International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5847
***Article Received**: 04 September 2022 **Revised**: 18 November 2022 **Accepted**: 09 December 2022*

A Novel Design to Minimise the Energy Consumption and Node Traversing in Blockchain Over Cloud Using Ensemble Cuckoo Model

[a] Ravikumar CH , [b]Isha Batra, [c]Arun Malik
[a,b,c] Department of Computer Science & Engineering, Lovely Professional University, Phagwara, Punjab**,** India-144411
E-mail: [a]chrk5814@gmail.com, [b]isha.batra2487@gmail.com,[c]arunmalikhisar@gmail.com

Abstract— The article outlines the Blockchain’s behavioral model for services. Their reliability is proven through the use of experimental evidence. The authors highlight the major technical aspects and characteristics that are associated with the transmission of data through the network. The authors define the scheme for the network, which works with blockchain transactions, and the relationship between network characteristics on parameters used by the application. They examine the use of this model to identification of the blockchain service and also the likelihood of existing security mechanisms that are based on the technology being bypassed. Additionally, the article provides guidelines to conceal the Blockchain's traffic profile to make it more difficult for its detection in the information network. This study offers a thorough analysis of blockchain-based trust models applied to cloud computing. The paper highlights the challenges that remain unsolved and offers suggestions for future studies in the area based on new cloud-edge trust management system and double-blockchain structure, which is a cloud-based transaction model. The paper also identifies the existing challenges and offers suggestions for future studies in the area based on new cloud-edge trust management system and double-blockchain structure, which is a cloud-based transaction model. The flow of the network will be supported by models that are enhanced by cuckoo to frame the perfect network transform of data from one point to cluster, or alternatively.

Keywords- Blockchain, Cloud computing, Botnet, Network, Trust management system

1. INTRODUCTION

Blockchain is a recent and promising distributed computing model as well as a decentralized framework. The legitimacy, security, and dependability of transaction data are all guaranteed by its special abilities in operating rules and the traceability of records. This makes blockchain appropriate for building the decentralized and distributed trust infrastructure. Management of networks has become an increasingly difficult job due to the complicated nature and the various structures of networks across various systems. The manual management of networks isn't practical due to issues such as the limited duration of time difficulties in tracking the configuration state of numerous devices, the requirement for specialists with different backgrounds, and the development of the most efficient method for managing network configurations [1]. These are the reasons for the increasing costs and effort needed to manage networks. In addition network topology is the extended version of the overall resources of the network. Information collection from techniques like software-defined networks (SDNs) has been an extremely challenging process for improving the quality of service, network management, and routing [2]. The number of devices that are connected to IP networks is expected to increase by 29 billion before the time of 2022.

Benefits include the fact that all members of a decentralization network have the same rights and data can be easily exchanged. Reliability any attempt to alter the data without authorization will be rejected because of inconsistent copies of prior copies; any compromise data that is added to it will then be inspected by other users; transparency[3]: any aspect of the transaction could be verified and, theoretically, it could be augmented with new data an endless number of times. Also, confidential data are saved in an encrypted format and the user can track the entire transaction, but not be able to identify those who send or receive information. Risks include errors and fraud since blockchain data can be irreversibly transferred (wrong actions are not reversible) as well as slow transaction speeds, which is a major disadvantage of blockchain technology, especially when utilized as the basis for digital currencies, as well as the possibility of illicit operations[4].

Topology in networks is one of the most important factors that determine the behavior of networks. In today's world, the need for the security of networks has grown because of an increased risk of malicious attacks. In this report, a blockchain-based technology is suggested to securely discover and store networks. Methods like cloud-based storage systems aren't efficient and lack trust privacy, security, and data management. Blockchain-based technology proposed in this paper has the potential of solving these issues [5]. Experiments were carried out with Minuet, Cisco Packet Tracer as well as the Ethereum blockchain, which uses an algorithm for network analysis. The algorithm is capable of determining the network's topology even if only a small amount of information about what is happening on the network. The results show how the system is invulnerable to malicious users as well as various external threats which make the network strong.

The component set can comprise a blockchain network component configured to transmit a block header or a non-blockchain network component configured to send a non-header. The hash-based cuckoo filter allows encryption of block headers during transmission. For applications that keep a lot of items and aim for reasonably low false-positive rates (FPR) in information-sending mistakes, the cuckoo filter permits adding, removing, and retrieving selected items dynamically. An enterprise network can include both a blockchain network and a non-blockchain network [6, 7].

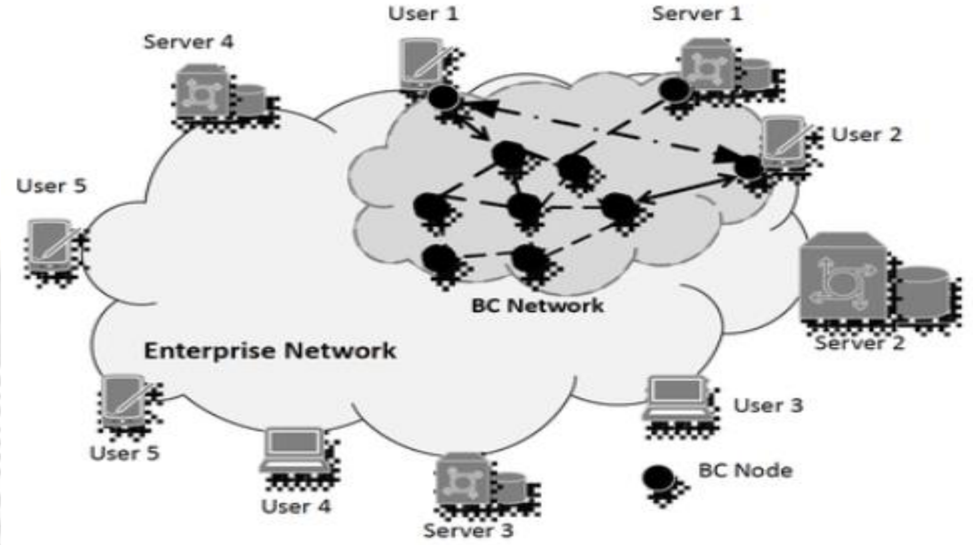


Figure 1: Blockchain can provide relatively immutable security even considering the entire communications networking environment is untrustworthy.

