ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 14, Issue, 11, pp.4354-4359, November, 2023

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

SECURING SMART CONTRACTS USING FACIAL RECOGNITION IN THE HEALTHCARE SECTOR

Gayathri. D[1] and Dr. V. Raghavendran[2]

Research Scholar[1] and Assistant Professor[2]
Department of Computer Science, VISTAS, Chennai

DOI: http://dx.doi.org/10.24327/ijrsr.20231411.0818

ARTICLE INFO

Article History:

Received 10th October, 2023
Received in revised form 21st October, 2023
Accepted 17th November, 2023
Published online 28th November, 2023

Keywords:

Blockchain Technology, PMR, Iris Recognition, Face Recognition, Securing Smart Contracts.

ABSTRACT

Biometric systems are defined as systems to deal with automated recognition of a particular person's aspects like face, fingerprints, retina, iris, and patterns like posture, signature, etc.. The detailed expansion of the various methodologies of Biometrics that are used for authentication and verification processes in the Healthcare Sector. Biometric systems have many practical and social applications. The effects of the Biometric system in modern society have been discussed in this paper. Biometric Authentication performance is completely based on the Extraction and Matching of the individual feature. This paper relates to Blockchain Technology in the Healthcare Sector and how the database is managed using Bio-metric Methodologies.

INTRODUCTION

This paper discusses the latest bio-metric methodologies for securing smart contracts that contain PMR (Patient Medical Record) in Healthcare through Blockchain Technology. A PMR is used to store the patient's medical history and it is been digitalized for future analysis. The term PMR refers to the complete repository of the person's medication and it is been confined in the block and it is added to the chain, which can only be retrieved for the user after the authentication process. The Authentication is completely based on the Iris (Retina) and Face. The Paper discusses the Blockchain Technology used for Securing Smart Contracts in Healthcare, Smart Contracts, Benefits of using Smart contracts, and how it can be accessed through Bio-metric Methodologies (Mainly IRIS and Face). This paper demonstrates blockchain technology in the healthcare sector, Hallmarks of Blockchain, Smart Contracts (SC), Perks of Smart Contracts, Unique Biometric Authentication Methodologies.

BLOCKCHAIN TECHNOLOGY IN HEALTHCARE SECTOR:

Blockchain technology ensures the PMR's immutability, while smart contracts automate the PMR system, facilitating convenient and secure access through proper credentials.. The features [1] of the Blockchain promote good confidential transactions of PMR between Networks. Blockchain functions as an interconnected series of records that are highly resistant to modification and safeguarded by cryptographic measures. It enables decentralized data storage for users. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings [31] and not as an independent document. The working of Blockchain is clearly given in Figure 1

HALLMARKS OF BLOCKCHAIN

a. Blockchain as a Secure Data Registry-The blockchain functions as a ledger that records transactions, and these transactions are grouped together into blocks [16].
b. Decentralized - The distributed end-to-end network is a fundamental aspect of blockchain technology, and it's one of its standout features. This network structure, where groups of users collectively maintain the system, is a key highlight of blockchain innovation and works exceptionally well.
c. Consensus- Consensus is an algorithmic procedure designed to guarantee the presence of a single, universally shared record among all nodes. These mechanisms verify the accuracy and integrity of records.
d. Immutability-Data stored in the blockchain is immutable and tamper-proof. It is protected by

Corresponding author:* **Gayathri. D
Department of Computer Science, VISTAS, Chennai

employing cryptographic techniques or hash values to ensure the integrity of block information.

e. Enhanced Security-Blockchain technology removes the necessity for a central authority, preventing any individual from altering the network's attributes for their own benefit. Each piece of data within the Blockchain is protected through cryptographic hashing, enhancing the system's security.

f. Transparency-Every member holds an identical version of the complete dataset, and to add transaction blocks to the ledger, it requires consensus from the majority of nodes. This enhances transparency and eradicates fraudulent activities, enabling businesses to monitor every facet of the system.

