Secure and Scalable Data Management in Medical Systems via Decentralized Privacy Framework

C Lakshmi Devi [1],R R Shantha Spandana[2] , G Swapna [3], G Viswanath[4]

[1] P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: lakshmidevi200302@gmail.com , ORCID-ID: 0009-0004-5139-131X

[2]Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: shanthaspandana@gmail.com , ORCID-ID: 0009-0003-4236-1250

[3] Assistant Professor, Apollo institute of pharmaceutical sciences, The Apollo University, Chittoor, India.

E-mail: swapnagv111@gmail.com, ORCID-ID: 0000-0002-9340-4148

[4] Associate Professor, Dept. of AI & ML, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, Email: viswag111@gmail.com, ORCID-ID: 0009-0001-7822-4739

Area/Section: Engineering with Medical Background
Type of the Paper: Regular Paper
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed in: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.15487830
Google Scholar Citation: IJHSP

How to Cite this Paper:

C Lakshmi Devi, Shantha Spandana, R. R., Swapna, G. & Viswanath, G.(2025). Secure and Scalable Data Management in Medical Systems via Decentralized Privacy Framework. *International Journal of Health Sciences and Pharmacy (IJHSP), 9*(1), 126-139. DOI: https://doi.org/10.5281/zenodo.15487830

International Journal of Health Sciences and Pharmacy (IJHSP)
A Refereed International Journal of Srinivas University, India.

Crossref DOI: https://doi.org/10.47992/IJHSP.2581.6411.0137

Received on: 16/04/2025
Published on: 22/05/2025

© With Author.

This work is licensed under a Creative Commons Attribution-Non-Commercial 4.0 International License subject to proper citation to the publication source of the work.

Disclaimer: The scholarly papers as reviewed and published by Srinivas Publications (S.P.), India are the views and opinions of their respective authors and are not the views or opinions of the SP. The SP disclaims of any harm or loss caused due to the published content to any party.

Secure and Scalable Data Management in Medical Systems via Decentralized Privacy Framework

C Lakshmi Devi [1],R R Shantha Spandana[2] , G Swapna [3], G Viswanath[4]

[1] P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,
Email: lakshmidevi200302@gmail.com , ORCID-ID: 0009-0004-5139-131X

[2]Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,
Email: shanthaspandana@gmail.com , ORCID-ID: 0009-0003-4236-1250

[3] Assistant Professor, Apollo institute of pharmaceutical sciences, The Apollo University, Chittoor, India.
E-mail: swapnagv111@gmail.com, ORCID-ID: 0000-0002-9340-4148

[4] Associate Professor, Dept. of AI & ML, Sri Venkatesa Perumal College of Engineering & Technology, Puttur,
Email: viswag111@gmail.com, ORCID-ID: 0009-0001-7822-4739

ABSTRACT

This project provides a Cloud-Assisted Decentralized privacy-preserving Framework (CA-DPPF) that amalgamates cloud computing, blockchain generation, and IPFS to tackle the complexities of securely and efficaciously storing sensitive healthcare data. The framework utilizes ECDSA digital signatures and RSA encryption to assure strong person authentication and statistics safety, in accordance with present day developments in safeguarding healthcare information. IPFS is applied for scalable storage solutions, addressing the limitations of traditional centralized cloud services, as indicated in previous research. Blockchain era augments the system through supplying immutable document-preserving, mitigating the weaknesses of centralized systems. A rankings module is incorporated to guarantee the legitimacy of healthcare feedback, allowing people to assess doctors, with these checks securely documented on the blockchain to prevent manipulation. smart contracts, created in Solidity, enable secure transactions and govern user data at the Ethereum blockchain, making certain transparency and integrity in all interactions. The studies gives a spread that integrates the CHACHA20 encryption algorithm, strengthening computational efficiency and safety while complementing present encryption methods and improving usual system overall performance.

Keywords: Interplanetary File System (IPFS), ECDSA Digital Signatures, RSA Encryption, CHACHA20 Encryption, Decentralized Storage, Patient Data Privacy, Healthcare Data Management.

1. INTRODUCTION:

The healthcare zone encounters great limitations in safeguarding the security, privacy, and effective management of affected person statistics, which can be critical for offering high-qualitycare. As healthcare structures regularly depend on virtual facts, safeguarding sensitive statistics from unauthorized access and breaches has emerged as a essential trouble. Blockchain technology provides a feasible answer to those troubles, presenting a decentralized, transparent, and immutable method for the garage and management of healthcare data. Its capability to assure records integrity and safety renders it particularly suitable for healthcare applications, where the preservation of patient report confidentiality and accuracy is paramount [1], [2].

This venture seeks to amalgamate blockchain generation with cloud computing to merge the computational skills and garage scalability of cloud offerings with the privateness and protection attributes of a decentralized blockchain framework. The initiative utilizes blockchain's immutable ledger to guarantee the safety of healthcare information towards alteration or unauthorized get right of entry to. The framework prioritizes patient privacy via using sophisticated cryptographic strategies, along with RSA encryption and ECDSA virtual signatures, which assure that best legal individuals can get right of entry to important facts even as permitting patients to keep control over their records [5], [6]. The amalgamation of cloud offerings and blockchain improves the efficiency and accessibility of healthcare information control at the same time as simultaneously addressing the urgent requirement for secure and personal patient information sharing in current networked healthcare settings [4], [16].