The purpose of this endeavor is to cut down on the energy consumption of a network. To maximize efficiency for the least energy use, care must be paid to make sure that other factors that affect the success of the transfer of data over this network are satisfied. To address this issue improved clustering-based Ensemble Cuckoo Search Algorithm: (ECSA) is recommended. In the algorithm proposed the new method called Proposed Differ Ratio (PDR) has been developed that consists of three parameters, including distance in energy, size, and the dimension of the group. To increase the efficiency of Cuckoo searches, a distinct encoder is used to decode the population.

1.1. Problem Statement:

The nodes in a network are powered by batteries and are typically utilized in a physical environment. The Node is described as a smart, small multi-functional, the self-organizing device that is inexpensive and has batteries, and radio communications in addition to a microcontroller and sensors. It's not as powerful in its processing power batteries, memory, and power also; it has an extremely limited range of sensors. It is a particular application that was designed to monitor and control the physical environment from far away areas with greater accuracy.

1.2. Contributions:

In the present work, the efficiency of the model is increased, and reducing traversing time for the nodes to update with the data processing has been increased compared to that of the existing cuckoo models. The work resembles to be efficient and worthy of the model developed. The major concern is about the data node communication which is very important in the cloud blockchain and has been at-most sorted out in the proposed model.

2. RELATED WORKS:

Cloud Data Integrity Verification: Many academics are aware of remote audits of data integrity as a result of the rising use of cloud-based storage systems. Cloud users can ensure the integrity and accessibility of data in cloud storage by verifying the integrity of the storage in the cloud. The integrity of data has been guaranteed using a variety of approaches to mitigate the security risks that cloud storage poses. Provable Data Possession (PDP) schemes and Proved

Retrievability (POR) strategies are two categories into which these schemes for verifying data integrity can currently be divided. PDP schemes use the "challenge–response" technique to verify that user data are correctly stored in cloud storage. POR schemes use the challenge-response method to verify that data is actually stored. Some data can be recovered using POR techniques. They can also confirm the identity of the verifier, so the verification process can be split into a public and private process. TPA provides better support for public auditing, instantaneous updates and more effective verification than private verification [8].

The challenge-response system, which uses the RSA algorithm to generate key pairings and trust third-party audits, to verify data integrity, has been first presented by Ateniese et al. [3]. To confirm that the data is in excellent shape, the CSP only needs to return the label information for the block in the file, which lowers the communication and computing burden of the verification procedure. However, this approach forbids the dynamic updating of data. An adaptive PDP was recommended by Ateniese et al. [11] to support the auditing of data in real-time.

Additionally, Zhou et al. [14] cautioned that the technique was unable to counteract a forgery attack, which meant that an adversary using evidence may fabricate new pieces of documentation by repeatedly employing the same secret code to go past the integrity verification procedure.

An index hash table (IHT) structured data structure was proposed by Zhu et al. ([15-16]) to allow the dynamic functioning of public audits. The amount of storage needed for verification data can be decreased with IHT. In order to allow the auditing of batch and dynamic data and to provide security for data privacy integrity systems, Yang et al. [17] used bilinear pairing in place of mask technology. However, Ni and colleagues [18] have shown that this method is unsafe since it lacks response authentication and is vulnerable to attacks from enemies.

3. PROPOSED METHODOLOGY

Let B = (b1. . . bm)⊂Rn be a set of linearly independent vectors, then the lattice Λ generated by B is Λ = Bc =M m ≤ n, and B is referred to as the base of the lattice.) size of the foundation B refers to its length in the longest vector B. The orthogonal basis standard for B is obtained using an ordinary Schmidt orthogonalization is a problem. If q is an integer and the matrix A ∈ Zn×m q, and a real number β, find a set of nonzero solutions such that the homogeneous equation Ae = 0 mo d q holds Blockchain. Blockchain is an essential idea of Bitcoin [15] that is fundamentally an open database that is decentralized and simultaneously functions as the base technology of Bitcoin. Blockchains are a collection of data blocks that are created using cryptographic techniques [19]. Each block is a record of the Bitcoin network transaction, which is used to confirm the validity of its data and create new blocks.

A distributed ledger that cannot be changed or produced by cryptography, a blockchain is a data structure chained that successively connects blocks of data by the time sequence. In general, blockchain technology uses the data structure of the Blockchain to validate and store information, distributed consensus algorithms to create or update information, cryptography to ensure that only authorized parties have access to data and transmission, and smart contracts, which are automated scripts that programmed and modify data.

3.1. Cuckoo Filter

A random data structure with a straightforward layout and excellent spatial efficiency is called a cuckoo filter [16]. This bloom filter outperforms other bloom filters in terms of query performance, capacity usage, and ability to reverse operations. For each keyword, there are two storage options available. Additionally, it quickly locates keywords during lookup operations and dynamically moves already-used keywords to make way for new ones during the insertion process. Although the insertion complexity of the cuckoo filter is projected to be O(1), repeated relocations are required.