g. Accelerated Settlements-Blockchain technology [3] holds the promise of expediting and increasing the flexibility of asset trade settlements. It achieves this by circumventing traditional intermediaries, leading to faster settlement processes. Investors with a greater urgency can choose to pay extra transaction fees to expedite the procedure.[22] By meticulously configuring block size and timing, miners are incentivized to prevent settlement errors and maintain precise transaction records

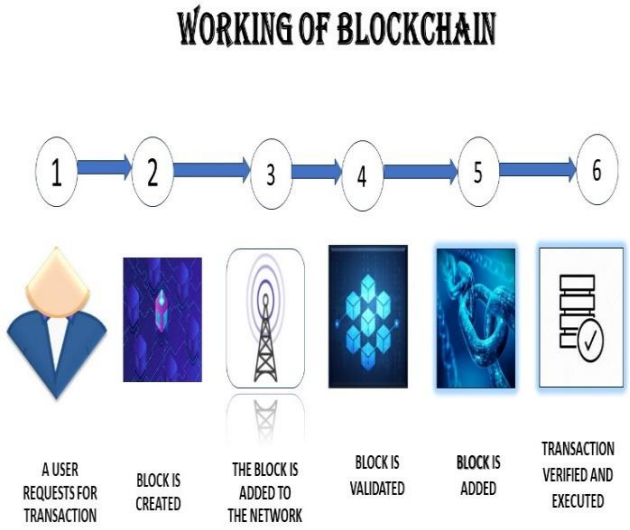

Figure 1 Working of Blockchain

SMART CONTRACTS

Smart contracts[2] at the crux is the code excerpt executed in a superior security that oversight digital assets. Besides, accumulating data, Blockchain technology acquires its prime proficiency through the support of smart contracts. Here PMR deals with the past Medical History[8] of the Patient. SC(Smart Contracts) are used to create patient profiles on Blockchain. This helps Medical Experts to suggest better Treatment procedures and possible outcomes. Medical Health Centers can also adapt SC to keep track of Patient Medical Health dilemmas. Furthermore, these SCs (Smart Contracts) can send the PMR to the insurance companies. The Structure of the Secured Smart Contract between the Stakeholders(Patient, HCP, Pharmacist) and the PMR(patient Medical Record) can be accessed across the world as depicted in Figure 2

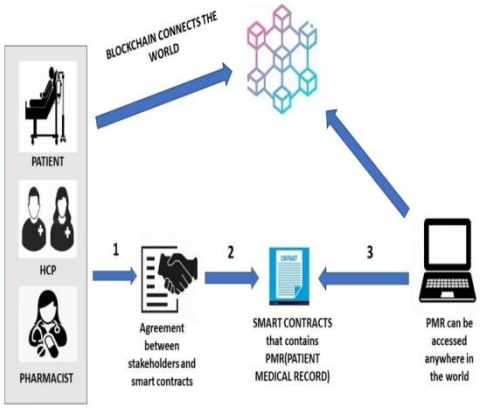

Figure 2 The Configuration of Secured Smart Contract

Here the Patients, HealthCare Providers(HCPs), and Pharmacists are the stakeholders of PMR(Patient Medical records)are secured in the Smart Contract[11] and can utilized anywhere in the Network after Completing the Biometric Authentication process like Iris Recognition or Face Recognition. Amidst all Biometric Authentication process, Iris recognition stands out for its superior efficiency and remarkable reliability in verifying authenticity. The constancy of the human iris remains unaffected by aging, maintaining stability over time. Additionally[5], the iris is inherently unique to each individual, including among siblings or twins. The iris is shielded by a structure, and altering it could potentially impact an individual's health[4]. It can be accessed using non-invasive devices. Therefore, numerous prominent companies, especially in the security sector, are eagerly anticipating the future of iris recognition technology due to its diverse applications and substantial potential.

VI.PERKS OF SMART CONTRACTS

Smart contracts are akin to self-executing computer algorithms that activate instantly if specific conditions are met. They form an integral part of an Ethereum network, managing the data and operations of blockchain transactions. Through binary interfaces, users can directly engage with smart contracts using their Ethereum wallet[6]. These contracts enable organizations to introduce extra functionalities, such as data transfer and access control. In essence, smart contracts offer a streamlined and automated approach to transactions and operational tasks.

a. Candor-Smart contracts enable the terms and conditions of these agreements to be completely transparent and available for review by all relevant parties. Once the agreement is in place, it becomes immutable and cannot be contested or disputed.

b. Exactitude-One of the fundamental prerequisites for smart contracts is the necessity to meticulously document[7] all the terms and conditions. This element is crucial as any omission can lead to transaction errors. Automated contracts aim to steer clear of the challenges linked with manually completing extensive sets of forms.

c. Risk Mitigation-Smart contracts utilize the most advanced data encryption methods, equivalent to those employed by cryptocurrencies. This results[9] in an exceptionally high level of security and protection, making them among the most secure entities on the internet.

d. Alacrity - Smart contracts exist online and operate through software code, enabling them to process transactions with exceptional speed. This rapidity can lead to substantial time savings when contrasted with conventional business procedures[10].

e. Efficacy - This results from the combination of precision and swiftness. What's particularly advantageous is that increased efficiencies result in a higher number of value-producing transactions completed within a given time frame.

f. Storage solutions and data replication -Smart contracts are employed to permanently record crucial information about every transaction. This means that whenever an individual's information is incorporated into a contract, it is securely stored for future reference. Consequently, if data loss occurs, these attributes can be readily recovered.

g. Trustworthiness – The advantageous of smart contracts is that they instill complete trust in their implementation[12]. The secure, self-governing, and transparent characteristics of these contracts eliminate any potential for favoritism, manipulation, or mistakes.

h. Surefire Outcomes - Another appealing aspect of automated contracts. They hold the capacity to greatly diminish or even eradicate the necessity for legal disputes and courtroom proceedings. Through the use of self-executing contracts[17], the involved parties pledge to abide by the regulations encoded within the contract itself.

i) Direct and Understandable Discussion -When establishing smart contracts, it's imperative to provide precise and comprehensive details [18]. This ensures there is no space for misunderstandings or misinterpretations, thus reducing the efficiency lost due to communication gaps.

SECURING HEALTHCARE CONFIDENTIAL DETAILS THROUGH SMART CONTRACT TEMPLATE

The fundamental concepts of the suggested architecture encompass the General Public Ledger [15], a specialized micro-leader, smart contracts, and an array of access controls. By applying the hash function, you can monitor and establish a connection between authentication and the blockchain outcomes. [19]Ultimately, the blockchain retrieves the hash. No third party is needed to access the Blockchain. Ethereum Blockchain is used to undertake Smart Contracts that contain PMR. The advantage of deploying a Smart Contract on the blockchain is the immutability of the contract and the reduced costs associated with delivery, authentication, and fraud detection. [20]

Additionally, distributed ledgers ensure seamless and tamper-proof execution. Every transaction is traceable and permanent. The Smart Contract's code is embedded in the blockchain, and actions occur based on predefined conditions. Compared to traditional contracts[13],Smart Contracts offer increased security and decreased operational expenses. The doctor or any end user enters a patient's information(PMR) into the database, that data is protected by smart contracts. The patient retains ownership of the data, and nobody can access it without their explicit permission.

The patient determines the list of individuals included in the smart contract. Members [14] on this list have the privilege to access the patient's data. Laboratory reports become accessible to doctors and consultants only after receiving authorization from the data owner. The patient grants access to others by adding their names to the smart contract list. Each record is encrypted through blockchain technology, and access is restricted to ensure the security of the data, all managed by smart contracts..The Smart Contract Template is shown in the Figure 3.