2. OBJECTIVES:

(1) This project aims to create a Cloud-Assisted Decentralized Privacy-Preserving Framework (CA-DPPF) by integrating cloud computing, blockchain, and IPFS. The goal is to provide secure, scalable, and efficient storage for sensitive healthcare data. It addresses the challenges of centralized storage by enabling decentralized data control and distribution.
(2) The framework incorporates ECDSA digital signatures and RSA encryption to ensure secure user authentication and data protection. These cryptographic methods safeguard healthcare information against unauthorized access or tampering. The system aligns with current advancements in healthcare data privacy and security compliance.
(3) A blockchain-based feedback ranking system is implemented to enhance trust and transparency in healthcare services. Patients can securely rate doctors, and all reviews are permanently stored on the blockchain. This prevents data manipulation and promotes integrity in user-generated healthcare feedback.
(4) The CHACHA20 encryption algorithm is integrated to boost performance and security within the system. It enhances computational efficiency compared to traditional algorithms, ensuring faster operations. This strengthens the execution of smart contracts and overall security on the Ethereum blockchain.

3. REVIEW OF LITERATURE/ RELATED WORKS:

The incorporation of blockchain generation in healthcare has been considerably tested to tackle safety, privateness, and statistics management troubles. Omar et al. [1] examined the software of blockchain smart contracts for automating procurement contracts in healthcare, emphasizing the advantages of decentralized, at ease, and transparent systems. Ray et al. [22] investigated the software of blockchain in IoT-based healthcare, emphasizing consensus platforms and realistic implementations that assure cozy data sharing and patient confidentiality. Tanwar et al. [5] provided a blockchain-primarily based electronic healthcare record (EHR) system, highlighting the necessity for at ease statistics management in Healthcare 4.0 applications. Blockchain has been utilized to thwart the infiltration of counterfeit prescription drugs, as confirmed by Pandey and Litoriya [3], who proposed a blockchain-primarily based framework to shield e-fitness networks.

IPFS has garnered interest as a decentralized opportunity for scalable facts storage. Borgia [11] emphasized the problems and opportunities supplied by way of the net of things (IoT) in healthcare, highlighting the need for effective facts storage solutions, with IPFS turning into as a viable alternative. Nagasubramanian et al. [24] employed blockchain era to comfortable e-health records inside the cloud, which corresponds with the proposed system's technique of utilizing blockchain to assure records integrity and transparency.

Numerous studies have examined the software of sophisticated cryptographic strategies, such as RSA and ECDSA digital signatures. Khalid et al. [18] brought a decentralized authentication approach for IoT systems, utilizing cryptography to strengthen security, pertinent to the proposed system's emphasis on safeguarding touchy healthcare records.

Grover [7] has investigated the combination of doctor rating systems on blockchain, specializing in its software for safeguarding facts in car networks and other decentralized systems. Such systems guarantee facts integrity, which is important for keeping the legitimacy of patient feedback in healthcare environments.

Those research together establish a foundation for the proposed device, illustrating the potential of integrating blockchain, IPFS, and cryptography to enhance protection, privacy, and efficiency in healthcare records control.

Table 1: Comparison Table for Related Work

Sl. No	Area & Focus of the Research	The result of the Research	Reference
1	Automating procurement contracts in the healthcare supply chain using blockchain smart contracts	Improved transparency and automation in healthcare procurement through blockchain-enabled smart contracts.	I. A. Omar et al., IEEE Access (2021) [1]
2	Securing e-health networks from counterfeit medicine penetration using blockchain	Enhanced e-health network security and reduced counterfeit drug risk using a blockchain-based traceability model.	P. Pandey and R. Litoriya, Wireless Pers. Commun. (2021) [3]
3	Blockchain-based electronic healthcare record system for Healthcare 4.0 applications	Introduced a secure EHR system ensuring data privacy, interoperability, and decentralization via blockchain.	S. Tanwar et al., J. Inf. Secur. Appl. (2020) [5]
4	Security of vehicular ad hoc networks using blockchain: A comprehensive review	Provided insights into the use of blockchain to enhance security and trust in vehicular communication systems.	J. Grover, Veh. Commun. (2022) [7]
5	Trust-enhanced blockchain P2P topology for enabling fast and reliable broadcast	Proposed a topology design that improves trust and performance in blockchain-based P2P communication networks.	W. Hao et al., IEEE Trans. Netw. Service Manag. (2020) [9]

4. MATERIALS AND METHODS:

The counseled solution is a Cloud-Assisted Decentralized privacy-preserving Framework (CA-DPPF) that amalgamates cloud computing with blockchain era and the InterPlanetary record answer (IPFS) to securely administer healthcare data. Blockchain, a decentralized digital ledger, files transactions across numerous nodes, ensuring each transaction is cryptographically connected to its predecessor, so forming an immutable and transparent chain [1], [5]. This generation ensures the integrity of patient data and stops unwanted changes. IPFS is employed to save great medical files in a scalable and green manner, overcoming the storage constraints of traditional cloud structures [16], [20]. Cryptographic techniques, like ECDSA virtual signatures and RSA encryption, are employed to shield sensitive healthcare records and authenticate users, ensuring that most effective authorized individuals may additionally get entry to affected person facts [2], [13]. The integration of blockchain, IPFS, and sophisticated cryptography provides an impressive technique for shielding patient privacy while ensuring data accessibility and integrity.