Cuckoo Search (CS) algorithm is a nature-inspired global optimization algorithm based upon the brood parasitic behavior of cuckoos. It has been proven to be a reliable algorithm, having been successfully used to solve a wide range of challenges in a variety of domains. CS utilizes Levy flights to produce steps to explore the solution space efficiently [19]. Local search is performed with the help of switch probability where certain proportions of the solutions are removed. While CS is an efficient algorithm, its performance could be improved by incorporating exploration and exploitation aspects of the process of searching.

3.2. Cuckoo Search algorithm:

Each nest in this optimization process corresponds to a potential resolution. Three rules simplify the cuckoo reproduction process in the algorithm:

1. Each cuckoo deposits an egg in a randomly selected nest;

2. The best nests are passed down to the subsequent generation;

3. With a probability Pa that ranges from [0,1], the host bird finds the cuckoo egg with a fixed (limited) number

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 1s
DOI: https://doi.org/10.17762/ijritcc.v10i1s.5847
***Article Received**: 04 September 2022 **Revised**: 18 November 2022 **Accepted**: 09 December 2022*

of host nests accessible. Because only the worst nests can be detected by birds, their number is decreasing.

3.3. Ensemble Cuckoo Search Algorithm:

The proposed improved cuckoo search method-based routing system features energy efficiency and has delays-aware routing. Cuckoo search is an efficient method that can be used to increase efficiency and improve the quality of service (QoS) components like the capacity to use energy, bandwidth delay the most efficient distance between two locations, and the ratio for the transmission to data transmission. It reproduces by placing eggs inside its nests. The bird that hosts them is a means of cuckoo reproduction. If one host becomes aware of cuckoo eggs within the nest, it could discard eggs from other species, or even leave the nest to build another nest. Cuckoo search optimization (CSO) is focused on reproduction and may help with a range of optimization issues. It is a much better strategy than the meta-heuristic algorithm.

1. Convergence of the Cuckoo Search algorithm can be significantly improved through the use of genetically replacing nests that have been abandoned (instead of using random replacements of the initial method).
2. Changes in the algorithm have been achieved through interbreeding between the most desirable high-quality nests and the method is successfully used to solve various industrial optimization issues.
3. The network's structure can be constructed by incorporating inputs, and outputs of layers interconnections, inputs, and interconnections. Then, the number of times can be calculated, and how many times are required to fully learn.
4. Diagram of architecture reveals that the Network first can be aware of the previous configuration created by its Nodes and the loads placed on it. Then it assigns load according to the design of learning and defines in incremental steps the amount of load that must be eliminated from every Node.
5. It is a back-forward propagation Neural Network as it traces back the outcomes. Based on the results of the verifications, it continues forward. After the validation has been completed it traces back the results with the mean of square Error. The subsequent environment was employed to analyze the results.
6. Perfect node connectivity for data transmission formed by using available nodes, available paths, and available clusters with blockchain by the intrusion system.

Three alternative CS modifications are suggested in this study to enhance exploring and exploration [20]. Instead of using Levy flights to efficiently explore the search area, each of these variations computes the step size using the Cauchy operator. To further ensure that exploitation and exploration are equally balanced, CS also incorporates the ideas of population division and generation division. 24 benchmarks with various dimensions and population sizes were used to evaluate the proposed CS algorithms, and the effects of probability switches are being investigated. Comparing the modified algorithms statistically against the existing ones using grey wolf optimization in differential evolution.

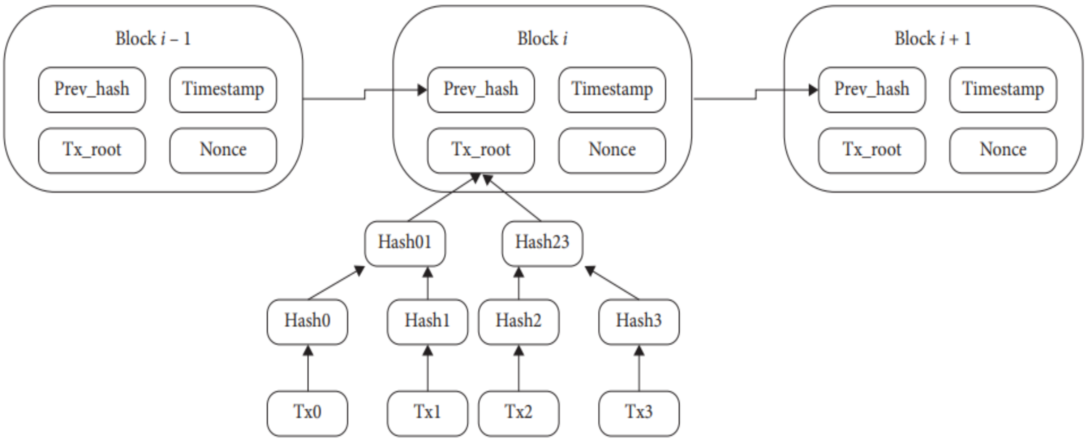


Figure 2: The basic structure of blockchain

DOI: https://doi.org/10.17762/ijritcc.v10i1s.5847
***Article Received**: 04 September 2022 **Revised**: 18 November 2022 **Accepted**: 09 December 2022*

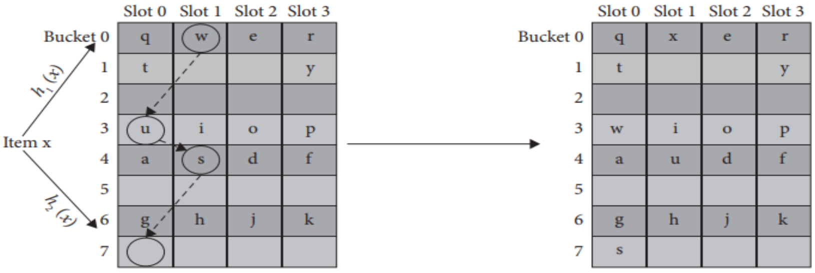


Figure 3: Working model of cuckoo filter.