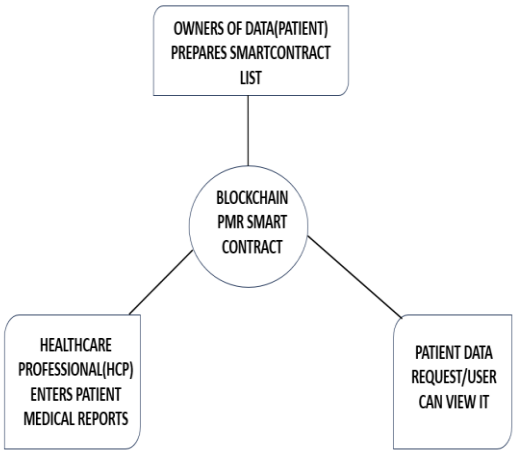

Figure 3 Smart Contract Templates

UNIQUE BIO-METRIC AUTHENTICATION METHODOLOGIES

A. Iris Recognition

Iris recognition techniques have demonstrated excellent performance in identification. These systems have garnered significant attention for their ability to identify individuals based on the unique and detailed patterns in the iris. Human irises possess a distinctive structure with intricate, small-scale features like freckles, coronas, and stripes. These observable characteristics of the iris are commonly referred to as 'iris texture,' making it a unique and well-suited feature for biometric measurement however,[37] despite these advantages, there are numerous challenges when it comes to recognizing irises in real-world, uncontrolled environments. The stability and reliability of the iris pattern, due to its exceptional uniqueness, surpasses that of other biometric technologies like facial recognition, palm prints, hand geometry, and voice recognition. The Iris validation system is structured into seven key phases. These include:

- Acquisition phase: Capturing the iris images.
- Preprocessing phase: Enhancing the quality of the iris image.
- Segmentation phase: Isolating the iris region from the image background.
- Normalization phase: Shaping the segmented iris region into a rectangle.
- Feature extraction phase: Extracting the iris region's distinctive features.
- Feature selection phase: Choosing the unique iris features using specific selection techniques.
- Classification phase: Sorting and categorizing the iris images.

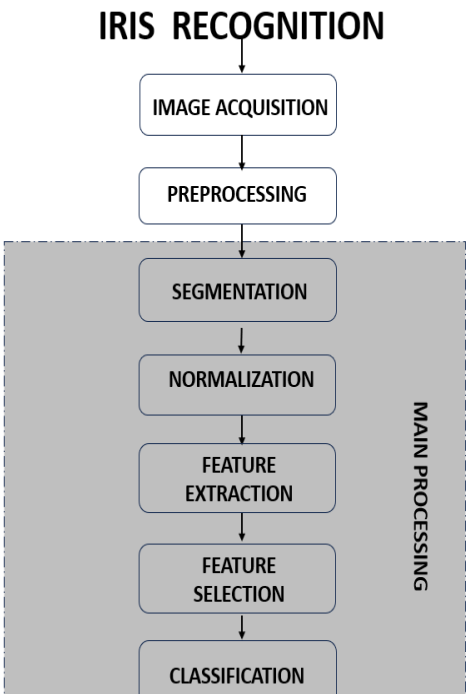

Figure 1.4 Key phases of iris recognition

B. Face Recognition

Facial recognition [21] is a technology-based method for identifying a human face. It employs biometrics to analyze facial features in an image and then compares this data with a database of known faces to find a match. The Architecture of Facial Recognition System is given in the Figure 1.5.This not only offers users a quicker and more secure login option but also enhances the security and dependability of the system when used in multifactor authentication, making it a highly reliable and trustworthy approach.[23]Face recognition technology is not a recent development, and you might already be familiar with it in your daily routines. Many of us use smart phones these days, and they frequently incorporate face recognition technology for unlocking. This technology serves as a robust[26] means of safeguarding personal information, ensuring that even if the phone falls into the wrong hands, sensitive data remains off-limits. Face recognition technology is finding applications in an increasingly wide range of areas, encompassing safety, security, and financial transactions. Face recognition is a comprehensive process that involves identifying or confirming an individual in digital images or video frames by analyzing their facial biometric patterns and data. This technology [24] collects a unique set of biometric data associated with an individual's face and facial expressions to verify their identity. Face recognition technology typically serves two primary purposes:

1. Face Verification: When presented with a face image, it determines if it matches any known images in a secure database, providing a yes/no decision (for instance, confirming if the person is who they claim to be). It checks if the person exists in the database.
2. Face Identification: Given a face image, it identifies the individual by matching it with known images in a secure database.

