, "Chainguard—a firewall for blockchain applications using sdn with openflow," in 2017 Principles, Systems and Applications of IP Telecommunications (IPTComm). IEEE, 2017, pp. 1–8