How to Cite:
Durga, R., & Poovammal, E. (2022). Calibration of chaos medichain by non-functional testing approaches. *International Journal of Health Sciences*, *6*(S4), 4456–4468. https://doi.org/10.53730/ijhs.v6nS4.9090

Calibration of chaos medichain by non-functional testing approaches

Durga R
Department of Computing Technology, SRM Institute of Science and Technology, Kattankulathur, India - 603203
Corresponding author email: dr8529@srmist.edu.in

Poovammal E
Department of Computing Technology, SRM Institute of Science and Technology, Kattankulathur, India - 603203
Email: poovamme@srmist.edu.in

***Abstract*---**The evolution of blockchain networks extends with the proliferation of the Internet of Medical Things devices. These devices require stupendous storage space which enlarges the maintenance cost. It raises undermined data security & Privacy, risk of failure, dishonest interlopes access to the centralized system. The propitious solution against these challenges of an extensive centralized system is decentralized-based blockchain technology. This paper implements decentralized-based blockchain architecture deployed with chaotic encryption and proof of consensus mechanism for mining. The disintermediate architecture as an enchanting target for Denial of Service (DoS) attacks. To covenant the trust, testers must certify that all the components of the blockchain network are employing flawlessly. The performance of non-functional testing assured the quality assurance services is a decisive aspect of the proposed blockchain architecture. The proposed decentralized-based blockchain framework is calibrated by injecting various malicious attacks. Moreover, the attacks are injected with other encryption-based blockchains to correlate the high effective scheme for medical data security. The evaluation reveals that the Proposed chaos medicine architecture shows 14% lower latency than SHA and 18 % lower latency than AES on all attacks and deliberate to be safe from malicious attack.

***Keywords*---**calibration, blockchain networks, non-functional testing approaches.

Introduction

The smart healthcare enhances the quality of healthcare through the intelligent Internet of things. The electronic medical record used in medical sector for intelligent processing. The healthcare service centres have serious attacks concerned over the intelligent processing past few years. The HIPAA (Health Insurance Portability and Accountability Act) reported attack breeches up to 418 thereby 34.9 million citizens of US had compromised their secured patient health information. In IOMT of interconnected devices of trusted network need mediators. It is found that many security breaches at various levels of IoT applications. The complexity occurs at various components due to low performance of heterogeneity devices. There are many properties affecting the IoT leads to attack on networks. The increase in count of attack on IoT based medical network leads to serious effects It leads to issues/ challenges of IoT in health care includes (i) Security measures (ii) Authentication (iii) Access Control (iv) Confidentiality. The diverse platforms are buildout to address the interoperability of digital health care records

Among that block chain technology [20] experimentation in scripts four issues on interoperability, confidentiality, patient centric access, flexibility and accountability. Therefore, the scientist of medical care brings the solution of decentralized based block chain technology with unique attributes like process automation, seamless data sharing, data monetization, advanced identity security and preserves privacy [25]. Hence, medichain architecture is considered as promising technology for storing the medical data.

The disintermediate technology adopts several standards on encipher techniques like AES [16], ECC and SHA [17]. These techniques have some negative reviews on security, while fetching the medical data securely due to fixed key generation and the key dependency [18]. To ameliorate the security within the block, the efficacious hybrid chaotic encryption was propounded based on 3D logistics maps and 3D Lorenz code. Hong Jun Liu proposed 2D Chebyshev sine map for colour image encryption. The results demonstrates that chaotic encryption algorithm works fast, the high randomness and very little accidental leakage information [13]. Xing Yuan Wang proposes [14] image encryption scheme on cat mapping and matrix magic transformation replacement method using SHA512 for generating 12 set keys to the initial value. The demonstration results shows that the algorithm gives good performance and resist on various statistical attacks. Shenyong Xiao [15] proposes new chaos-based image encryption scheme based on switch control mechanism uses three dimensional Lorenz chaotic system to generate pseudorandom sequence. It shows the good performance in comparing with another algorithm. The hybrid chaotic encryption is a high-powered process which consists of many eccentric inbuilt features like high sensitivity and high randomness behaviour [24]. The block chain technology inherits these features to do unwavering secure transmission as it is infeasible to find the time series created by the high-rise dynamic hybrid chaotic system.