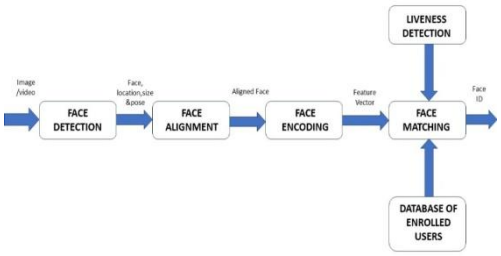

Figure 5 Architecture of Face Recognition system

REVIEW OF IRIS AND FACIAL RECOGNITION TECHNOLOGY

Iris recognition involves the use of infrared light and a digital camera to capture a high-contrast iris image. Nevertheless, the hardware for iris scanners [36] can be costly, user training is necessary, and these systems are typically bulky in size. While iris scanners excel in high-security environments due to their high accuracy, they may not be the most user-friendly option for frequently used areas. Iris matching algorithms are efficient and operate relatively swiftly once they have the iris image. These qualities make iris biometrics a viable choice for biometric authentication in scenarios where the top-notch user experience can be sacrificed in favor of a high level of security assurance.

Pros –

- Provides high accuracy under optimal conditions.
- Presumes user consent.

Cons -

- Involves a steep learning curve.
- Demands attended enrollment.
- Ineffective for all user types.
- Unreliable in varying environmental conditions.
- Authentication process is relatively slow.

Facial authentication[21] represents one of the least intrusive forms of biometric authentication. It's worth noting that each facial biometric solution has its approach to adapting to various lighting conditions, with varying degrees of effectiveness. Some solutions incorporate a large screen to guide users in aligning their faces correctly, while others, like the Rock, achieve this without a large screen by utilizing multiple sensors and AI. This allows them to detect a person, locate the face, assess liveness, and authenticate the user within a fraction of a second. High-quality facial authentication products can offer additional features, as mentioned earlier, beyond their authentication role. Additional motives [25] for opting for facial authentication comprise:

- Enabling one-to-many (1-N) matching for broader identity checks.
- Achieving cost savings.
- Facilitating smooth integration with pre-existing access control systems.
- Supporting two-factor and three-factor authentication methods.
- Providing touchless access capabilities.

Pros -

- Hygienic: No need for user interaction or physical contact.
- Swift: Quick in operation.

- Validates distinct credentials.
- Offers high-quality video at eye level.
- Employs computer vision and AI for exceptional capabilities.
- Provides an indisputable audit trail.
- Enables a seamless and effortless experience without friction

Cons -

- Certain systems are responsive to variations in lighting conditions.

CONCLUSION

Analysis of Blockchain Technology in Healthcare, Securing Smart Contracts that contain PMR (Patient Medical Records) through Unique Biometric Methodologies like Iris and Face implementation have been illustrated and the Scrutiny Iris and Facial Recognition Pros and Cons of the same have been discussed. In accordance with the study of Securing Smart Contracts through achieved through Facial Recognition than Iris. Face recognition involves the detection of faces from images or videos. Its applications range from authentication, such as the use of ATM cards (as in China), to military purposes. Over time, face recognition has evolved from theoretical concepts to automatic and artificial intelligence phases. Initially, traditional methods like geometric, template-based, and PCA were used for face recognition. These methods rely on comparing stored images in a database with the input using linear operations and Euclidean vectors. The market demand and advancements in technology have led to the improvement of face recognition through the use of ANN and DL methods. AI algorithms like FaceNet, DeepID, DeepID2, DeepID2+,Deep imbalanced, HyperFace, and DeepFace are examples of advancements in face recognition technology. Face recognition, a significant area of research, involves various methods to identify individuals.[35] Numerous algorithms rely on local features, dimensionality reduction, and hybrids for this purpose. This study reviews these approaches, including Principal Component Analysis, Independent Component Analysis, Linear Discriminant Analysis, and others like Gabor Wavelet. To enhance face recognition, future prospects include using soft computing and combining neural networks with fuzzy logic. The aim is to employ multiple techniques in combination for improved performance.

References

1. Amrita Jyoti and R. K. Chauhan, "A blockchain and smart contract-based data provenance collection and storing in cloud environment", Wireless Networks (2022) 28:1541–1562, March 2022.
2. Efthymios Chondrogiannis, Vassiliki Andronikou, Efstathios Karanastasis, Antonis Litke, Theodora Varvarigou, "Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations", National Technical University of Athens, 9 Heroon Politechniou Str, 15773, Athens, Greece, July 2021.
3. Rui Zhang, Rui Xue, and Ling Liu, Fellow, IEEE" Security and Privacy for Healthcare Blockchains", arXiv: 2106.06136v1 [cs.CR], 11 Jun 2021.
4. P. Chinnasamy, Ashwag Albakri,, Mudassir Khan , A. Ambeth Raja , Ajmeera Kiran and Jyothi Chinna Babu, "Smart Contract-Enabled Secure Sharing of Health Data for a Mobile Cloud-Based E-Health System", m. Appl. Sci. 2023, 13, 3970. https://doi.org/10.3390/app13063970, March 2023.
5. Abdulrahman Aminu Ghali, Sapiee Jamel,, Kamaruddin Malik Mohamad, Nasir Abubakar Yakub, Mustafa Mat Deris, "A Review of Iris Recogntion Algorithms" International Journal on Informatics Visualization, 2017.
6. Jasem Rahman Malgheet ,Noridayu Bt Manshor , and Lilly Suriani Affendey "Iris Recognition Development Techniques: AComprehensive Review",Hindawi ComplexityVolumeAugust 2021.
7. Christopher Libby1, 2 & Jesse Ehrenfeld "Facial Recognition Technology in 2021: Masks, Bias, and the Future of Healthcare", Journal of Medical Systems, February 2021.
8. K. Krishnakumar, S. Saravanan and Amine Naite-Ali, "Secured Face Recognition System Based on Blockchain with Machine Learning", Home Innovations in Computational Intelligence and Computer Vision Conference paper, October 2023.
9. Shahina Anwarul & Susheela Dahiya "A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy", November 2019.
10. Akib Mohi Ud Din Khanday, Aamir Amin, Irfan Manzoor, Rumaan Bashir" Face Recognition Techniques: A Critical Review", Recent Trends in Programming Languages January 2018.
11. Sneh Prabha, Rahul Bulchandani, Rajiv Mishra, Sarthak Agarwal, Shreya Chauhan, "Face Recognition Algorithms: A Review", International Research Journal of Engineering and Technology (IRJET), July 2021.
12. Waqar Ali, Wenhong Tian, Salah Ud Din, Desire Iradukunda and ullah Aman Khan "Classical and modern face recognition approaches: a complete review", October 2020.
13. Manuj Kumar, Tahera Hussaini," Face Recognition Algorithm based on Traditional and Artificial Intelligence: A Systematic Review", International Conference on Intelligent Technologies (CONIT), 2021.
14. Manal Abdullah, Shoaa Alhijily, "Biometric in Healthcare Security System, Face - Iris Fusion System", January 2011.
15. Mohammed Hazim Alkawaz, TuerxunWaili, Syaza Marisa binti Adnan, "Augmented Reality for Patient Information using Face Recognition and Cloud Computing", International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 6, Issue 1,2020.
16. Irfan Ahmed, Amina Asghar," Evaluating the Efficacy of Biometric Authentication Techniques in Healthcare", International Conference on Innovative Computing (ICIC), 2019.
17. Janelle Mason, Rushit Dave, Prosenjit Chatterjee, Ieschecia Graham-Allen, Albert Esterline, Kaushik Roy," An Investigation of Biometric Authentication in the Healthcare Environment", December 2020.
18. Meredith Van Natta, Paul Chen, Savannah Herbek, Rishabh Jain, Nicole Kastelic, Evan Katz, Micalyn Struble, Vineel Vanam and Niharika Vattikonda," The

rise and regulation of thermal facial recognition technology during the COVID-19 pandemic", Advance Access Publication, June 2020.
19. N. J. Abed and Ehab, Abdulrazzaq Hussein, "Design and Implementation of Real Time Health Care Monitoring System Based on IoT" 2021.
20. Dr. Santosh T. Jagtap, Chetan M. Thakar, Ouail El imrani, Khongdet Phasinam, Shaifali Garg, Randy Joy Magno Ventayen," A Framework For Secure Healthcare System Using Blockchain And Smart Contracts",2021.
21. Jayendra S. Jadhav, Jyoti Deshmukh,"A review study of the blockchain-based healthcare supply chain", 2022.
22. Cristina Vargas, Miguel Mira da Silva, Case studies about smart contracts in healthcare", National Library of Medicine, 2023.
23. Firas H.N. Al-mutar, Osman N. Ucan, Abdullahi A. Ibrahim," Providing scalability and privacy for smart contract in the healthcare system", December 2022.
24. Shafaq Naheed Khan, Faiza Loukil, ChirineGhedira-Guegan, Elhadj Benkhelifa and Anoud Bani-Hani," Blockchain smart contracts: Applications, challenges, and future trends", April 2021.
25. Farjana Khanam Nishi, Mahizebin Shams-E-Mofiz, Mohammad Monirujjaman Khan, Abdulmajeed Alsufyani, Sami Bourouis, Punit Gupta, and Dinesh Kumar Saini, "Electronic Healthcare Data Record Security Using Blockchain and Smart Contract", May 2022.
26. Hongru Yu, Haiyang Sun, Danyi Wuand Tsung-Ting Kuo," Comparison of Smart Contract Blockchains for Healthcare Applications", March 2020.
27. Kailash Chandra Bandhu, Ratnesh Litoriya, Pradeep Lowanshi, Manav Jindal, Lokendra Chouhan & Suresh Jain," Making drug supply chain secure traceable and efficient: A Blockchain and smart contract based implementation", November 2022.
28. Asma Khatoon," A Blockchain-Based Smart Contract System for Healthcare Management", January 2020.
29. Ibrahim Shawky Farahat, Waleed Aladrousy, Mohamed Elhoseny, Samir Elmougy and Ahmed Elsaid Tolba," Improving Healthcare Applications Security Using Blockchain", November 2022.
30. Lodovica Marchesi, Michele Marchesi, Roberto Tonelli, Maria Ilaria Lunesu" A blockchain architecture for industrial applications", 2022.
31. Francesco Bruschi, Manuel Tumiati, Vincenzo Rana, Mattia Bianchi, Donatella Sciuto," A scalable decentralized system for fair token distribution and seamless users on boarding", 2022.
32. Kristen N. Griggs, Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, Thaier Hayajneh," Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring", May 2018.
33. Koshechkin K.A,Klimenko G.S, Ryabkov I.V, Kozhin P.B," Scope for the Application of Blockchain in the Public Healthcare of the Russian Federation",2018.
34. Kanksha Saini, Zhu Qingyi, navneetsingh, Yong Xiang," A Smart Contract Based Access Control Framework for Cloud Smart Healthcare System", October 2020.
35. Noshina Tariqa, Ayesha Qamara, Muhammad Asima, Farrukh Aslam Khanb," Blockchain and Smart Healthcare Security: A Survey", 2020.
36. Moulouki Reda, DOMINIQUE BERNARD Kanga, Taif FATIMA, Mohamed AZOUAZI," Blockchain in health supply chain management: State of art challenges and opportunities"2020.
37. Abid Haleem, Mohd Javaid, Ravi Pratap Singh, Rajiv Suman, Shanay Rab," Blockchain technology applications in healthcare: An overview", International Journal of Intelligent Networks, September 2021.
38. Pranto Kumar Ghosh, Arindom Chakraborty, Mehedi Hasan, Khalid Rashid and Abdul Hasib Siddique" Blockchain Application in Healthcare Systems: A Review", January 2023.
39. Mahdi Ghafourian, Bilgesu Sumer, Ruben Vera-Rodriguez, Julian Fierrez, Ruben Tolosana, Aythami Moralez, and Els Kindt, "Combining Blockchain and Biometrics: A Survey on Technical Aspects and a First Legal Analysis", February 2023.
40. Youn Kyu Lee, Jongwook Jeong," Securing biometric authentication system using blockchain Securing biometric authentication system using blockchain", 2021.

How to cite this article:

Gayathri. D and V. Raghavendran, 2023. Securing Smart Contracts Using Facial Recognition in the Healthcare Sector. *Int J Recent Sci Res.* 14(11), pp.4354-4359.