Secure Medical Records Through Big Data Analytics and Blockchain

Hamad Almani [1], Shailendra Mishra [2], Aditi Singh[3]

[1] Department of Information Technology Majmaah University, Majmaah, Saudi Arabia
[2] Department of Computer Engineering Majmaah University, Majmaah, Saudi Arabia
[3] Department of Mathematics and Statistics, Indian Institute of Technology, Kanpur, 208016, India
Emails: 441104465@s.mu.edu.sa ; s.mishra@mu.edu.sa; aditisi22@iitk.ac.in

Abstract

As healthcare shifts to digital platforms, the healthcare sector is suffering from multiple security vulnerabilities that make it vulnerable to various types of cyberattacks. Therefore, robust security solutions need to be implemented to resolve these vulnerabilities. In this context, blockchain technology has emerged as a promising solution in several sectors, including the healthcare sector. This study harnesses blockchain technology to improve medical record management. By integrating blockchain, we address issues like data breaches and inefficient data sharing. The proposed study ensures a seamless health record exchange that is secure, transparent, and beneficial to both patients and healthcare providers. The goal of this study is to empower patients to be more in control of their data while streamlining processes and enhancing security for healthcare institutions. Medical records are increasingly secure, interoperable, and accessible when blockchain technology and big data are used. According to the study, healthcare workers recognize the importance of protecting medical records through blockchain technology and big data, which can improve security, interoperability, and accessibility. This minimizes concerns related to data manipulation while providing a more cost-effective and efficient method of managing medical records. Medical records management is made more cost-effective and efficient by reducing concerns related to data manipulation.

Keywords: Big data analytics; Blockchain; medical records; security; privacy; healthcare

1. Introduction

In the modern era of healthcare, the sanctity and security of medical records stand as pillars of trust between patients and healthcare providers. As the volume of digital medical data continues to surge, ensuring the confidentiality, integrity, and accessibility of these records has become an imperative of paramount importance. In response to this pressing need, the convergence of two groundbreaking technologies Big Data Analytics and blockchain offers a transformative solution that has the potential to revolutionize the landscape of medical record security.[4].

The advent of Big Data Analytics has ushered in an era of unparalleled insights derived from vast and diverse datasets. Its applications in healthcare have ranged from predictive analytics for early disease detection to personalized treatment plans based on comprehensive patient profiles. Concurrently, Blockchain technology, originally devised for secure and transparent financial transactions, has evolved into a robust platform for ensuring the integrity and immutability of digital records.[1].

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

This research embarks on a comprehensive exploration of the symbiotic relationship between Big Data Analytics and blockchain in the domain of medical record security. By harnessing the analytical power of Big Data, we aim to fortify the mechanisms through which medical records are collected, stored, and analyzed. [3] Concurrently, by leveraging blockchain's distributed ledger and cryptographic security, we endeavor to establish an impervious fortress against unauthorized access, tampering, and data breaches.

The timeframe between 2020 and 2023 represents a critical juncture in the evolution of both Big Data Analytics and Blockchain technologies. During this period, significant strides have been made in refining the capabilities, scalability, and interoperability of these technologies. This research endeavors to encapsulate the state-of-the-art developments and discern their application in the context of securing medical records.

In the pursuit of this objective, the research will delve into the existing challenges and vulnerabilities in medical record security, seeking to identify gaps that the integration of Big Data Analytics and Blockchain can address. Additionally, it will scrutinize practical implementations, case studies, and best practices, offering a roadmap for healthcare institutions and stakeholders seeking to fortify their information management systems.[2].

Ultimately, the culmination of this research aims not only to bolster the security of medical records but also to empower healthcare providers, researchers, and patients with a robust, transparent, and trustworthy system. By forging this new frontier, we envision a healthcare ecosystem where patient data is safeguarded with utmost diligence, ensuring that the promise of modern medicine is upheld with the highest ethical standards.