In this paper Chaos based medichain is propounded to share the medical based record among the authorized users in the decentralised network. Even, the disintermediate immutable architecture also suffers from the attacks. There are

many attacks against the nodes of the blockchain network. The nodes of the decentralised network processing the data and imparts the data based upon predefined protocols. The intruder can attack the disintermediate decentralised network which relays on the software and system by means of destructing the software misconfiguration, passing Denial of service attacks, malwares.

The researchers Cornell Tech identified and described the blockchain denial of service attack on the decentralised network on ACM 2020 SIGSAC Conference. The Distributed Denial of Service attacks conduces to target the web servers of the private organisations [21]. The DoS attacker blasted the servers with heavy spam traffic. It leads to overloading causes the server unable to serve the genuine request. The sybil attack on blockchain results in refusing the new blocks added in the network by running malicious node. So, these attacks aim to slowdown the process or it collapses the network. It also causes severely damages to the bandwidth connectivity results in disruption of all medical services in the network [22].

While developing the decentralised blockchain network, it is crucial to consider the infrastructural security [23]. Since the disintermediated peer to peer network processing the medical sensitive data should be tested to minimize the vulnerability of the attacks. To calibrate the proposed chaos medichain, testing the propounded architecture by injecting the DDoS, DoS, Ultradoser, Botnet attack code. The codes will be passed with different percentage as 25%,50%,75%,100% to the proposed network to find out how chaos medichain have implemented to deal with medical sensitive data on resisting the attacks.

The Blockchain applications need to integrate with other systems in order to access the data through the smart contract agreement. The application program interface acts as the integration point for the foundation for blockchain technology. Security susceptibility also endures in this technology that attacks the distributed ledger. Recurrently the attacks are lofted on the blockchain applications due to their reputation or the type of sensitive data involved their decentralised system. DDoS, DoS attacks are contemplated as most treacherous cyberattacks in the computer. It directs to the huge loss for the organization. So thereby received the lots of attention today. Henceforth, there is need to preclude these attacks by testing the decentralised system.

The decentralised based cryptocurrencies such as bitcoin, gold, Litecoin cash, mona coin, Zen cash, verge is targeted on May and June 2018 by 51% attack [1]. The attackers gain 51% of the network redirects the transaction and excludes the other miners from the mining process. It led to the $ 5 million USD loss and double spending. The disintermediate peer to peer system is exposed to the eclipse attack [2] in which a cluster of malicious nodes detached the nearby neighbouring node using IP addresses. Due to detachment of the honest nodes the compromised nodes in the network control the traffic, that feeds the fabricated information about the transaction happened in the blockchain.

MedRec[3] relays on the blockchain network adopts the Electronic Medical Record in the decentralised manner. The author [4] provides some trust less measurements on Med Rec for sharing health care records due to security

limitations. Yue at al [5] proposed the private blockchain to store the healthcare data against integrity attacks. The limitations of this private blockchain is leakage of the sensitive data by sending replicas to the requestors without the permissions of the owner and high cost computation.

The DDoS attack in PBFT relayed private blockchain produces 33% malicious node [6], since the participation nodes are small in the private network it calculates the automatically that how many 'M'sybil nodes are needed to attack the network. It launches all the sybil nodes to hurdle the verification procedure. The primary procedure is to get the approval from at least 3M+1 replica, it will not able to follow the systematic progress to initiate the transaction and the decentralisation system will leads to DDoS attack.

The medical image data with the features of high volume and redundancy with strong correlation in health care application needs more cryptology technique than Data Encryption Standard, Advance Encryption Standard, RSA, SHA. The encryption technique which has drawn great fascinate on researches to be used in block chain technology for health care application. Based on the innate properties of chaos [19], such as high pseudorandom, sensitivity, control parameters crypto systems have evinced exemplary properties such as complexity, security and computing power.