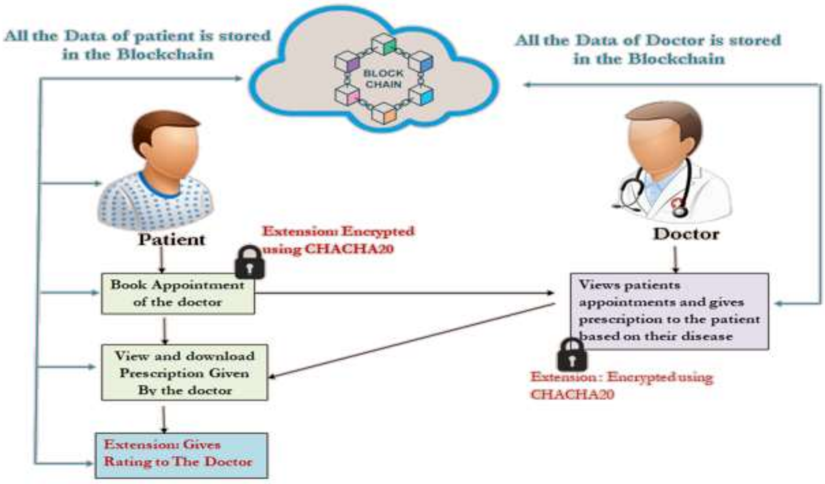

All the Data of patient is stored in the Blockchain
BLOCK CHAIN
All the Data of Doctor is stored in the Blockchain
Patient
Extension: Encrypted using CHACHA20
Doctor
Book Appointment of the doctor
Views patients appointments and gives prescription to the patient based on their disease
View and download Prescription Given By the doctor
Extension: Encrypted using CHACHA20
Extension: Gives Rating to The Doctor

Fig 1: Proposed Architecture

This instance (Fig.1) depicts a blockchain-based totally system for healthcare management. Patient and physician facts is securely preserved inside the blockchain. Patients may additionally time table appointments, access and download prescriptions, and evaluate physicians. Physicians retrieve patient appointments and prescribe cures in keeping with patient situations. All interactions between patients and physicians are encrypted with the ChaCha20 algorithm to assure data security. The blockchain guarantees openness and immutability, presenting a dependable platform for the transmission of medical data while keeping confidentiality.

4.1 Implementation:

The execution of the proposed system is segmented into more than one modules to guarantee comfortable and efficient administration of healthcare data. the brand new user sign-Up module enables doctors and patients to check in at the application, with user facts securely stored at the blockchain to ensure authenticity and keep away from tampering [1], [5]. Within the patient Login module, patients can authenticate, schedule appointments, and create a digital signature, using RSA encryption to safeguard patient data and ensure privacy [13], [18]. The doctor Login module allows physicians to oversee visits and medicines, with all files securely kept and controlled thru blockchain generation to guarantee integrity [4], [19]. Data storage and access management use IPFS for scalable data storage, whereas blockchain is utilized for transaction verification and integrity [16], [20]. The comments and ratings module documents patient feedback as blockchain transactions, guaranteeing authenticity and transparency [12], [19]. The Execution Time monitoring module assesses algorithm performance, facilitating efficiency comparisons among encryption algorithms [13], [14].

4.2 System Modules:

4.2.1. New User Sign-Up: This module permits physicians and patients to register inside the system by submitting their personal information. User information is preserved at the blockchain to offer immutable and genuine facts. Blockchain technology guarantees the cozy recording and verification of all data, along with current tendencies in employing decentralized ledgers for secure data management in healthcare [1], [5].

4.2.2 Patient Login: The patient Login module lets in patients to get entry to the device, observe a roster of physicians, and time table appointments. Upon scheduling an appointment, a digital signature is created, and RSA encryption is hired to shield the individual's personal and medical data. This guarantees that simplest verified physicians can access patient records, for this reason safeguarding privacy [13], [18].

4.2.3 Doctor Login: Physicians can access the system, review their appointments, and produce prescription reports. All interactions, inclusive of appointment booking and prescription generation, are securely recorded and managed via blockchain era, assuring data integrity and transparency [4], [19].

4.2.4 Data Storage and Access Management: patient reports and medical data are archived utilising the InterPlanetary file system (IPFS) to permit scalable and efficient storage. Blockchain is hired to store and authenticate every record as a transaction or block with a wonderful hash, as a result preserving data integrity and confidentiality [16], [20]. This decentralized storage approach mitigates the constraints of conventional cloud systems.

4.2.5 Feedback and Ratings: The feedback and scores module allows patients to offer evaluations and ratings for physicians. These ratings are documented as blockchain transactions, guaranteeing that the feedback is real and immutable. This mechanism ensures that physician evaluations are transparent and dependable for potential patients [12], [19].

4.2.6 Execution Time Monitoring: This module monitors the execution length of different algorithms employed inside the system. It offers graphical representations to facilitate performance comparisons among the authentic and elevated encryption algorithms, particularly RSA and CHACHA20, for the evaluation of computational performance and protection [13], [14].

4.3 Components:

4.3.1 Inter Planetary File System (IPFS): IPFS enables scalable, decentralized storage of extensive medical files, consisting of patient reports, medicinal drugs, and different personal statistics. The system employs IPFS to facilitate the effective storage and retrieval of medical records, for this reason diminishing dependence on centralized servers. This optimizes storage performance and improves data access times, mitigating the shortcomings of traditional cloud storage systems [16], [20].

4.3.2 Cryptographic Algorithms: superior cryptographic methods, like as RSA encryption and ECDSA digital signatures, are utilized to guarantee the security and integrity of patient records. These algorithms protect sensitive healthcare data during transactions, such as when consumers agenda appointments or physicians difficulty prescriptions. Cryptography guarantees that simplest authorized individuals can access and modify the data, safeguarding patient privacy and retaining system safety [13], [18].

4.3.3 Execution Time Monitoring Tool: This component evaluates the efficacy of various algorithms hired within the system, with precise emphasis on encryption and decryption operations. It monitors and contrasts execution durations of RSA encryption with the CHACHA20 algorithm, providing insights into system efficiency and computational performance. This optimizes system performance, guaranteeing that encryption operations are speedy and useful resource-efficient while maintaining safety [13], [14].