Each bucket is equipped with one slot and each has four slots. Data Integrity verification System: To verify the data integrity of data safely and effectively, this scheme must possess the following characteristics.

(1) Dynamic integrity validation: Users frequently need to update the data they have submitted to the CSP. Data must be capable of dynamic changes, such as the capacity to insert data as well as delete and modify existing data.

(2) Avoid quantum attacks. Lattice cryptography is becoming more crucial in the realm of information security and cryptography as a result of the development of quantum technology and the introduction of quantum computers. The suggested approach ought to be secure in a quantum setting and robust enough to resist off attacks from quantum computers.

(3) Trusted audit: If users upload their files to CSP and take ownership of their data, the security of that data is significantly compromised because cloud-based environments may not be compatible with traditional methods of verification. Additionally, the CSP may be vulnerable to deliberately altering the data security [21]. Therefore, the proposed approach for preserving data integrity must guarantee the validity and dependability of the findings of data authenticity verification[22][23].

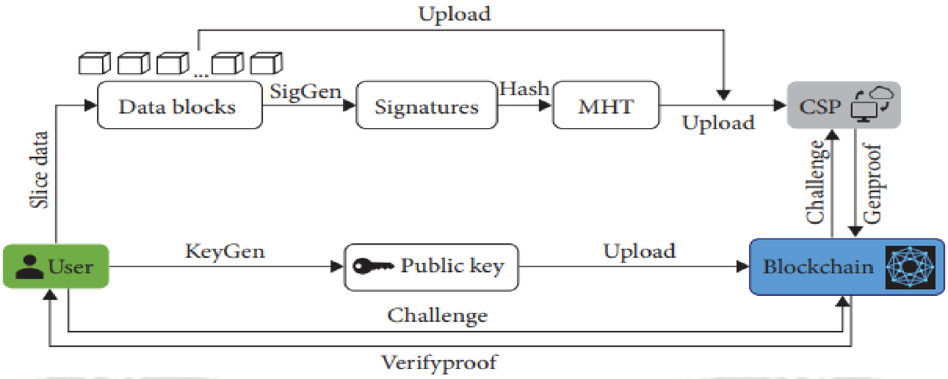


Figure 4: System Verification process

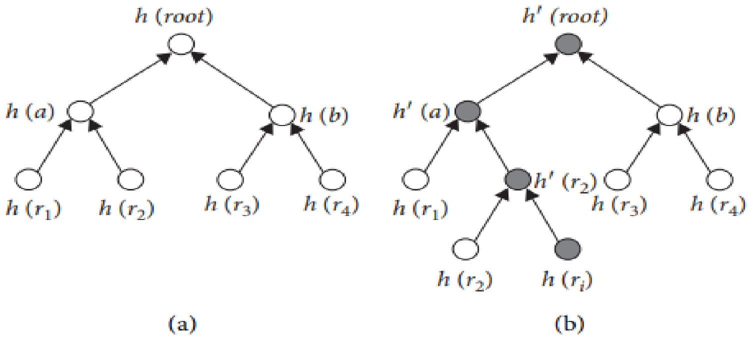


Figure 5: Insert MHT operation

DOI: https://doi.org/10.17762/ijritcc.v10i1s.5847
Article Received: 04 September 2022 Revised: 18 November 2022 Accepted: 09 December 2022

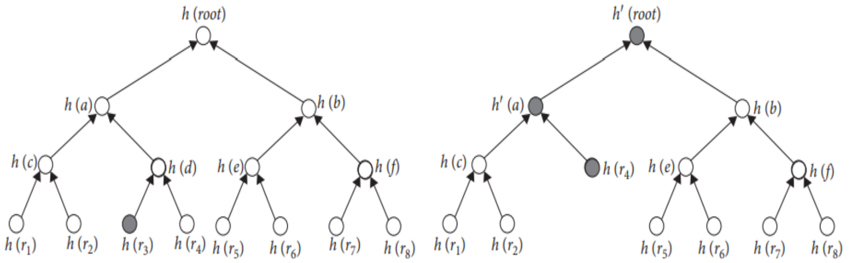


Figure 6: Delete MHT operation

4. EXPERIMENT RESULTS AND EVALUATION

The architecture of the network can be constructed with inputs, and outputs of layers interconnections, inputs, and interconnections. Then, the number of times can be determined, as well as the number of iterations that are needed to complete learning. A diagram depicting the structure says that the Network first can be aware of the previous configuration created by its Nodes and the load that it is placed on it. Then it assigns load according to the learning model and then outlines in successive steps the quantity of load to be taken away from every Node[24][25]. It is a back-forward propagation Neural Network as it traces back the outcomes. Based on the results of the verifications, it moves forward. After the validation has been completed it traces back the results with the mean of square Error [26][27]. The subsequent environment was employed to analyze the results.

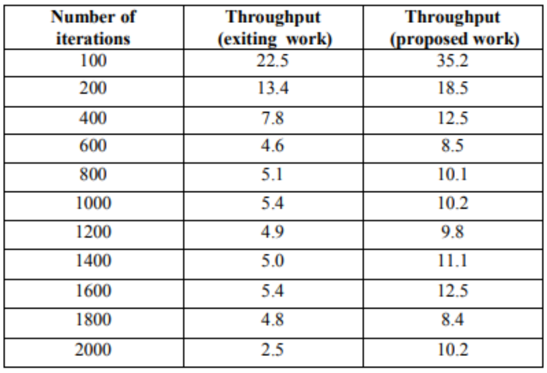
Steps:

- Find the nests of nodes by collaborating with the host.
- The maximum number of nodes generated, after which Cuckoo randomly replaces cuckoo's response with Levy flights.[28]
- Examine its suitability and quality.
- Replace the old solution with the new one (near).
- A part (Pa) of the most harmed nests is discarded and nests are built;
- Be sure to be using the most effective methods and nests.
- Find the most effective solutions by comparing them and determining the most effective solution.
- Transfer the most effective strategies that are in use today to the next generation
- The show will close at the conclusion

Table 1: Simulation Parameters

Attributes	**Measures**
Sample Nodes	100
Size of Area	1000 X 1000 m
Address MAC-IP	801.41
Frequency Range	350m
Result Estimated Time	100 sec
Network Traffic	Dataset with Packets
Size of Packets	90 Bytes

Table 2: Throughput comparison with predicted measures



Number of iterations	**Throughput (exiting work)**	**Throughput (proposed work)**
100	22.5	35.2
200	13.4	18.5
400	7.8	12.5
600	4.6	8.5
800	5.1	10.1
1000	5.4	10.2
1200	4.9	9.8
1400	5.0	11.1
1600	5.4	12.5
1800	4.8	8.4
2000	2.5	10.2

***Article Received**: 04 September 2022 **Revised**: 18 November 2022 **Accepted**: 09 December 2022*

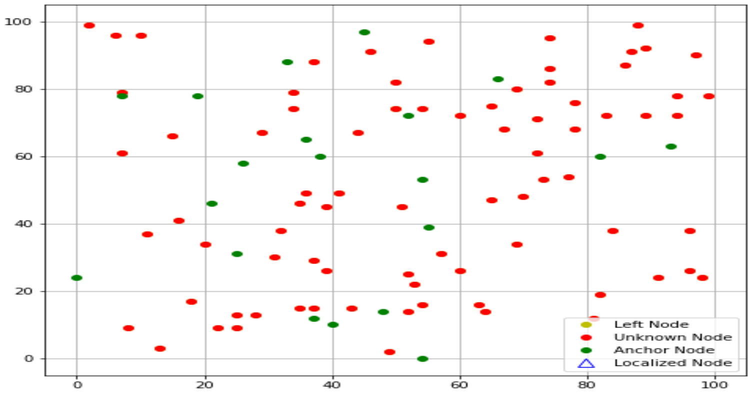


Figure 7: The above graph shows us the nodes which are being pointed or made available for data transmission and were ready for the connectivity

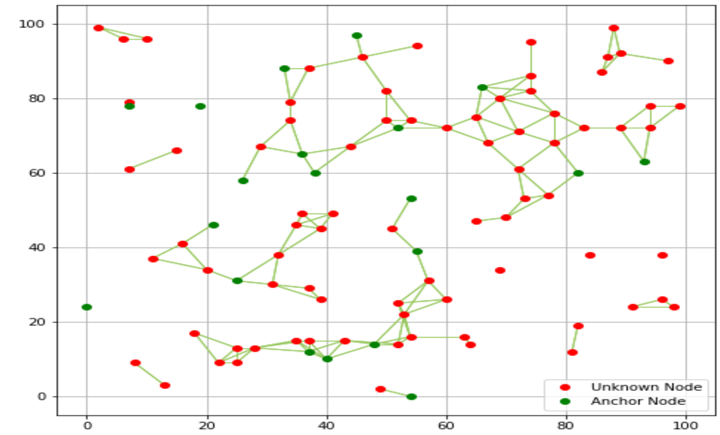


Figure 8: Exiting The Connected nodes with the network which has been formed from the nodes that cuckoo trained and these are available for the data transmission

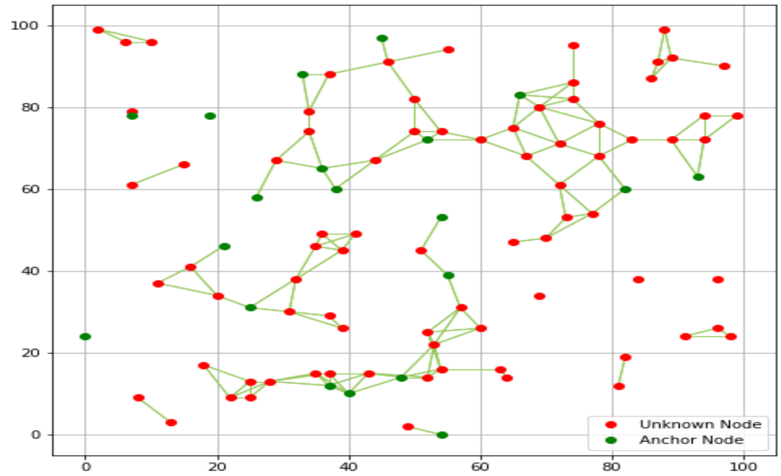


Figure 9: Results show the best and most reliable nodes that are connected for the transmission and the remaining nodes which are been left over by the cuckoo model

DOI: https://doi.org/10.17762/ijritcc.v10i1s.5847
***Article Received**: 04 September 2022 **Revised**: 18 November 2022 **Accepted**: 09 December 2022*

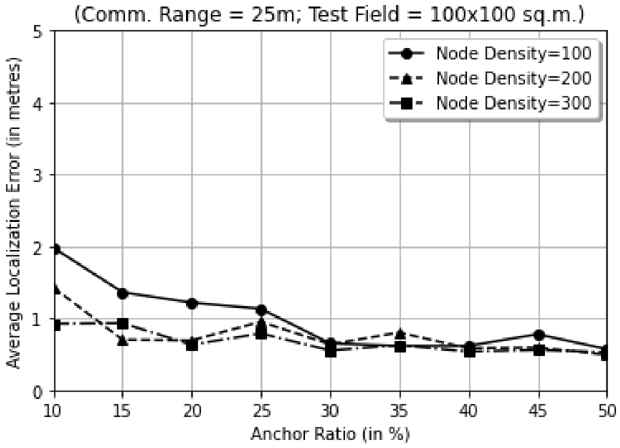


Figure 10: The node density shows the range of the nodes and their error rate in the connectivity of the model and their strength

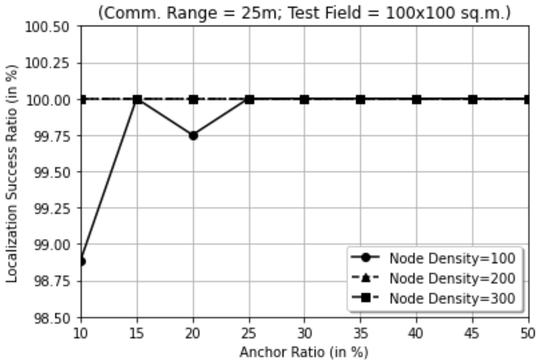


Figure 11: The results show us the success ratio of the model in terms of connectivity measured with a variable number of nodes; our model proves that connectivity is stable with the increase in the number of nodes

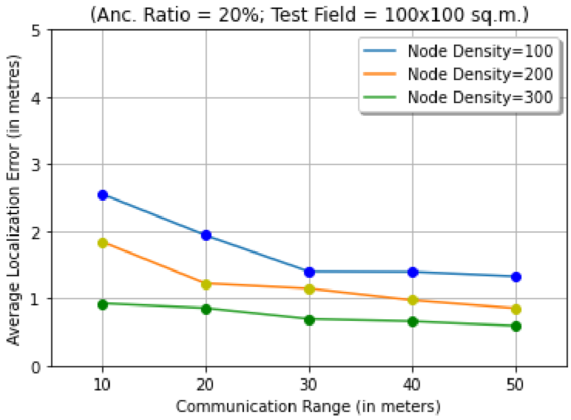


Figure 12: Data transmission range and the communication of the nodes, this shows us that the more range and more nodes the transmission is perfect.

***Article Received**: 04 September 2022 **Revised**: 18 November 2022 **Accepted**: 09 December 2022*

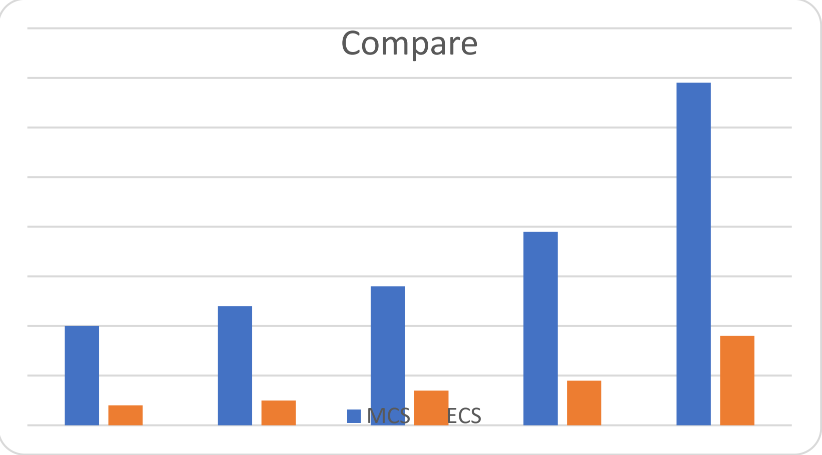


Figure 13: Compare the average localization error ratio between existing and proposed cuckoo models

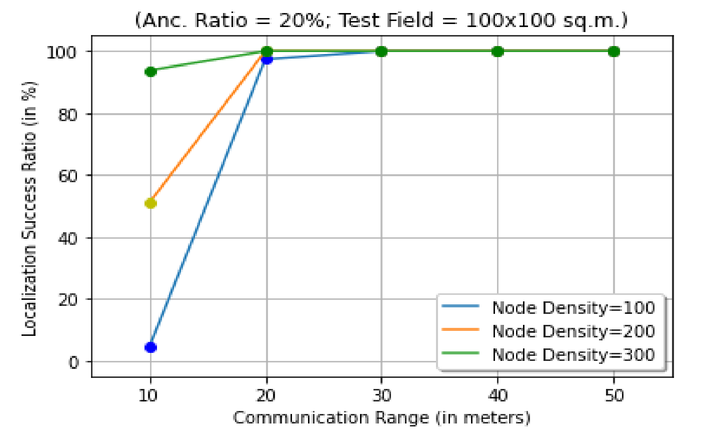


Figure 14: The Success ratio of the model with most nodes which has been communicated with the help of the advanced cuckoo model, this again shows us the connectivity is good and efficient when the nodes and more and is directly reflected in the density of the nodes