To evaluate the security schemes of the system to identify the protection behaviour, there exists many experimentation techniques like security audit. In this paper, simulation of a DDoS, DoS, botnet, ultradoser attack using this security audit technique is intended to explore the strength of the proposed chaos medichain network. It is an opportunity to verify the behaviour of the decentralised system during an attack and recognise the potential vulnerabilities. Then the results are compared with the basic standard encryption algorithm to check the enhancement of the complexity of the chaos algorithm.

Architecture of chaos medichain

Chaos Medichain inculcates the bi-scroller chaotic encryption method for encrypting the image [8] and stores the chaotic encrypted medical image in to the blockchain. We rely on chaos based medichain to accomplish the strong security, antileakage of sensitive medical data. The private block chain-based architecture consists of chain of blocks interconnected consists of the following fields for best operation. It consists of medichain block, storage, API service layer and User Interface layer as depict in figure 1. The medichain block constitutes Version, Previous block hash, Merkle root, Time Stamp, Nonce, Consensus Mechanism,

Transaction, Smart Contract.

1. Version: The block chain version evolution number.
2. Previous block hash: It is the reference for the previous block in the network. With the assist of this hash number, the blocks are ordered.
3. Merkle Root: This root holds all the hashes of all approved transactions occurred in the blocks. All the approved transactions are combined as pair by pair until becomes a single entity hash.

4. Timestamp: Each approved block is created with the timestamp.
5. Nonce: With the Nonce, the node is approved to append the block to the chained network.
6. Consensus Mechanism: The Proof of Work is the consensus mechanism used in our architecture. It solves the mathematical puzzle and find the valid hash key. It is frequently battle tested mechanism to reach out the consensus in effective time. It is intensively computable mechanism to achieve the consensus in block validation. The hashes with the high number of zero's defined as higher difficulty. It can be achieved by including the computed hash function in the proposed consensus mechanism that satisfies the difficulty criteria.
7. Smart Contract: The propounded chaos medichain consists of smart contract with predefined rules in the executable environment. Before starting the transaction, the smart contract was invoked to verify the agreement based on the predetermined rules. The smart contract holds the parameters like new state and successful transaction information.
8. Transaction: The transaction of the chaotic encrypted image is between client and server. It constitutes three layers (i) Retrieval, (ii) Transaction, (iii) Timestamp. In retrieval section, User ID Number, is the unique number to upload the medical image. downloading site information and the image label. The transaction consists of unique hash generated by the bi-scroller chaotic hashes for enhancing the complexity level in security. The timestamp reflects the time of exchanging the medical data.

The storage unit constitute the firebase realtime database is a cloud-hosted database for our propounded chaos medichain architecture. The medical data is stored and synchronized in real-time to all connected blocks in the network using blockchain access API. API service layer is used to do the following (i)The Private and Public Keys for signing transactions, (ii) Creating a HTTP Provider for web3, (iii) Storing the contract as well as address. API gateway accept the various services from the user and aggregates the response with the appropriate results. The User Interface layer connects to the medichain through API gateway to incorporate data exchange, data request to the chaos medichain

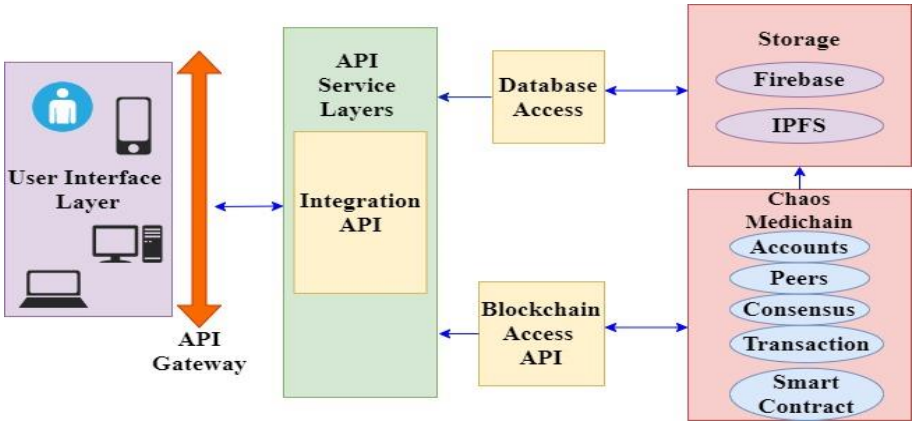

Figure 1. Medichain Architecture

Methodology adopted

The private servers /clouds for implementing the image encryption algorithms using Django Framework. The blockchain server runs on the PC workstation with 2TB hard Disk, 16GB RAM @3.00 GHZ operating frequency. The blockchain servers are developed with Python 3.6 .8 along with the integration of Angular JS. To develop decentralized applications on Blockchain using Python. (i) Remix IDE: Remix is an open-source tools that not only lets you write your smart contracts but also supports testing, debugging as well as deployment of smart contracts. (ii) Web3.py: This is the tool that will allow us to talk to the smart contract and call its functions. The fundamental steps to be followed to create the blockchain network. They are

- define a concept of single block by inculcating the chaotic encryption schemes for hashing.
- define a proof of work system to develop the smart contract for mining the new blocks.
- create the framework using REST API to interact with the multiple nodes.

To interact with multiple nodes or users, REST API is used to create the framework, lightweight web application is configured by initializing the following attributes. They are i. apikey, domain, databaseURL, project ID, storage, sender ID, app ID, measurement ID as depicted in figure 2.

```
config = {
    apiKey":"AIzaSyBvhRrPSQo4Nvhh85N1AZWsAcFbDgTCd3A",
    "authDomain": "blockchain-282705.firebaseapp.com",
    "databaseURL": "https://blockchain-282705.firebaseio.com",
    "projectId": "blockchain-282705",
    "storageBucket": "blockchain-282705.appspot.com",
    "messagingSenderId": "785889741411",
    "appId": "1:785889741411: web:cd458830a9b8a2bd124656",
    "measurementId": "G-X8P4C4Q9ET"
     }
```

Figure 2. REST API Code to Configure the FLASK

Results and Analysis

Google Firebase authorizes the storage of user medical file uploads such as images, audios, videos etc. The Firebase SDK imparts a repository to clasp these files which can be collaborated among users. These files can also be available as private or public, by restricting or granting access to precise users in the medichain network. The propounded chaos medichain is micro-framework and it makes it easy to map endpoints to Python functions. It sanctions us talk to our blockchain over the web using HTTP requests. Figure. 3 depictions of launching a built-in server, which is good enough for testing. The server initiates with debugging mode and listens to the IPs to verify the authentic IP. The code is executed local server *http://127.0.0:8000.*

The figure. 4 depicts the input medical image which undergoes bi scroller chaotic high-level encryption to make the sensitive data more secured and exhibits high randomness. Before uploading to the decentralised network, it is necessary to encrypt the image to reach the exorbitant security [8]. The python Flask framework maps the endpoints and allows the decentralised network over the web using the HTTP request. The medical image encrypted was ready to mine inside the block on the decentralised network.

Figure 3. Launching the Server

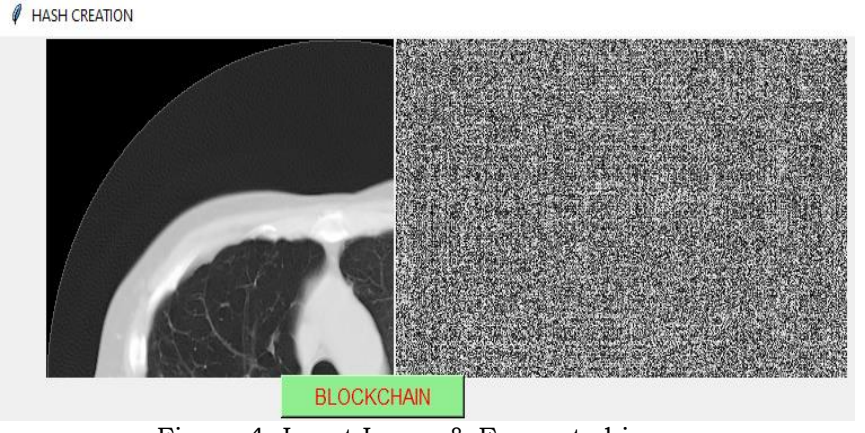

Figure 4. Input Image & Encrypted image

The figure.5 depicts the encrypted medical image is ready to mine in to a new block uploaded to the server. The mining of a new block on the server http://127.0.0:8000. The uploaded encrypted image was successfully mined in the decentralised network. The block which is mined is the address of the node.