The main objectives of the proposed study are:

1. To analyze the current challenges and vulnerabilities associated with securing medical records in the healthcare industry.
2. To investigate the potential of big data analytics in identifying and mitigating security threats in medical record systems.
3. To explore the use of blockchain technology in ensuring the integrity, transparency, and privacy of medical records.
4. To develop a framework that integrates big data analytics and blockchain for securing medical records.

By focusing on these goals, the research seeks to improve the comprehension, efficiency, and expandability of Secure Medical Records systems, thereby bolstering the security and dependability of Big Data Analytics And blockchain. This research provides more accurate and reliable forecasts, which bolster big data analytics and blockchain security by thwarting data breaches, unauthorized entry, and service denials.

1.1 Research Motivations:

There are several research motivations in big data analytics and blockchain to secure medical records. Some of the key motivations include:

- To improve the security and privacy of medical records: Medical records contain sensitive personal data, such as health history, financial information, and medication lists. This data is a valuable target for hackers, and there have been several high-profile data breaches involving medical records in recent years. Blockchain technology can help to improve the security and privacy of medical records by making them tamper-proof and decentralized.
- To facilitate the sharing of medical records: Medical records are often shared between different healthcare providers, such as hospitals, clinics, and pharmacies. This can be a complex and time-consuming process, and it can be difficult to ensure that medical records are shared securely and accurately. Big data analytics can help to facilitate

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

the sharing of medical records by automating many of the tasks involved and by providing a secure and efficient way to share data.

- To improve the quality of healthcare: Big data analytics can be used to improve the quality of healthcare in several ways. For example, big data analytics can be used to identify patterns in medical data that can lead to new insights into diseases and treatments. Big data analytics can also be used to develop personalized treatment plans for patients based on their individual medical history and genetics.

The organization of the paper is as follows; section 2 shows the related work, section 3 represents the methodology of the proposed work, section 4 includes experimental setup, section 5 discusses results and analysis, and section 6 shows the conclusion and future work.

2. Related Work

IRMT defines "Information record management" as the competent and effective management of information. A crucial aspect of this is ensuring that medical records accurately document diagnoses and treatments allowing physicians to provide future care. Proper management of health records plays a role in making healthcare decisions shaping legislation and contributing to the success of healthcare organizations and agencies.

According to [2,3] blockchain-based technology offers a shared platform for easy access to records, which is essential for maintaining the health of a nation. Therefore it is crucial to maintain records for effective monitoring of both healthcare providers and their patients. These records also play a role, in shaping healthcare policies that directly affect the well-being of a nation's citizens.

Blockchain and big data are two technologies with great potential and great influence in the field of information technology. Big data research is applied in many fields of society[4]. However, big data has features such as large size, temporal events, complex structure, and incompleteness. Therefore, big data has many challenges that need to be researched such as data security, data integrity, anti-fraud, data quality, data management, data analysis, and data mining [5]. Medical records that are centralized are convenient and secure [6]. Patients and doctors benefit from improved resource utilization.

Blockchain technology has the characteristics of distribution, immutability, transparency, and security. Therefore, integrating Blockchain technology into big data is a promising solution to overcome these challenges. However, Blockchain technology is not mature yet. Researchers need to identify the problem and have a suitable approach for applying Blockchain technology to big data. In this article, we survey and present a complete picture of the integrated base. At the same time, cloud services for big data, application range, and Blockchain big data projects are also presented, the researchers were able to identify the development challenges and future directions [7].

Integrating Blockchain technology with big data analytics can lead to efficient and transparent record management in the healthcare sector, reducing administrative burdens. [3] highlights that blockchain can create an elaborate and highly efficient database management system for healthcare providers, enabling easy management of various types of data. [1] emphasizes the role of big data in making predictive decisions for quality care and better health planning, with technologies like Hadoop providing cost advantages and the ability to analyze large amounts of structured and unstructured data. [9] discusses the challenges and potential of big data in healthcare, emphasizing the need for proper management and analysis to derive meaningful information and improve public health. [3] focuses on the integration and standardization of heterogeneous healthcare and medical data, suggesting the use of suitable data governance policies and software development frameworks to reveal valuable insights. In summary, the papers suggest that integrating big data analytics with blockchain technology can enhance data management in healthcare, leading to efficient record-keeping and valuable insights for personalized healthcare.