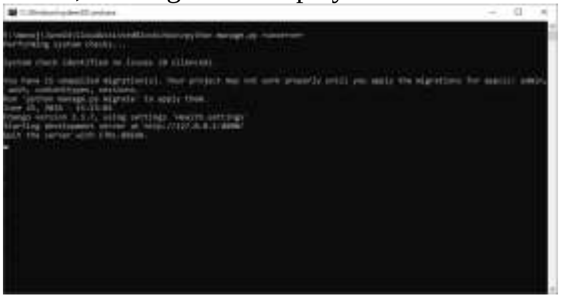
Together, these elements set up a resilient, secure, and efficient framework for managing healthcare data, ensuring privateness, integrity, and scalability while permitting seamless interplay amongst patients, physicians, and medical institutions.

4.4 Technical Implementation:

The machine utilizes superior era to enhance the security, privacy, and efficiency of healthcare data administration. Blockchain technology features as the fundamental element, imparting a decentralized, immutable ledger for the secure storage of transactions pertaining to patient data, medical appointments, prescriptions, and feedback [1], [5]. This guarantees transparency and integrity while obstructing unauthorized access. The InterPlanetary file system (IPFS) helps scalable and affordable storage of extensive medical data, addressing the limitations of traditional cloud storage via presenting a decentralized option for speedy and dependable data retrieval [16], [20]. advanced cryptographic strategies, such as RSA encryption and ECDSA digital signatures, are utilized to guard critical patient statistics, making certain that handiest authorized people can access or adjust the data [13], [18]. Furthermore, smart contracts developed with Solidity provide automated transactions on the Ethereum blockchain, making sure secure, rule-based interactions between patients and physicians [17], [5]. Together, those technologies facilitate a secure, transparent, and efficient healthcare environment.

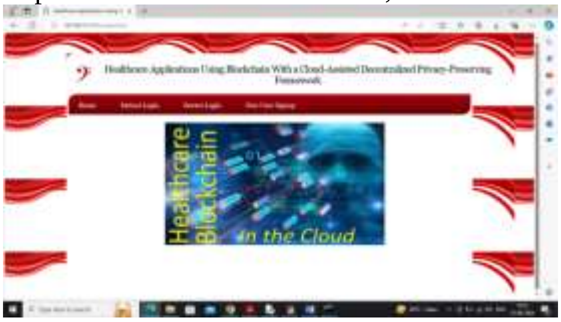
5. RESULTS AND DISCUSSION:

To execute the mission, double-click the 'runServer.bat' document to provoke the Python web cloud server, ensuing in the display of the screen beneath.

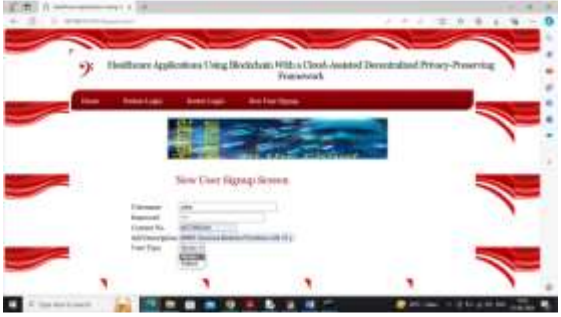


```
[illegible]
Performing system checks...

System check identified no issues (0 silenced).

You have [illegible] unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): [illegible]
 [illegible]
Run 'python manage.py migrate' to apply them.
[illegible]
Django version [illegible], using settings [illegible]
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

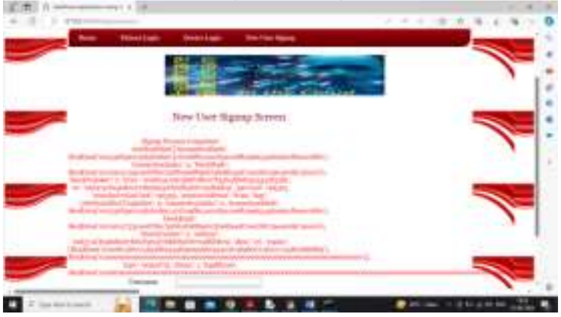
In the previous screen, the Python server has been initiated. Now, open a browser and input the URL http://127.0.0.1:8000/index.html, then click on the input key to display the following web page.


Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework
Home
Patient Login
Doctor Login
New User Signup
Healthcare Blockchain
in the Cloud

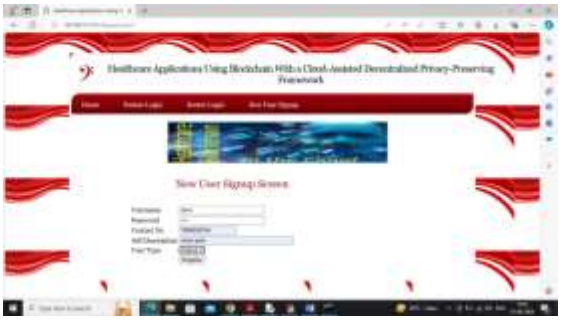
Click on the 'New user sign up' choice at the upper display screen to access the subsequent page.



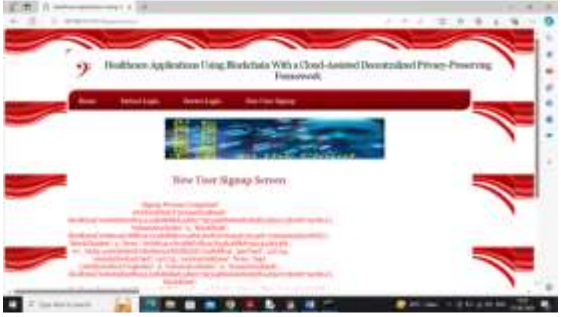
Within the previous screen, the doctor inputs the sign-up statistics and eventually presses a button to access the following web page.



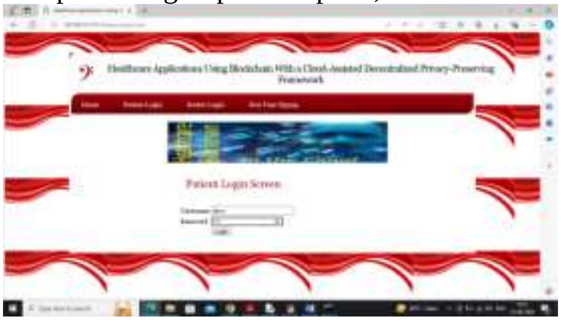
The sign-up work has been done on the aforementioned screen, and i am presenting the comprehensive log retrieved from the Blockchain post-storage, which includes details like as the hash code, block number, transaction quantity, and numerous other specifics. Additionally, consist of patient information as well.


Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework
New User Signup Screen

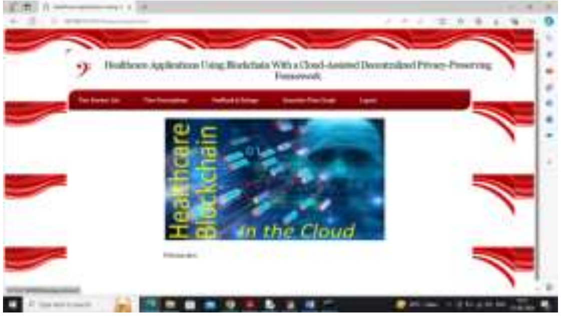
In the above page, the patient is inputting sign-up information and pressing a button to obtain the following output.


Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework
New User Signup Screen

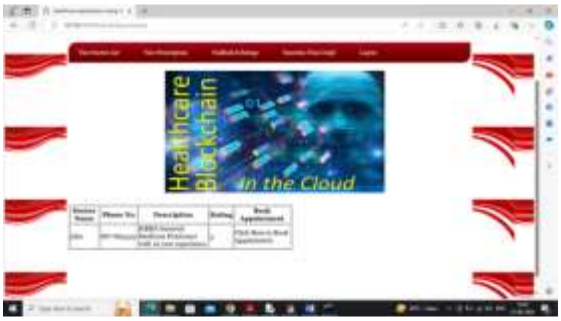
The patient sign-up is complete; now click at the 'patient Login' link to access the subsequent web page.


Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework
Patient Login Screen

Upon logging in, the patient will be directed to the following page displayed above.

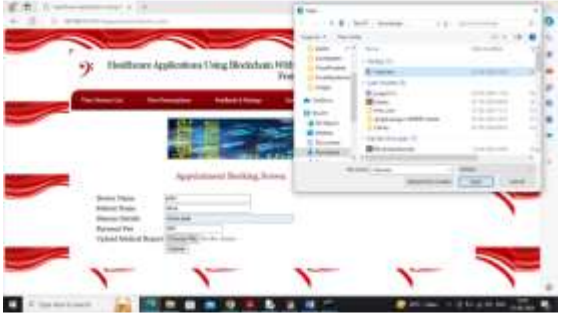

Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework
Healthcare Blockchain
In the Cloud

On the aforementioned screen, the patient can select the 'View doctors list' link to access the roster of doctors from the Blockchain.

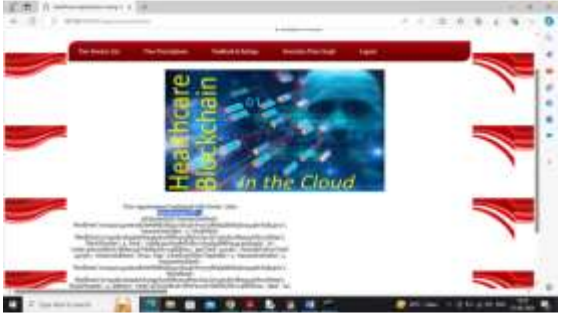


Doctor Name	Phone No	Description	Rating	Book Appointment
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

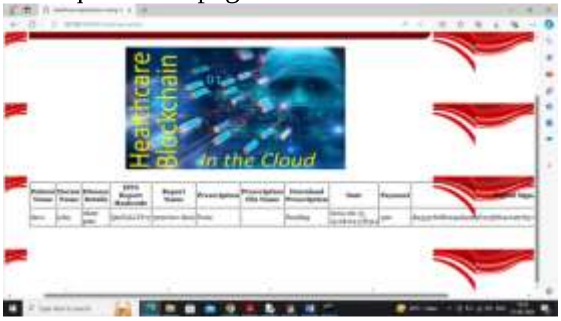
At the aforementioned screen, the patient can view a list of doctors and click at the 'click here to e-book Appointment' link to access the subsequent web page.



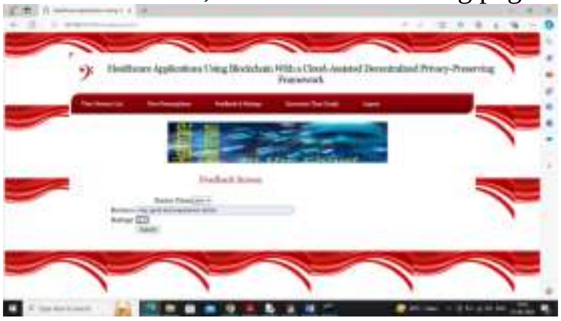
On the aforementioned screen, the patient will input disease details and thereafter upload relevant supporting papers to schedule an appointment, leading to the following page.



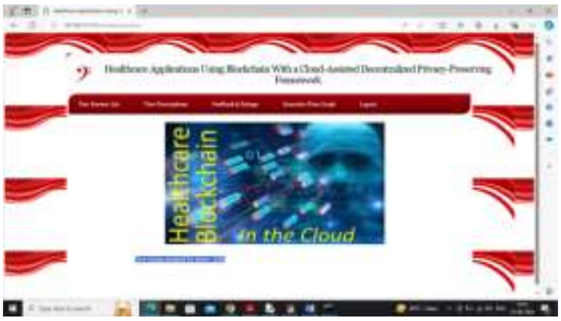
The appointment is verified at the above screen; now click at the 'View Prescription' link to access the subsequent web page.



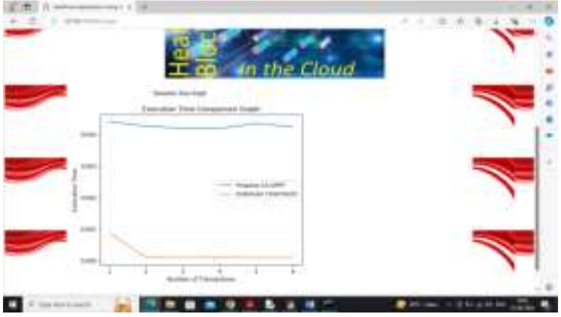
Inside the aforementioned screen, the patient can access all appointment details, such as a digital signature. The prescription is marked as 'None' since the doctor has not but generated it. Once the prescription is created, the user can view its details and ultimately click on the 'feedback & ratings' link to offer feedback, main to the following page.



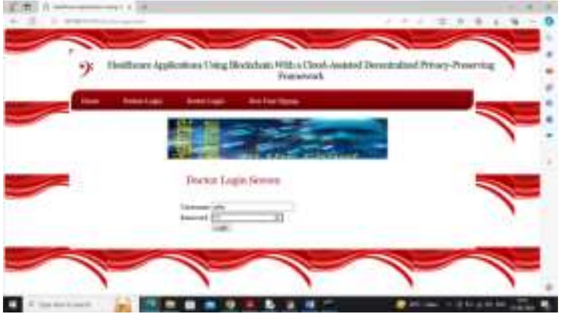
The patient can offer feedback and ratings for the chosen doctor, and all details can be recorded at the Blockchain, resulting inside the output below.


Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework
Healthcare
Blockchain
in the Cloud

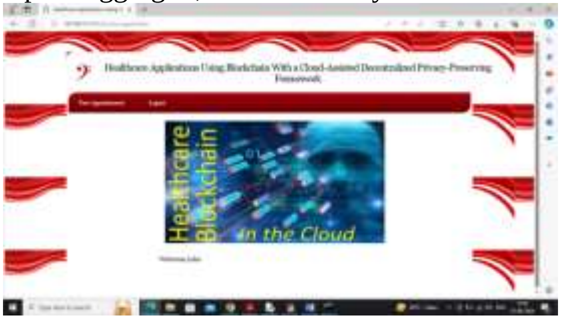
The feedback information are stored in the Blockchain; now click on the 'Execution Time Graph' link to get the following page.



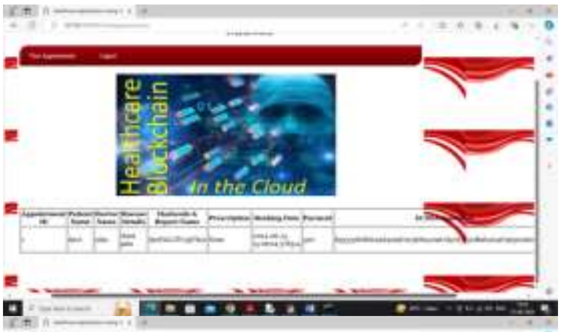
The graph above illustrates the number of transactions on the x-axis and execution time on the y-axis, indicating that the proposed technique requires extra time as compared to the extension algorithm. Finally, log out and log in as 'doctor' to generate a prescription.

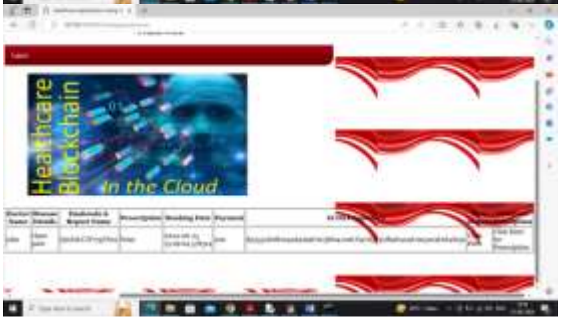

Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework
Doctor Login Screen

Upon logging in, the doctor may be directed to the subsequent page displayed above.

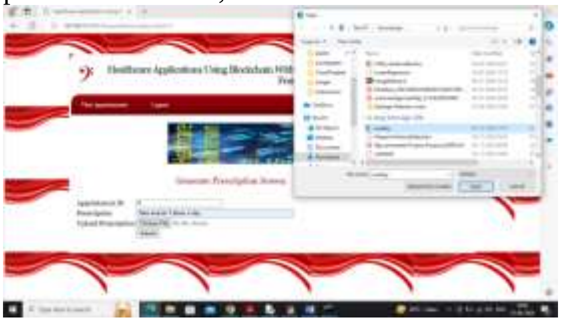

Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework
Healthcare
Blockchain
in the Cloud

On the aforementioned screen, the doctor can select the 'View appointments' option to access a page displaying all of his appointments.

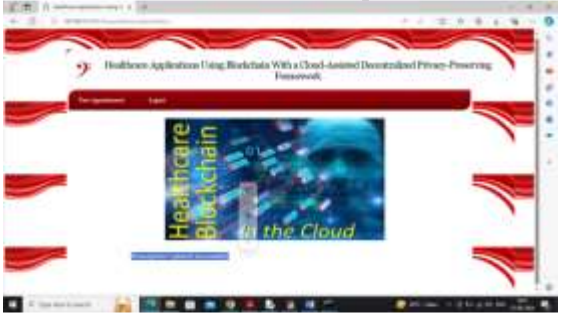




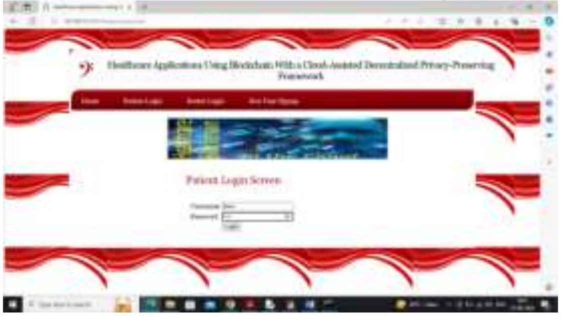
In the aforementioned display screen, the doctor can see a list of appointments observed by using a digital signature. they'll click on the 'click here' link to download and view supporting files related to the patient's condition, and click at the 'click here for Prescription' link to generate a prescription.



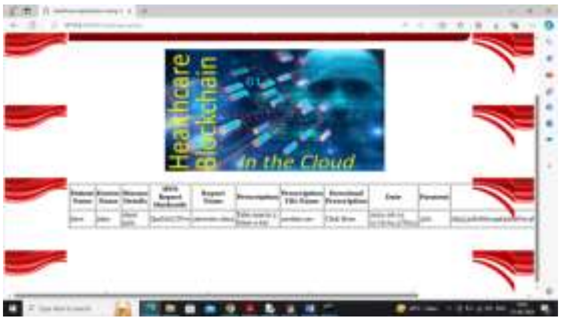
In the aforementioned screen, the doctor will compose a prescription, upload the accompanying documentation, and thereafter push a button to access the subsequent web page.


Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework
Healthcare Blockchain
In the Cloud

The prescription has been successfully updated on the screen, and patients can view and download it.


Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework
Patient Login Screen

In the screen above, the patient is logged in to access the next web page.



Patient Name	Doctor Name	Disease Details	IPFS Report Hashcode	Report Name	Prescription	Prescription File Name	Download Prescription	Date	Payment	
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	Click Here	[illegible]	[illegible]	[illegible]

On the above screen, the patient can view and download the created prescription.

In a comparable manner, by adhering to the aforementioned screens, we can ensure the privacy of patient data through the usage of cloud and blockchain technology.

6. CONCLUSION:

The challenge correctly combines cloud computing, blockchain technology, and the InterPlanetary file system (IPFS) to set up a at ease and efficient framework for handling patient data. The solution effectively resolves privacy and data management worries by utilizing the traits of each technology. The incorporation of the CHACHA20 encryption algorithm optimizes system performance by diminishing processing time relative to traditional encryption strategies, consequently enhancing data control efficiency and encryption velocities. IPFS enables decentralized storage, managing vast portions of medical data while diminishing dependence on centralized servers, hence improving storage efficiency and data retrieval speeds. Blockchain and Peer-to-Peer (P2P) processing beautify data management by alleviating the computational burden on centralized servers, enhancing processing speed, and reducing prices. The implementation of a blockchain-based physician evaluation system improves transparency and credibility, guaranteeing that patient feedback is truthful for knowledgeable decision-making. This era enhances patient privacy and safety of medical data, streamlines data management for healthcare practitioners, and offers medical institutions a comprehensive solution for secure data handling.

Future Scope may augment the system's competencies and user revel in. The integration of effective artificial intelligence (AI) and machine learning algorithms will facilitate predictive analytics and customized treatment strategies, enhancing healthcare outcomes. Improving the system to integrate with global healthcare networks will enable cross-border data trade, fostering international collaboration and studies while ensuring privacy and safety. The development of mobile packages and IoT device integration might facilitate real-time access to health data, subsequently enhancing patient-company interactions. Furthermore, ensuring interoperability with current electronic health record (EHR) systems will enhance data flow across platforms, facilitating improved care coordination and patient consequences. These impending enhancements would cultivate an extra holistic, efficient, and user-centric healthcare ecosystem.

REFERENCES:

[1] Omar, I. A., Jayaraman, R., Debe, M., Salah, S. K., Yaqoob, I., & Omar, M. (2021). Automating procurement contracts in the healthcare supply chain using block chain smart contracts. *IEEE Access*, 9(1), 37397-37409.

[2] Viswanath, Gudditi. (2022). A Smart Recommendation System for Medicine using Intelligent NLP Techniques. *International Conference on Automation, Computing and Renewable Systems (ICACRS)*, 5(2)1081-1084.

[3] Pandey, P., & Litoriya, R. (2021). Securing E-health networks from counterfeit medicine penetration using blockchain. *Wireless Pers. Commun*., 117(2), 7-25.

[4] Swapna, G., & Bhaskar, K. (2024). Early-Stage Autism Spectrum Disorder Detection Using Machine Learning. *International Journal of HRM and Organizational Behavior*, 12(3), 269-283,

[5] Tanwar, S., Parekh, K., & Evans, R. (2020). Block chain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl*., 50(10), 236-251.

[6] Viswanath, G. (2024). Multiple Cancer Types Classified Using CTMRI Images Based On Learning Without Forgetting Powered Deep Learning Models. *International Journal of HRM and Organizational Behavior*, 12(3), 243-253.

[7] Grover, J. (2022). Security of vehicular ad hoc networks using blockchain: A comprehensive review. *Veh. Commun*, 34(4), 124-126.

[8] Viswanath, G., & Dr. Swapna, G. (2024). Health Prediction Using Machine Learning with Drive HQ Cloud Security. *Frontiersin Health Informatics*. 13(8), 2755-2761.

[9] Hao W et al. (2020). Towards a trust-enhanced block chain P2P topology for enabling fast and reliable broadcast. *IEEE Trans. Netw. Service Manag*, 17(2), 904-917.

[10] Viswanath, G., & Swapna, G. (2025). Data Mining-Driven Multi-Feature Selection for Chronic Disease Forecasting. *Journal of Neonatal Surgery*, 14(5s), 108-124.

[11] Borgia, E. (2014). The Internet of Things vision: Key features applications and open issues. *Comput. Commun*, 54(5), 1-31.

[12] Viswanath, G. (2024). Personalized Breast Cancer Prognosis through Data Mining Innovations. *Cuestiones de Fisioterapia*, 53(2), 538-548.

[13] Deebak, B. D., Turjman, F. AI., Aloqaily, M., & Alfandi, O. (2019). An authentic-based privacy preservation protocol for smart E-healthcare systems in IoT. *IEEE Access*, 7(3), 135632-135649.

[14] Viswanath, G. (2021). Adaptive Light Weight Encryption Algorithm for Securing Multi-Cloud Storage. *Turkish Journal of Computer and Mathematics Education*, 12(9), 545-554.