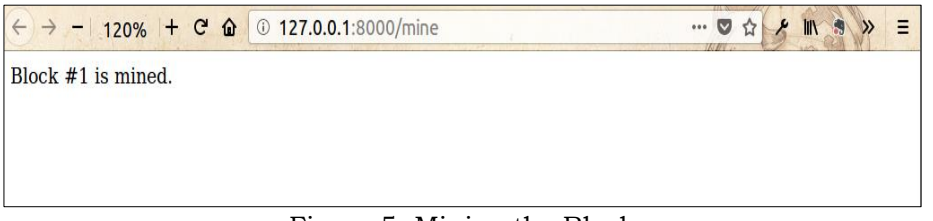

Figure 5. Mining the Block

The figure 6 (a), (b) depicts the installation of malware on a server, by injecting the server scripting code such as DDoS, Botnet, Ultradoser, DoS and the percentage of attack passed in to the network to identify the strength of the network.

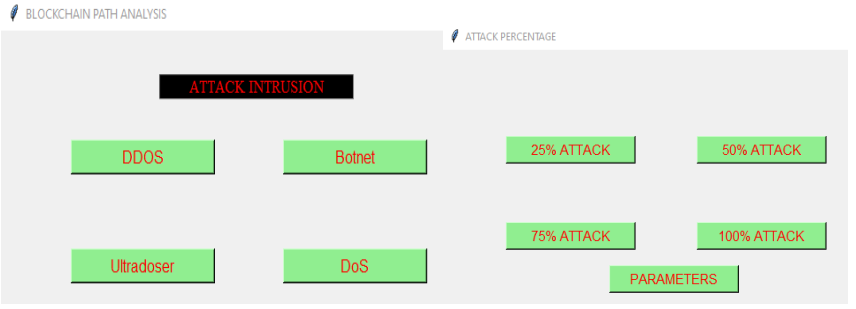

Figure 6 (a) Figure 6(b)

Figure 6 Installation of malware on a server and Percentage of attack

The figure.7 depicts the execution of injecting the DDoS attack codes to the server *http://127.0.0.0:8000* to check the strength of the network by calibrating the sensitivity, throughput, latency and computation time size.

Figure. 7 Injection of malicious DoS attack

Then the larger amount of DDoS injected packets generated by the malicious code in to the port of the server. It may lead to consumption of all services happens at the targeted network. It accomplishes the purpose by overloading the medichain server thereby clogging the network link and all memory resources will be accessed results in crashing the server.

Network Latency

Network latency is called as delay of sent the data from one node to another node, so lower the latency is the high-speed connectivity of interconnected nodes in the

network. The Network latency is calculated in milli seconds, the lower value near to zero gives more responsive connection. Latency is calculated by using the formula mentioned as Eqn. 1

Latency = Size of data/ Bandwidth used -- (1)

To analyze the latency, the attacks such as DDoS, DoS, Ultradoser and Botnet are injected to the propunded chaos based medichain. To assure the quality, the same set of attacks are passed to SHA [16], AES [17] encrypted based blockchain to share the medical data. It was observed in the figure 8 that the results of chaos medichain reveals that the latency was low at all 25%,50%,75%,100% level of the attacks passed to the chaos medichain network than AES, SHA encrypted blockchain