Integrating electronic health records (EHRs) and granting patients access to their medical records can empower patients and give them greater control over their healthcare information. [4] and [7] emphasize the importance of patient empowerment through online access to health records. [3] also highlights patients' desire for more control over their medical records. Additionally, [4]emphasizes the need for an integrated view of patient information to improve the quality of care and patient safety.

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

2.1 Research Gap

While there is a growing interest in the application of big data analytics and blockchain in healthcare, there are still significant research gaps that need to be addressed. Some of the key areas for future research include:

1. Integration of big data analytics and blockchain: There is a need to explore how big data analytics and blockchain can be integrated to provide a comprehensive solution for securing medical records. This includes developing frameworks, algorithms, and architectures that leverage the strengths of both technologies.
2. Scalability and performance: Big data analytics and blockchain are resource-intensive technologies. Research is needed to develop scalable and high-performance solutions that can handle the large volumes of healthcare data generated in real time.
3. Data privacy and consent management: While blockchain technology provides a mechanism for data privacy, there is a need to develop frameworks and protocols for managing patient consent and ensuring compliance with privacy regulations.
4. Interoperability and standardization: Research is needed to develop interoperability standards and protocols that enable seamless data exchange between different healthcare entities. This includes addressing the challenges of data mapping, data transformation, and semantic interoperability.
5. Ethical and legal implications: As with any emerging technology, there are ethical and legal implications associated with the use of big data analytics and blockchain in healthcare. Further research is needed to understand and address these implications, including issues of data ownership, liability, and informed consent.

3. RESEARCH METHODOLOGY

The patient record is a data file that contains different items of security requirements and can be chosen to share with a wide spectrum of distinct individuals that may include but is not limited to admitting staff members, physicians assisted by nurses, And technicians that provide the required treatment, and maybe even financial or discharging staff members. Selectively sharing data files on the cloud becomes a burden on the data owner as the hierarchy grows (the access privileges increase in number) and/or as the access restrictions become more complex due to an increase in the sensitivity of the file segments. If those staff members can access the necessary parts of the patient's medical record(s), it can expedite their specific jobs, such as patient admittance and treatment, and prevent iatrogenic illnesses caused by administering inappropriate medication or harmful drugs.

However, for the sake of patient privacy, staff Members should only be permitted to access patient record(s) from the medical history based on the profile of the patient. A trivial solution is to encrypt each part of the patient record using public-key encryption and grant access to the private keys to the staff members based on their permissions. However, this solution is quite inefficient due to the large number of encryptions and storage spaces required. Therefore, the challenge is to provide the data owners with an efficient, secure, and privilege-based method that allows them to selectively share their data files.

Blockchain technology is formed together by different blocks that are connected as chains in a network. It makes a decentralized system. Each block contains a hash code of previous blocks along with current block data. Any records can be added to this type of blockchain because it uses cryptographic functions that provide security to the database connected to its network.

The main purpose of this study is to secure the data of medical records in a database using a blockchain that uses the hash function Algorithm. It is Hashing is a mathematical function that takes a set of inputs and fits them in the form of a blocks table or different data structure that contains fixed-size values. It is a combination of the latest message block and the output of the previous block. The integrity of data is a common factor in the hash function that is used to generate the sum of correct digits to use later for comparison to find out errors in the data blocks. It will detect any changes made to the original file. For every block, there is a hash value generated to check the previous block and in this way, all blocks are connected in a chain of hash codes without the data being tampered with. hash codes can be verified by the administrator to check the data has not been tampered with. If any attempt to compromise the data in all the blocks in the database then the chain of hash codes will be irrational and it can be easily recognizable by the

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

administrator. Fig.1,2 and 3 shows System Architecture, