sciendo

Journal of Smart Internet of Things (JSIoT)
VOL 2024, No.02 | 166-178 | 2024
DOI: 10.2478/jsiot-2024-0019

Article

ENHANCING BLOCKCHAIN FRAMEWORK USING WEB3.0 FOR IOT BASED PLANT DISEASE DETECTION SYSTEM

Jyoti B k [1], R. Nirmala [2], G. Gurumita [3]

[1] Department Electronics and Communication Engineering, Sir M Visvesvaraya College of Engineering, Raichur, India
[2] Department Electronics and Communication Engineering, St.Peter's Institute of Higher Education and Research
[3] Enterprise Solutions Team, Astrafinserv, Chennai, India

*Corresponding author: Jyoti B k (email: jyotiresearch2023@gmail.com)

Received 30 September 2024; Accepted 01 November 2024; Published 15 December 2024

Abstract: Plant diseases are considered as the major bottleneck for the farmers to monitor and diagnosis with the super intelligent methods. With the onset of Artificial Intelligence, Internet of Things(IoT) , predicting the plant diseases in early stages has given the bright light of hope to farmers for boosting the productivity of agriculture in which increases the country's economy. But the current advances in the IoT-AI-driven data gathers data from the agricultural fields and integrates the strong communication system for the early prediction and diagnosis process. Though these intelligent drive systems have several advantages, these procedure have been suffering from the varied security challenges which accelerates an outcry for a cognitive systems in the form of data breaches and privacy problems. The protection of patient data remains a significant concern due to the sensitivity and value of healthcare information, especially when transmitted over the Internet. This has heightened the demand for secure systems to safeguard against data breaches and privacy issues. Similarly, in agriculture, security challenges have been addressed using Web 3.0 and Blockchain technologies, which are favored for their immutable and decentralized features. This research proposes an advanced Web 3.0 Ensemble hybrid blockchain framework to enhance authentication security within the agricultural sector. To improve the authentication process further, chaotic maps are used to generate highly dynamic hashes during the creation of genesis blocks, ensuring that all data is securely stored in the recommended approach. The framework was tested on the Ethereum blockchain using Web 3.0, with Python 3.19 as the primary programming language for developing various interfaces. The security strength of the framework was thoroughly assessed using NIST standard tests, and its robustness was compared with other blockchain models. The results demonstrate that the proposed framework provides stronger defenses against various attacks and surpasses varied approaches in terms of complexity and robustness.

Keywords: Plant Diseases, Web3.0, Hybrid Chaotic keys, Ethereum,, NIST, Internet of Things, Artificial Intelligence

1. Introduction

Human race has revolved around the agriculture and even survived, developed and existed as the agriculture is the major source of their day to day food. Agriculture continues to be a key contributor to the GDP of nations, accounting for nearly 50% of employment in many countries [1]. Several factors, including climate change, the overuse of synthetic fertilizers, and a shortage of labor, have already impacted agricultural productivity worldwide and remain difficult to manage. Among these challenges, plant diseases are particularly detrimental, causing significant economic losses by damaging both food quality and crop yield [2].

Various methods and techniques are employed to diagnose plant diseases. While some farmers are fortunate enough to have access to labs and expert guidance, the majority cannot afford such resources to identify plant diseases early on and prevent their spread. Additionally, to diagnose a plant's illness, farmers often have to take samples to specific labs. The cost and resources required to establish these labs are not financially feasible, and those resources could be better allocated to other investments that would enhance crop yield [3]. To reduce such disease, the complex and cognitive agricultural ecosystems are required for continuous monitoring for an early prediction of such threats.[4]

As the use of these technologies expands, storing plant disease data presents significant security risks and privacy concerns. This underscores the need for a robust authentication system that not only defends against potential attacks but is also easily implementable within plant disease detection systems. While numerous authentication protocols exist to safeguard user data, many of them are cost-effective to deploy but fail to adequately protect against the increasing range of cyber threats[5-8].

1.1 Block Chain Technology For Plant Disease Detection Systems

To fix this limitations, blockchain technology [9-11] presents a promising solution to secure the storage of patient clinical data. It acts as a distributed ledger that meticulously records every transaction between users. It operates without a central authority, much like the systems used by banks [12-14]. Once information is entered into the ledger, it cannot be erased or altered, making it cryptographically robust and immutable. This technology relies on a consensus mechanism, where all nodes validate transactions before they are added to the ledger, ensuring uniform agreement on the data. As a result, blockchain offers a reliable solution to security concerns [15]. Due to its dynamic features, blockchain is increasingly adopted in the healthcare sector, particularly for the secure transmission of medical images. It has the potential to revolutionize healthcare systems by providing enhanced security across communication networks.

1.2 Motivation

Blockchain has emerged as a promising technology to ensure the security and privacy of agricultural data. However, it still faces several issues, like slow adoption [16], vulnerability to attacks [17], lack of intelligent security algorithms [18], poor robustness [19], and insufficient transparency [20]. These issues make residing secure architectures susceptible to various attacks, raising concerns about the security and trustworthiness of healthcare data stored in digital chains. To mention these concerns, this research proposes a secure and intelligent framework that integrates Web 3.0 with the blockchain framework. This integration is enhanced by hybrid chaotic encryption techniques for hashes, keys, and stored data, which facilitates secure information exchange. The

key contributions of this paper pursues:

a. The paper proposes the Web3.0 enabled Blockchain robust architecture for a securing and storing the plant disease data for the further analysis.
b. The paper reccommends integrating hybrid chaotic encryption techniques into blockchain technology to attain optimal security against various types of cyberattacks.
c. An optimized chaotic encryption approach for storing plant disease data is introduced, enhancing the blockchain's resilience while minimizing computational overhead, making it ideal for IoT-based ecosystems.
d. The recommended approach is deployed in Etherum blockchain using Influra and Ganache API which is then compared with the other existing blockchain architectures. Additionally, encryption strength of the proposed model is also analyzed and assessed with the varied state-of-art learning models. Experimentation outcomes clearly depicts that the recommended approach outperforms the other models.

The rest of the paper is structured as pursues: Section 2 clearly depicts the reviews from the different authors. The recommended approach is demonstrated in the Section-3. Section4 and Section-5 presents the implementation module, experimentation outcomes with the comparative analysis. Finally, the paper is concluded with the future scope in Section-6

2. Literature Review

Kuricheti et al. [21] proposed a classification system for turmeric leaf diseases. After preparation, the K-means method was utilized to conduct edge detection on the input image. After that, the GLCM technique was used to extract features, after which the SVM technique was trained to do the leaves categorization. Although this approach produces superior plant disease identification findings, it is unable to perform better on samples with large brightness variations.

Arguesoa et al. [22] developed a DL-based system for detecting and classifying fungal infection called Few-Shot Learning (FSL). To begin, the important points were calculated using the Inception V3 framework. The collected features were then fed into a multiclass support vector machine (SVM). This approach is resistant to crop disease categorization; nonetheless, the results are displayed on a short dataset and must be validated on a broad and diverse corpus. To localize and categorizes the tomatoes crop illness, Agarwal et al. [16] developed a CNN-based architecture. To extract the essential points from the input samples and categorizes them, this method used three convolutions and max-pooling layers. This technique has a higher accuracy in classifying tomato diseases, but it suffers from the problem of over-fitting over a small number of classes.

Richey et al. [23] introduced a method for identifying and categorizing maize crop diseases through a mobile application. This approach utilized a deep learning model called "ResNet50," which was trained on the ImageNet dataset, to calculate key deep points from the input images and organize them into different categories. While the technique provides a mobile-based solution for crop disease classification, it is resource-intensive, making it unsuitable for smartphones due to limitations in memory, processing power, and battery life. In contrast, Zhang et al. developed a novel deep learning classification system for identifying tomato crop diseases. They proposed a custom Faster-RCNN model that leveraged a deep residual network for automatic feature extraction, instead of using the VGG16 model. Additionally, the edge pixels were clustered using the k-means method. Although this approach delivers more accurate disease diagnosis for tomato crops, it comes with higher costs.

Batool et al. [24] proposed an approach for the early identification and categorization of tomato leaf diseases. In the initial phase, the "AlexNet" approach was employed to extract deep feature points from the input images, which were subsequently used to train a "KNN" classifier to

distinguish between healthy and diseased leaves. While this method enhances the prediction accuracy, KNN remains a relatively slow and resource-intensive technique. A deep learning-based method for detecting tomato leaf diseases was presented by Karthik et al. In this approach, deep features from the input images were extracted using a residual network, and a CNN model was then trained to classify the leaves as either healthy or affected. This method has a higher accuracy in classifying leaf diseases, but it is inefficient in terms of cost.

Turkoglu et al. proposed an ensemble approach where the deep keypoints of various plant species were extracted using several deep learning models, such as “AlexNet, GoogleNet, DenseNet201, ResNet50, and ResNet101” architectures [25]. These extracted features were subsequently employed for training a support vector machine (SVM) to classify different plant diseases. Despite offering enhanced accuracy in plant leaf classification, this method comes at the cost of higher computational overhead for feature extraction.

In [26], Shradha Verma et al. investigated the use of capsule networks for identifying disinfected plants. The authors employed the conventional capsule network, which proves to be highly effective in agriculture by accurately capturing attributes like "texture, orientation, and pose," outperforming traditional deep learning models. The capsule network's structure groups related features into capsules, forming a cohesive network. While the capsule network demonstrated improved accuracy over CNN models, its performance was not validated using segmented or real-time datasets.

Loise Wanjiru et al. explored the use of capsule networks for plant disease classification in [27]. They proposed a novel model that combined CapsNet with a support vector machine (CapsNet-SVM) for classifying tomato leaf diseases. In this approach, the SVM served as a reliable classifier, while the capsule network was fine-tuned for feature extraction. The results demonstrated that the CapsNet-SVM model could independently extract features from raw images and perform the final classification effectively.

Gökhan et al. introduced a novel approach using the "CapsNET architecture" to assess its effectiveness in detecting plant leaf diseases. These diseases are prevalent and pose significant threats to agricultural productivity. The CapsNET model offers the ability to perform detailed analysis, even identifying subtle blemishes that could influence the timing and duration of seed dressing. The proposed "CapsNET" system aimed to explore various feature learning strategies for bell pepper plants and enhance the learning potential of deep learning models. The CapsNET was trained using images of both healthy and diseased leaves [28].

In their study, Patrick Mensah et al. [29] suggest employing a combination of Gabor filters and Capsule Networks to identify blurred, distorted, and previously unobserved images of tomato and citrus diseases. The Gabor layer is incorporated as a convolutional layer, with the filters specifically designed to adhere to the Gabor function. This approach introduces significantly more complexity to the architecture when compared to a traditional CNN model.

To the best of our understanding, blockchain-based plant disease detection systems, which are designed to address multiple security threats while maintaining low computational costs, continue to pose a significant challenge for researchers.

3. Proposed Methodology

The recommended approach uses varied modules and systems to manage the block enabled security systems. In Figure 1, the recommended approach depicts the four components such as Image processing and Acquisition Module(IPAM), Encryption Process(EP) and Integration Phase(IP).

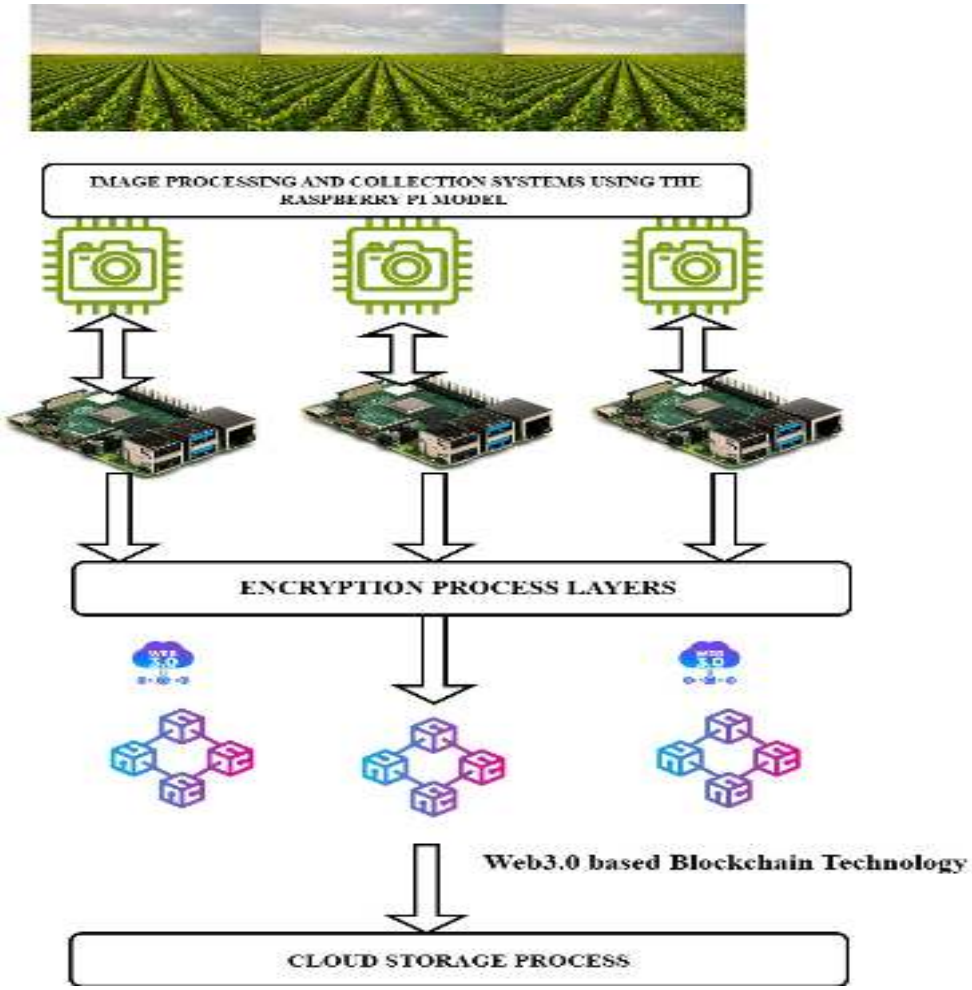


Figure 1: Web.3.0- Block Chain Frameworks for Secured Plant Disease Detection

3.1 Image Processing And Acquisition Process

In our proposed study, we introduce an innovative methodology that integrates plant image analysis and data collection through image sensors, providing a fresh perspective on this domain. Raspberry Pi Model B+ is used as the major CPU for collecting the plant diseases from the agricultural fields. These systems runs the encryption engine for encrypting the plant diseases and leverages Blockchain technology can be employed to guarantee an unalterable and clear record of each transaction and data point recorded throughout the agricultural workflow. This ensures transparency and security in the entire process. Figure 2 presents the sample plant diseases captured from the Image Acquisition Systems.

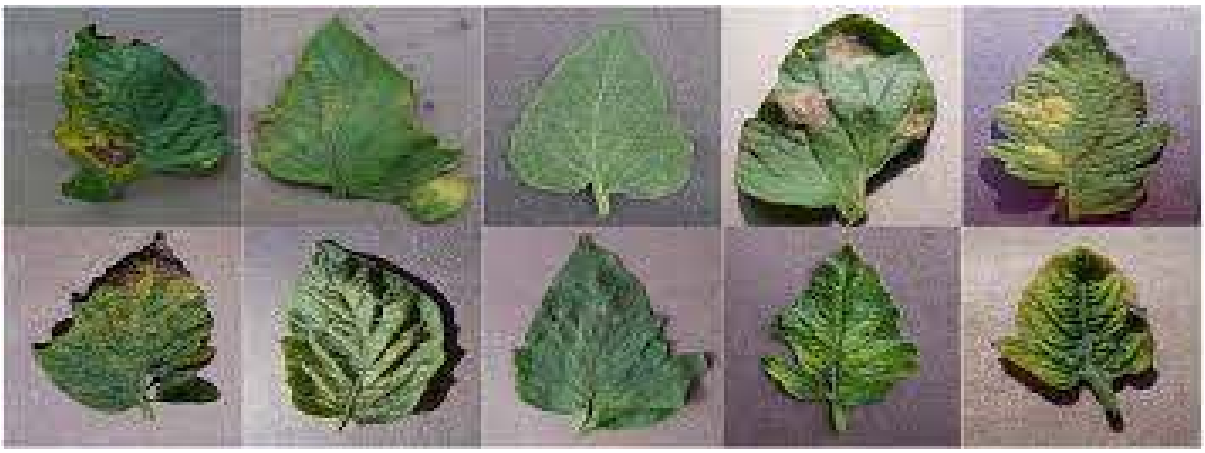


Figure 2: Sample Plant Disease Captured from the Image Acquisition Systems

3.2 Image Encryption Process

For securing the plant disease images, Scroll based Advanced Encryption (SBES) System has been proposed in which scroll attractors are used to encrypt the images which is then stored in the Blockchain for further processing. The proposed model overcomes all the drawbacks of traditional authentication systems which are then defined for the IoT based imaging system

3.2.1 Multi-Scroll Chaotic Attractors:

Dynamical systems that exhibit multiscroll attractors can display more intricate behaviours. Chaotic system is expressed as follows.

$$\dot{x}_1 = -ax_1 + bx_2x_3 \quad (1)$$
$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \quad (2)$$
$$\dot{x}_3 = ex_3 - fx_1x_2 \quad (3)$$
$$\dot{x}_1 = -ax_1 + bx_2x_3 \quad (4)$$
$$\dot{x}_2 = -cx_2^3 + dx_1x_3 \quad (5)$$
$$\dot{x}_3 = ex_3 - fx_1x_2 + p_1\, tanh(x_2 + g) \quad (6)$$

Chaotic attractor is obtained when $a = 2$, $b = 6$, $c = 6$, $d = 3$, $e = 3$, $f = 1$, $p_1 = 1$, $g = 2$and the chosen initial conditions are $[x_1(0), x_2(0), x_3(0)] = [0.1, 0.1, 0.6]$.

3.2.2 Advantages of Multi-Scroll attractors

The following pros of the recommended scroll attractors utilized for encryption is mentioned below

This system requires less memory to generate the same number of scrolls, as it uses fewer components for the generation process [30-32s]. This makes it more suitable for IoT-based data collection systems.

Random scrolls can be produced by altering any component in any direction.

The randomness of scroll maps is not dependent on the number of scrolls, unlike other methods where randomness is closely tied to the initial values.

3.3 Encryption Process

To simplify the use of matrices in encryption techniques, inter –pixels of the images are encrypted by the scroll based encryption process. The intermediate outputs are then used to encrypt

the intra-pixels of the plant images. The permutations and diffusion process has been employed to obtain the high secured encrypted images. Algorithm -1 presents the complete encryption cycle for the plant disease images.

Steps	Algorithm-1 // Encryption Process Involved For the Complete Images
1	Input : Plant Images
2	Output : Encrypted Images
3	While n=1 to Max_iterations
4	X= Scrolls_Maps Creation using Equation(1),(2) and(3)
5	Rescale the X into 256
6	Y1= X Permutated I1// Intermediate Key Generation Process
7	Y2 =Y1 Permutated I2// Intermediate Encrypted Results
8	Y3= Y1 ^ Y2
9	End

As mentioned in Algorithm-1, two intermediate process of key generation is adopted which the scroll maps are formed to form the keys using the inter-pixels(I1) and Intra-pixels(I2) . These two secured keys are permutated to form the encrypted images which are then used to store in the Blockchain layers using Web3.0 techniques.