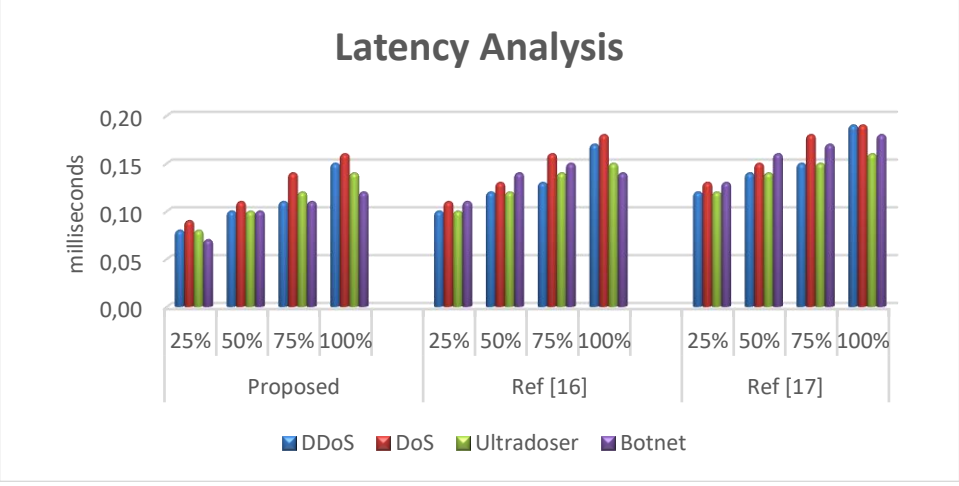

Figure 8: Comparison of latency analysis with other algorithms

At all levels of attack, SHA and AES shows 14% and 18% higher latency than the proposed chaos medichain. If lower the latency, the higher is connectivity and efficiency. The reduced latency of chaos medichain proves its efficiency.

Computational Time

Computational time is defined as amount of time, the defined architecture has to spend on processing the data that is sent by the user. Computational time is calculated using the Eqn.2

Computational time = Runtime --(2)

To analyze the computational time, the attacks such as DDoS, DoS, Ultradoser and Botnet are injected to the propunded chaos based medichain. To assure the quality, the same set of attacks are passed to SHA [16], AES [17] encrypted based blockchain to share the medical data The experimentation results are demonstrated in figure 9 as graph. The proposed architecture took 0.7 seconds to process the medical image even after the attack where else SHA [16] took 0.8 sec and DES [17] took 0.9 sec. For high-definition image it takes 0.5 sec to 0.7 sec to

process the data. Thus, the proposed architecture took 0.7 sec proves the better performance of processing the data in the the network.

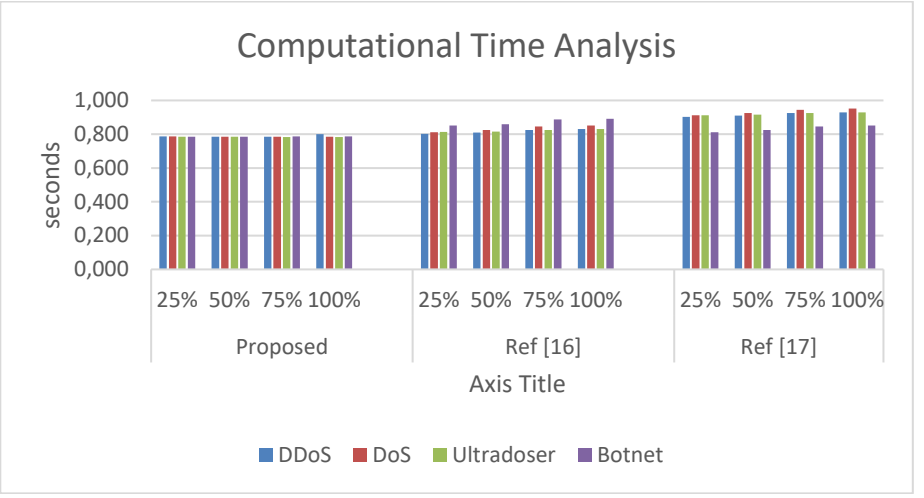

Figure. 9: Comparison of computational analysis with other algorithms

Sensitivity

Sensitivity analysis helps in prediction of the model, by analysing the fringes of uncertainties of one or more input variables. The sensitivity parameter helps to evaluate the robustness of the network. The performance parameter sensitivity is observed as near to the computational time proves the robustness of the system. The observation of the results in figure 10 reveals that the sensitivity value achieved by the proposed chaos medichain is 0.8 which is near to 0.7 sec of computation time of the proposed. The SHA [16] and DES [17] encrypted blockchain are also significantly produces the sensitivity value the nearby value results to the corresponding computation time. Thus, the result of the sensitivity analysis states that the system is robust at all levels of attacks.