[15] Turjman, F. AI., Deebak, B. D., & Mostarda, L. (2019). Energy aware resource allocation in multi-hop multimedia routing via the smart edge device. *IEEE Access*, 7(1), 151203-151214.

[16] Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *J. Med. Syst*., 42(2), 1-11.

[17] Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Inf. Process. Manage*, 58(2), 145631-145652.

[18] Khalid, U., Asim, M., Baker, T., Hung, P. C., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Comput*, 23(3), 2067-2087.

[19] Patwary, A. N., Fu, A., Battula, S. K., Naha, R. K., Garg, S., & Mahanti, A.(2020). Fogauthchain: A secure location-based authentication scheme in fog computing environments using blockchain. *Comput. Commun*, 162(2), 212-224.

[20] Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019). Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. *IEEE Access*, 7(3), 136704-136719, 2019.

[21] Swapna, G. (2023). A Drug-Target Interaction Prediction Based on Supervised Probabilistic Classification. *Journal of Computer Science*, 19(10), 1203-1211.

[22] Ray, P. P., Dash, D., Salah, K., & Kumar, N. (2021). Blockchain for IoT-based healthcare: Background consensus platforms and use cases. *IEEE Syst. J.*, 15(1), 85-94.

[23] Viswanath, G. (2024). Machine-Learning-Based Cloud Intrusion Detection. *International Journal of Mechanical Engineering Research and Technology*, 16(3), 38-52.

[24] Nagasubramanian, G., Sakthivel, R. K., Patan, R., Gandomi, A. H., Sankayya, M., & Balusamy, B. (2020). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Comput*. Appl., 32(2), 639-647.

[25] Swapna, G. & Bhaskar, K. (2024). Malaria Diagnosis Using Double Hidden Layer Extreme Learning Machine Algorithm With Cnn Feature Extraction And Parasite Inflator. *International Journal of Information Technology and Computer Engineering*, 12(3), 536-547.

[26] Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaria, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough?. *Future Internet*, 10(2), 1-16.

[27] Viswanath, G., & Dr.Swapna, G. (2025). Diabetes Diagnosis Using Machine Learning with Cloud Security. *Cuestiones de Fisioterapia*, 54(2), 417-431.

[28] Jiang, M., & Qin, X. (2022). Distributed ledger technologies in vehicular mobile edge computing: A survey. *Complex Intell. Syst.*, 8(5), 4403-4419.

[29] Viswanath, G. (2024). Improved Light GBM Model Performance Analysis and Comparison for Coronary Heart Disease Prediction. *International Journal of Information Technology and Computer Engineering*, 12(3), 658-672.

[30] Saqaf-AI W & Seidler N, (2017). Blockchain technology for social impact: Opportunities and challenges ahead. *J. Cyber Policy*, 2(3), 338-354.

[31] Viswanath, G., (2024). Enhancing Cloud Security: A Blockchain-Based Verification Framework for Multi-Cloud Virtual Machine Images. *Frontiers in Health Informatics*, 13(3), 9535-9549.

[32] Yang, J., Wen, J., Jiang, B., & Wang, H. (2020). Block chain-based sharing and tamper-proof framework of Big Data networking. *IEEE Netw*., 34(4), 62-67.

[33] Viswanath, G. (2021). Hybrid encryption framework for securing big data storage in multi-cloud environment. *Evolutionary intelligence*, 14(2), 691-698.

[34] Chattaraj, D., Bera, D., Das, A. K., Saha, S., Lorenz, P., & Park, Y. (2021). Block-CLAP: Block chain-assisted certificate less key agreement protocol for Internet of Vehicles in smart transportation. *IEEE Trans. Veh. Technol*., 70(8), 8092-8107.

[35] Viswanath, G. (2023). A Real-Time Case Scenario Based On URL Phishing Detection Through Login URLS. *Material science and technology*, 22(9), 103-108.

****