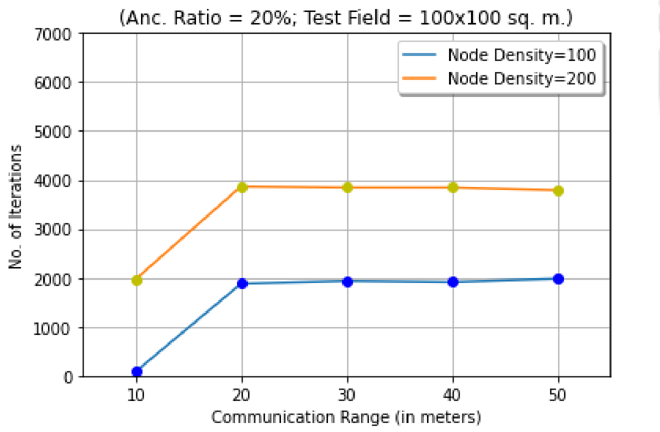


Figure 15: The communication range is projected in the graph

DOI: https://doi.org/10.17762/ijritcc.v10i1s.5847
***Article Received**: 04 September 2022 **Revised**: 18 November 2022 **Accepted**: 09 December 2022*

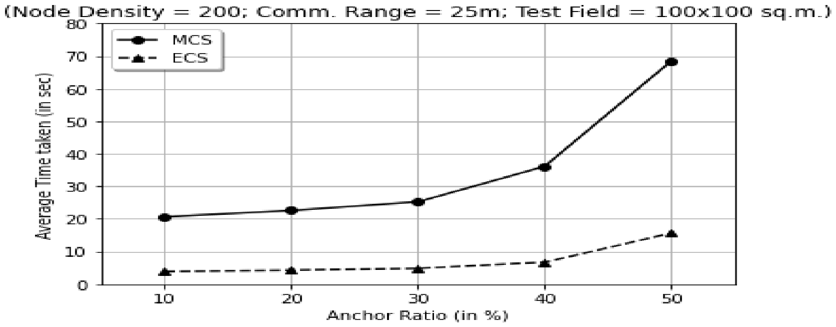


Figure 16: The approach between existing and proposed cuckoo models

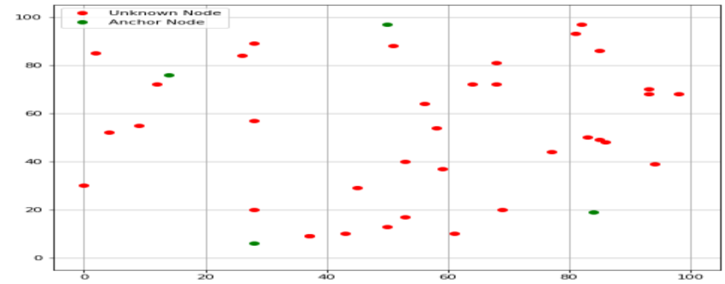


Figure 17: The nodes which are made available from the cuckoo-based model, the advanced model will work on the empty and remaining idle nodes to make a stronger and reliable, and efficient model

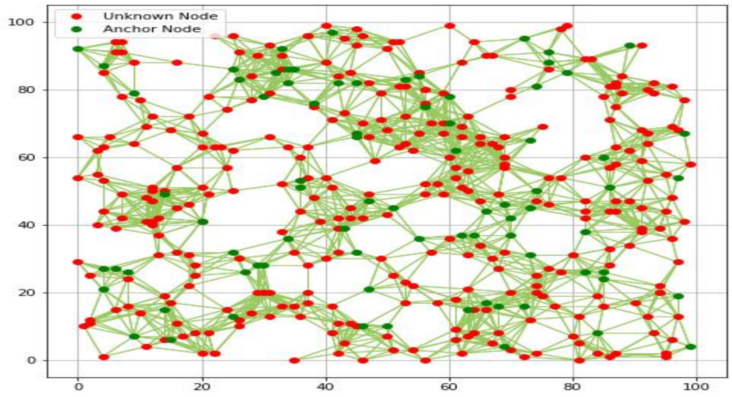


Figure 18: The proposed cuckoo model with perfect node connectivity for data transmission and enable efficiency in terms of energy consumption and utilization.

5. CONCLUSIONS

The need to protect the integrity of cloud-based data and the rapid rise of cloud storage and cloud data storage are now common themes. This study introduces a powerful blockchain-based cloud-based data integrity checking solution. We intend to use blockchain to strengthen the effectiveness and security of the system while addressing some flaws in the conventional central audit methods. We believe that our system can withstand the threat posed by quantum computing, and by combining lattice-based authentication and cuckoo filtering, we can address the issue of users' insufficient computing power while still simplifying the process of user identity verification. Our plan is based on the assumption that there is a SIS problem. The effectiveness of the suggested plan is assessed, and the findings show that it is effective. Studying the potential integration of integrity-based verification with blockchain is necessary, and the scheme's more extensive requirements must be fully met.

REFERENCES

[1]. S. Nepal, S. Chen, J. Yao, and D. Thilakanathan, “DIaaS: Data Integrity as a Service in the Cloud,” in Proceedings of the 2011 IEEE 4th International Conference on Cloud Computing, pp. 308–315, IEEE, Washington, DC, USA, 2011.