The comprehensive experimentation results of network latency, sensitivity and computational time, reveals that behaviour of the decentralised network-based chaos in propounded architecture medichain is robust on various malicious attack. It prevents the attack and denies the access of sensitive data shared over the medichain.

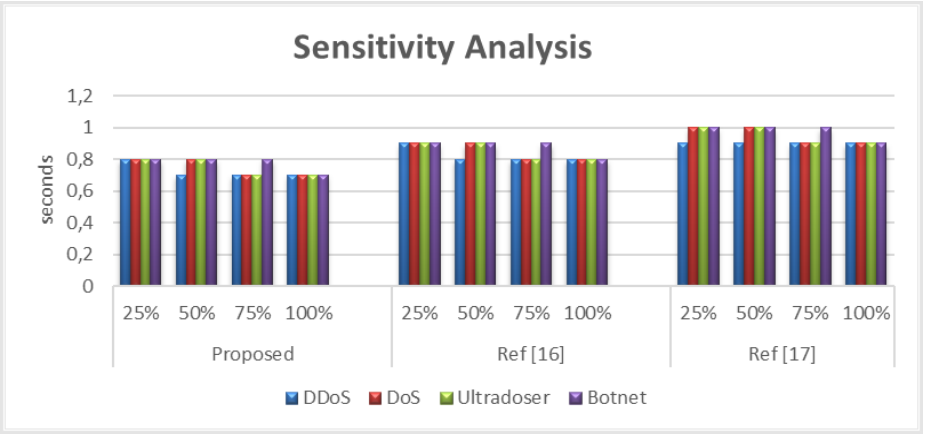

Figure.10 Comparison of sensitivity analysis with other algorithms

Conclusion

Testing the quality of the architecture is significant solution for shielding the medical data. The propounded architecture was tested by injecting the malicious codes of various attack to the server. The experimentation results reveal that the latency was low at 25%,50%,75%,100% level of the attacks passed to the chaos medichain network than AES, SHA encrypted blockchain. At all levels of attacks, the proposed shows 14% lower latency than SHA and 18 % lower than AES. On analysing the sensitivity and computational time, the propounded system was robust at all level of attacks than SHA and DES encryption based blockchain. Thus, the outcome of the experimentation yields the trust on proposed chaotic medichain network can deal with the medical sensitive data. In this paper the dependent parameters of the network only considered for experimentation and processing. Further the end-to-end framework will be contemplated for overall performance of the chaos medichain environment

References

1. B. Community, “The 51% attack,” October 2017. [Online]. Available: https learncryptography .com /cryptocurrency/51-attack
2. Y. Marcus , et al,“Low-resource eclipse attacks on ethereum’s peer-to-peer network,” IACR Cryptology ePrint Archive, vol. 2018, p. 236, 2018. [Online]. Available: http://eprint.iacr.org/2018/236
3. A. Azaria, et al, “Medrec: Using blockchain for medical data access and permission management,” in 2016 2nd International Conference on Open and Big Data (OBD), Aug 2016, pp. 25–30
4. Q. Xia, et al, “Medshare: Trustless medical data sharing among cloud service providers via blockchain,” IEEE Access, vol. 5, pp. 14 757–14 767, 2017
5. A. Greenberg, “Hacker redirects traffic from 19 internet providers to steal bitcoins,” Jun 2017. [Online]. Available: https://www.wired.com/ 2014/08/isp-bitcoin
6. M. Castro, et al, “Practical byzantine fault tolerance and proactive recovery,” ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 398– 461, 2002.