3.4 Block Chain Technology

For implementing in an IoT System, Etherum BlockChain technology is implemented. A node can initiate a transaction, which serves as the fundamental unit within the blockchain. These operations are bundled to form a block, which is then appended to the blockchain after being validated by miners or endorsing nodes. Various sets of protocols are defined by the system administrator to manage blockchain activities.

In this system, administrator can configure the endorser and non-endorser peers. Since the IoT devices are battery powered and requires the larger power to run the mining algorithms, internal IoT nodes act as the validator nodes. A node or peer significant place in processing transaction and it sustains in the replica of a blockchain.

A new structure has been designed to direct the encrypted image transactions among users and servers/clouds. After receiving certification from the miner, an ethical transaction is generated. The transaction's input consists of chaotic encrypted image features, while the output provides a fixed IP address, facilitating the image download process. This proposed transaction structure has three layers: the retrieval layer, transaction layer, and timestamp layer. The User ID is a unique identifier for each user, which is utilized for uploading encrypted images. The original image URL is provided to improve the searchability and downloadability based on the query result. Lastly, the Image Label describes the device type and uses chaotic hashes to represent the unique hash of the image.

3.5 Web3.0 Technology

Web3.0, built on decentralized control, offers immutability, enhanced security, and robust query capabilities, along with integrated asset management. It is primarily devised for machine-to-machine communication and outperforms traditional web technologies (Web2.0) in managing

blockchain networks. Interfaces for Web3.0 can be developed using programming languages like Java, Python, and JavaScript. These transactions are executed within a real-time database. The first type, the CREATE transaction, allows users to establish new records in the database. The second, SEND transaction, enables the transfer of record ownership to another user within the blockchain ecosystem. Infura API is utilized to connect IoT devices to the blockchain.

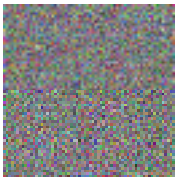
4. Results and Discussions

This section discusses about the implementation process, results discussion and comparative analysis in the performance of the recommended approach and its performance is assessed with the state-of-art learning algorithms

4.1 Implementation Details

The recommended approach was created using Web3.0 Python libraries, enabling its evaluation within an Ethereum blockchain setting. Distributed applications were developed, and Infura APIs were utilized to establish a connection with the Ethereum network. The diagram below shows the deployment phase of the proposed framework.

4.2 Encrypted Results of Plant Images

Sl.No	Input Images	Encrypted Images
1		
2		
3		

4.3 Performance Evaluation

The performance assessment of the recommended framework is utilized by analyzing the security robustness of the keys and performing a computational analysis of the Blockchain implementation. A comprehensive examination of the recommended approach is presented below

4.3.1 Randomness of the Keys

To evaluate the randomness of the output bits, the National Institute of Standards and Technology (NIST) test suite was employed. All test outcomes met the NIST standards, demonstrating the robustness of the randomness and ensuring high security capable of preventing breaches. Table 1 illustrates the comprehensive NIST evaluation results of the proposed approach. As mentioned in [36], and to highlight the algorithm's strong resistance to numerous threats, the randomness value P is computed as pursues.

$$(P) > 0.01 \quad \text{for 'n' iterations} \tag{12}$$

The randomness values are roughly assessed according to Equation (12), and the keys produced at each stage are examined based on the previously mentioned criteria. The generated keys meet all the NIST standard tests, as they comply with the conditions outlined in Equation (12). As can be seem , proposed keys has sustain the much defensive nature against the multiple attacks.

Table 1: NIST Performance of the Recommended Key generation

Sl.No	NIST Test Specification	Status of test
1	DFT Test	PASS
2	RunTest	PASS
3	Long Run Test	PASS
4	Frequency Test	PASS
5	Block Frequency Test	PASS
6	Frequency MonoTest	PASS
7	Matrix Rank Test	PASS
8	Lempel-ZIV Compression Test	PASS
9	Random Excursion Test	PASS
10	Universal Statistical Test	PASS

The performance analysis of the recommended approach focuses on evaluating the computational cost infused with signing and verifying operations as the number of transactions expands. The analysis is represented graphically in Figure 3. Results shows that the latency linearly increases as the number of transaction increases.

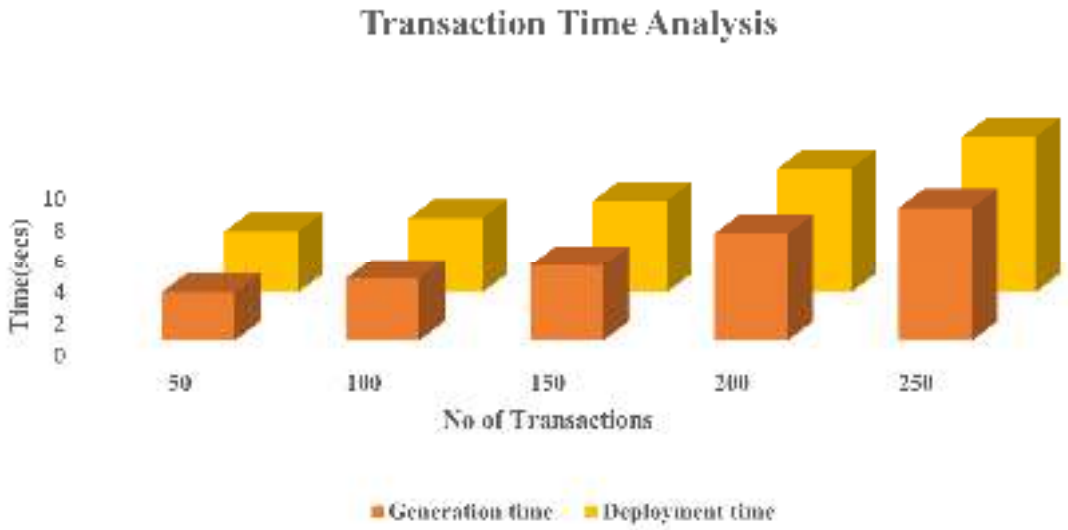


Figure 3: Transaction Time Analysis for the Recommended approach

4.4 Comparative Analysis :

To prove the supremacy of the recommended model, approaches in [33-36] are used for experimentation. Figure 3 shows the comparative analysis among the proposed blockchain framework with the varying transactions. From the figure 4 and 5, it is evident that the recommended approach shown the less latency examined with varied residing approaches.

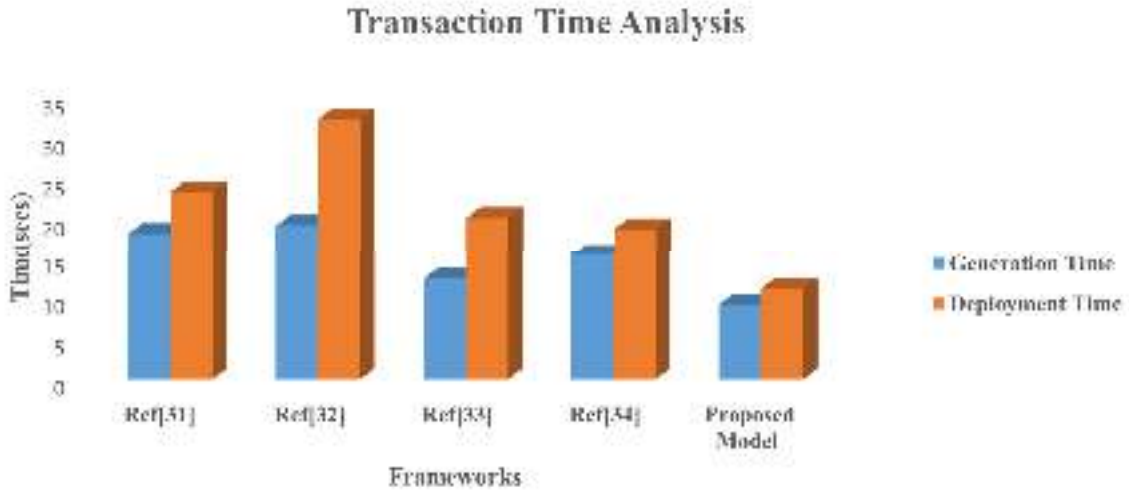


Figure 4: Analysis Average of 100 Transactions with residing approaches.

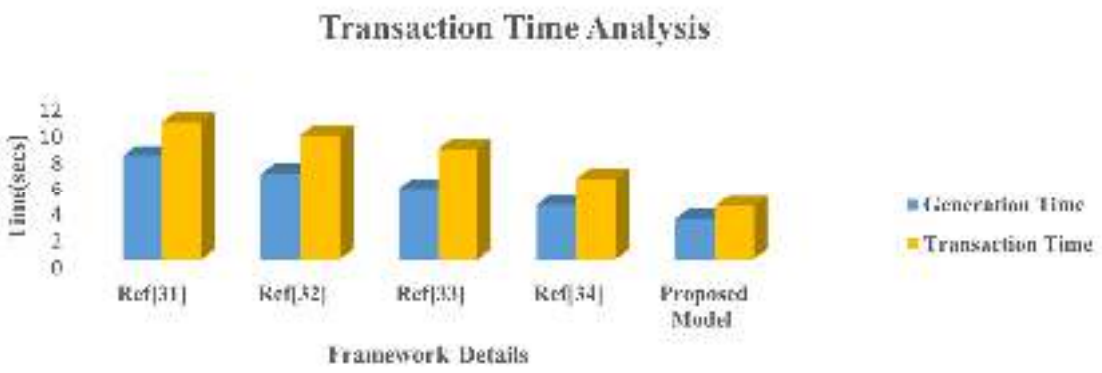


Figure 5: Analysis Average of 200 Transactions with residing approaches.

5. Conclusion

Agriculture is considered as one of the hot fields after the infusion of advanced and disruptive technologies like IoT and AI. But the adoption of these technologies in residing health care systems leads to several issues like data breaches, privacy and non-ethical hacking of plant data. Current systems also suffers vulnerable to new breeches that have been put to mitigate against the new born multiple attacks. To solve the issue, this study introduces a secure mutual authentication framework for plant image transmission, leveraging blockchain technology and a hybrid of lightweight chaotic protocols. To begin, Web 3.0 interfaces are utilized for the storage of patient health records. Secondly, proposed blockchain enabled architectures used Infura API to prevent the data from the several challenges that are prevalent in existing systems. Finally the mutual authentication protocol based Choatic double encryption principles for data security and privacy preserving mechanism. The extensive experimentation is carried out using NIST and it is deployed in Etherum Blockchain. To prove its light weight and efficiency, performance of the recommended approach is examined with the other techniques. Results demonstrates that recommended approach has outperformed the varied residing approaches in terms of security and time complexity. Moreover, the recommended method can be further enhanced by incorporating a DL-based encryption technique to bolster security against emerging threats.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Koosha Mohammad Hossein, et al., BCHealth: a novel blockchain-based privacy-preserving architecture for IoT healthcare applications, Comput. Commun, vol. 180, pp. 31-47 (2021).

[2] Aparna Kumari, et al., Fog computing for Healthcare 4.0 environment: opportunities and challenges, Comput. Electr. Eng. 72 (2018) 1–13.

[3] Alexander McLeod, Diane Dolezel, Cyber-analytics: modeling factors associated with healthcare data breaches, Decis. Support Syst. 108 (2018) 57–68.

[4] Hussien, Mansur Hassan, et al., Blockchain technology in the healthcare industry: trends and opportunities, J. Ind. Inf. Integrat. 22 (2021), 100217.

[5] B. Shickel, P.J. Tighe, A. Bihorac, P. Rashidi, Deep EHR: a survey of recent advances in deep learning techniques for electronic health record (EHR) analysis, in: IEEE Journal of Biomedical and Health Informatics,

vol. 22, Sept. 2018, pp. 1589–1604, https://doi.org/10.1109/JBHI.2017.2767063, 5.
[6] Z. Ying, L. Wei, Q. Li, X. Liu, J. Cui, A lightweight policy preserving EHR sharing scheme in the cloud, in: IEEE Access, vol. 6, 2018, pp. 53698–53708, https:// doi.org/10.1109/ACCESS.2018.2871170.
[7] X. Yang, T. Li, W. Xi, A. Chen, C. Wang, A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRs sharing in the cloud, IEEE Access 8 (2020) 170713–170731, https://doi.org/10.1109/ACCESS.2020.3025060.
[8] Y. Wang, A. Zhang, P. Zhang, H. Wang, Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain, in: IEEE Access, vol. 7, 2019, pp. 136704–136719, https://doi.org/10.1109/ACCESS.2019.2943153.
[9] Y. Zhuang, L.R. Sheets, Y.-W. Chen, Z.-Y. Shae, J.J.P. Tsai, C.-R. Shyu, A patientcentric health information exchange framework using blockchain technology, IEEE J. Biomed. Health Inf.cs 24 (8) (Aug. 2020) 2169–2176, https://doi.org/ 10.1109/JBHI.2020.2993072.
[10] Y. Yang, et al., Medshare: a novel hybrid cloud for medical resource sharing among autonomous healthcare providers, IEEE Access 6 (2018) 46949–46961, https:// doi.org/10.1109/ACCESS.2018.2865535.
[11] F. Deng, Y. Wang, L. Peng, H. Xiong, J. Geng, Z. Qin, Ciphertext-policy attributebased signcryption with verifiable outsourced designcryption for sharing personal health records, in: IEEE Access, vol. 6, 2018, pp. 39473–39486, https://doi.org/ 10.1109/ACCESS.2018.2843778.
[12] Z. Wu, Group-oriented cryptosystem for personal health records exchange and sharing, in: IEEE Access, vol. 7, 2019, pp. 146495–146505, https://doi.org/ 10.1109/ACCESS.2019.2946266.
[13] L. Ismail, H. Materwala, S. Zeadally, Lightweight blockchain for healthcare, in: IEEE Access, vol. 7, 2019, pp. 149935–149951, https://doi.org/10.1109/ ACCESS.2019.2947613.
[14] A. Shahnaz, U. Qamar, A. Khalid, Using blockchain for electronic health records, in: IEEE Access, vol. 7, 2019, pp. 147782–147795.
[15] Yogesh Sharma, B. Balamurugan, Preserving the privacy of electronic health records using blockchain, Proc. Comput. Sci. 173 (2020) 171–180, https://doi.org/ 10.1016/j.procs.2020.06.021. ISSN 1877-0509.
[16] C. Pirtle, J. Ehrenfeld, Blockchain for healthcare: the next generation of medical records? J. Med. Syst. 42 (2018) 172, https://doi.org/10.1007/s10916-018-1025- 3.
[17] Sara Saberi, Mahtab Kouhizadeh, Joseph Sarkis, Lejia Shen, Blockchain technology and its relationships to sustainable supply chain management, Int. J. Prod. Res. 57 (7) (2019) 2117–2135, https://doi.org/10.1080/00207543.2018.1533261.
[18] P. Treleaven, R. Gendal Brown, D. Yang, Blockchain technology in finance, in: Computer, vol. 50, 2017, pp. 14–17, https://doi.org/10.1109/MC.2017.3571047, 9.
[19] Sudeep Tanwar, Karan Parekh, Richard Evans, Blockchain-based electronic healthcare record system for health
[20] E. Daraghmi, Y. Daraghmi, S. Yuan, MedChain: a design of blockchain-based system for medical records access and permissions management, in: IEEE Access, vol. 7, 2019, pp. 164595–164613, https://doi.org/10.1109/ACCESS.2019.2952942.
[21] N. Samwel, L. Batina, Practical Fault injection on deterministic signatures: the case of EdDSA, Prog. Cryptol.–AFRICACRYPT 2018 Lecture Notes in Comp. Sci. (2018) 306–321.
[22] Kondapally Ashritha, Lakshmy KV& Sindu.M, "Redactable Blockchain using Enhanced Chameleon Hash Function," IEEE -International Conference on Advanced Computing & Communication Systems, pp. 323-328, 2019.
[23] Meng Shen, Nadra Guizani, Yawen Deng, Xiaojiang Du, Liehuang Zhu,"Privacy-Preserving Image Retrieval for Medical IoT Systems: A Blockchain-Based Approach," IEEE Network, Vol.33, No.5, 2019.
[24] Huanrong Tang, Jianquan Ouyang & Ning Ton, "Medical Images Sharing System based on Blockchain and Smart Contract of Credit Scores," IEEE International Conference on Hot Information-Centric Networking,pp. 240-241, 2018
[25] Matzutt Roman, Ziefle Martina, Müllmann Dirk, ZeissigEva-Maria, Horst Christiane, Kasugai Kai, Lidynia Sean, Wieninger Simon, Ziegeldorf Jan Henrik, Gudergan Gerhard, gen. Döhmann Indra Spiecker, Wehrle Klaus,''MyneData: Towards a trusted and user-controlled ecosystem for sharing personaldata,'' inProc.GesellschaftFürInformatik, pp.1073, 2017.
[26] Zhen Cheng, Runhuai Li, Xinrui Hou, Yajin Zhou, Jinku Li, Xiapu Luo, Kui Ren ''Towards a first step to understand the crypto currency stealing attack on ethereum,'' International Symposium on Research in Attacks, Intrusions and Defenses, pp. 47–60, 2019.
[27] Huru Hasanova, Mu-gon Shin, Myung-Sup Kim, Kyunghee Cho, Ui-jun Baek, ''Asurveyon block chain cybersecurity vulnerabilities and possible countermeasures,'' International Journal Network Management, Vol. 29, No. 2, 2019.

[28] Pratima Sharma, et al., Blockchain-based IoT architecture to secure healthcare system using identity-based encryption, Expet Syst. 39 (10) (2022) e12915. Vol no is not available
[29] Suchi Kumari, et al., Intelligent deception techniques against adversarial attack on the industrial system, Int. J. Intell. Syst. 36 (5) (2021) 2412–2437.
[30] Pratima Sharma, et al., Blockchain-based privacy preservation for IoT-enabled healthcare system, ACM Trans. Sens. Netw. 19 (3) (2023) 1–17.
[31] Raghubir Singh, et al., Edge AI: a survey, Internet of Things and Cyber-Phy. Sys. 3 (2023)
[32] 8. Chi, T.; Qin, B.; Zheng, D. An Efficient Searchable Public-Key Authenticated Encryption for Cloud-Assisted Medical Internet of Things. Wirel. Commun. Mob. Comput. 2020, 2020, 8816172:1–8816172:11
[33] Liang Qiao, Zhihan Lv, A blockchain-based decentralized collaborative learning model for reliable energy digital twins, Internet of Things and Cyber-Phy. Sys. 3 (2023) 45–51.
[34] Kai Fan, Qi Luo, Kuan Zhang, Yintang Yang, “Cloud-based lightweight secure RFID mutual authentication protocol in IoT,” Information Sciences, vol. 527, pp. 329-340, 2020.
[35] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi and N. Kumar, "BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications," in IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1242-1255, 1 April-June 2021, doi: 10.1109/TNSE.2019.2961932.
[36] B. D. Deebak et al., "A Lightweight Blockchain-Based Remote Mutual Authentication for AI-Empowered IoT Sustainable Computing Systems," in IEEE Internet of Things Journal, vol. 10, no. 8, pp. 6652-6660, 15 April15, 2023, doi: 10.1109/JIOT.2022.3152546.