[2]. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds,” in Proceedings of

the 16th ACM Conference on Computer and Communications Security, pp. 199–212, ACM, New York, NY, USA, 2009.

[3]. G. Ateniese, R. Burns, R. Curtmola et al., "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 598–609, ACM, New York, NY, USA, 2007.

[4]. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: beyond bitcoin," Applied Innovation, vol. 71, no. 2, pp. 6–10, 2016.

[5]. W. S. H. M. W. Ahmad, N. A. M. Radzi, F. S. Samidi et al., "5G technology: towards dynamic spectrum sharing using cognitive radio networks," IEEE Access, vol. 8, pp. 14460–14488, 2020.

[6]. J. Su, R. Xu, S. Yu, B. Wang, and J. Wang, "Idle slots skipped mechanism based tag identification algorithm with enhanced collision detection," KSII Transactions on Internet and Information Systems, vol. 14, no. 5, pp. 2294–2309, 2020.

[7]. J. Su, R. Xu, S. Yu, B. Wang, and J. Wang, "Redundant rule detection for software-defined networking," KSII Transactions on Internet and Information Systems, vol. 14, no. 6, pp. 2735–2751, 2020.

[8]. X. Jiang, J. Yu, J. Yan, and R. Hao, "Enabling efficient and verifiable multi-keyword ranked search over encrypted cloud data," Information Sciences, vol. 403-404, pp. 22–41, 2017.

[9]. Z. Zhou, Q. M. J. Wu, Y. Yang, and X. Sun, "Region-level visual consistency verification for large-scale partial-duplicate image search," ACM Transactions on Multimedia Computing, Communications, and Applications, vol. 16, no. 2, pp. 1–25, 2020.

[10]. Z. Zhou, Y. Mu, and Q. M. J. Wu, "Coverless image steganography using partial-duplicate image retrieval," Soft Computing, vol. 23, no. 13, pp. 4927–4938, 2019.

[11]. G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, pp. 1–10, ACM, New York, NY, USA, 2008.

[12]. C. C. Erway, A. K¨upç¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," ACM Transactions on Information and System Security, vol. 17, no. 4, pp. 1–29, 2015.

[13]. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.

[14]. E. Zhou, Z. Li, H. Guo, and Y. Jia, "An improved data integrity verification scheme in cloud storage system," Acta Electronica Sinica, vol. 42, no. 1, pp. 150–154, 2014.

[15]. Y. Zhu, H. Wang, Z. Hu et al., "Dynamic audit services forintegrity verification of outsourced storages in clouds," ", ACM, in Proceedings of the 2011 ACM Symposium on Applied Computing, pp. 1550–1557, ACM, New York, NY, USA, 2011.

[16]. Y. Zhu, G. J. Ahn, H. Hu et al., "Dynamic audit services for outsourced storages in clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227–238, 2011.

[17]. K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717–1726, 2012.

[18]. J. Ni, Y. Yu, Y. Mu, and Q. Xia, "On the security of an efficient dynamic auditing protocol in cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 10, pp. 2760-2761, 2013.

[19]. G. Xu, Y. Bai, C. Yan et al., "Check algorithm of data integrity verification results in Big data storage," Journal of Computer Research and Development, vol. 54, no. 11, pp. 2487–2496, 2017.

[20]. W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling identitybased integrity auditing and data sharing with sensitive information hiding for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 14, no. 2, pp. 331–346, 2019.

[21]. A. Li, S. Tan, and Y. Jia, "A method for achieving provable data integrity in cloud computing," Ee Journal of Supercomputing, vol. 75, no. 1, pp. 92–108, 2019.

[22]. H. Zhu, Y. Yuan, Y. Chen et al., "A secure and efficient data integrity verification scheme for cloud-IoT based on short signature," IEEE Access, vol. 7, pp. 90036–90044, 2019.

[23]. K. Huang, M. Xian, S. Fu, and J. Liu, "Securing the cloud storage audit service: defending against frame and collude attacks of third party auditor," IET Communications, vol. 8, no. 12, pp. 2106–2113, 2014.

[24]. Y. Wu, X. Lin, X. Lu, J. Su, and P. Chen, "A secure light-weight public auditing scheme in cloud computing with potentially malicious third-party auditor," IEICE Transactions on Information and Systems, vol. E99.D, no. 10, pp. 2638–2642, 2016.

[25]. Shere, R., Shrivastava, S., & Pateriya, R. K. (2017). CloudSim Framework for Federation of identity management in Cloud Computing. International Journal of Computer Engineering in Research Trends, 4(6), 269–276.

[26]. PRAVEEN KUMAR, & S.NAGA LAKSHMI. (2015). Efficient Data Access Control for Multi-Authority Cloud Storage using CP-ABE. International Journal of Computer Engineering in Research Trends, 2(12), 1182-1187. Retrieved from https://www.ijcert.org.

[27]. Prakash, P. S., Janardhan, M., Sreenivasulu, K., Saheb, S. I., Neeha, S., & Bhavsingh, M. (2022). Mixed linear programming for charging vehicle scheduling in large-scale rechargeable WSNs. Journal of Sensors, 2022, 1-13. doi:10.1155/2022/8373343

[28]. Yedukondalu, G., Samunnisa, K., Bhavsingh, M., Raghuram, I. S., & Lavanya, A. (2022). MOCF: A multi-objective clustering framework using an improved particle swarm optimization algorithm. International Journal on Recent and Innovation Trends in Computing and Communication, 10(10), 143-154. doi:10.17762/ijritcc.v10i10.5743