7. https://www.seba.swiss/research/are-blockchains -safe-how-to-attack-them-and-prevent-attacks.
8. R.Durga, et al," Generation of RAESSES Hash Function for Medical Blockchain Formation Based on High Dynamic Chaotic Systems". International Journal of Advanced Science and Technology, 2020,29(06), 8427-8440.
9. Saqib Hakak, et al" Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges",2020, Published in: IEEE Network
10. Khan, Prince W, et al, "A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things" ,2020, Entropy 22, no. 2: 175. doi.org/10.3390/e22020175
11. J. Indumathi et al., "Block Chain Based Internet of Medical Things for Uninterrupted, Ubiquitous, User-Friendly, Unflappable, Unblemished, Unlimited Health Care Services (BC IoMT U6 HCS)," 2020, IEEE Access, vol. 8, pp. 216856-216872, doi: 10.1109/ACCESS.2020.3040240
12. Choi, Y.J et al," Scalable and Secure Internet of Things Connectivity". Electronics 2019, 8, 752
13. H.Liu, et al, "Construction of a new 2D Chebyshev-Sine map and its application to color image encryption". Multimed Tools Appl 78, 15997–16010 (2019)
14. Xing yuan Wang ,et al , "A chaotic image encryption scheme based on cat map and MMT permutation", Modern Physics Letters B VOL. 33, NO. 27, https://doi.org/10.1142/S0217984919503263
15. Shenyong Xiao, et al "Design and Analysis of a Novel Chaos-Based Image Encryption Algorithm via Switch Control Mechanism", Security and Communication Networks, vol. 2020, Article ID 7913061, 12 pages, 2020.
16. B.Aruna, et al" Security Analysis on Block Chain using the Ecc and Sha Algorithms", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8, June 2019
17. P.Nivethini., et al," Data Security using Blockchain Technology", Special Issue Published in Int. Jnl. Of Advanced Networking & Applications (IJANA),2017 279-
18. Zhai, Sheping et al." Research on the Application of Cryptography on the Blockchain", 2020, Journal of Physics: Conference Series. 1168. 032077. 10.1088/1742-6596/1168/3/032077
19. Donia Fadhil Chalob, Amal Abdulbaqi Maryoosh, Zainab Mohammed Essa, Elaf Nassir abbud," A new block cipher for image encryption based on multi chaotic systems", TELKOMNIKA Telecommunication, Computing, Electronics and ControlVol. 18, No. 6, December 2020, pp. 2983~2991
20. S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. Guizani, "Securing smart cities through blockchain technology: Architecture, requirements, and challenges," IEEE Network, vol. 34, no. 1, pp. 8–14, 2020
21. G. Kothai, E. Poovammal, Gaurav Dhiman, Kadiyala Ramana, Ashutosh Sharma, Mohammed A. AlZain, Gurjot Singh Gaba, Mehedi Masud, "A New Hybrid Deep Learning Algorithm for Prediction of Wide Traffic Congestion in Smart Cities", Wireless Communications and Mobile Computing, vol. 2021, Article ID 5583874, 13 pages, 2021. https://doi.org/10.1155/2021/5583874

22. Alam, Tanweer. (2018) "A reliable framework for communication in internet of smart devices using IEEE 802.15.4." ARPN Journal of Engineering and Applied Sciences 13(10), 3378- 3387
23. Balasubramanian, Sowmiya & E., Poovammal. (2019). Blockchain Technology Is a Boost to Cyber Security. 10.4018/978-1-5225-8241-0.ch013.
24. Joan S. Muthu, P. Murali,A new chaotic map with large chaotic band for a secured image cryptosystem,Optik,Volume 242,2021,167300,ISSN 0030-4026,https://doi.org/10.1016/j.ijleo.2021.167300.
25. R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh and B. Yoon, "CES Blocks—A Novel Chaotic Encryption Schemes-Based Blockchain System for an IoT Environment," in IEEE Access, vol. 10, pp. 11354-11371, 2022, doi: 10.1109/ACCESS.2022.3144681.
26. Rinartha, K., & Suryasa, W. (2017). Comparative study for better result on query suggestion of article searching with MySQL pattern matching and Jaccard similarity. In *2017 5th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-4). IEEE.
27. Rinartha, K., Suryasa, W., & Kartika, L. G. S. (2018). Comparative Analysis of String Similarity on Dynamic Query Suggestions. In *2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)* (pp. 399-404). IEEE.
28. Susilo, C. B., Jayanto, I., & Kusumawaty, I. (2021). Understanding digital technology trends in healthcare and preventive strategy. *International Journal of Health & Medical Sciences*, *4*(3), 347-354. https://doi.org/10.31295/ijhms.v4n3.1769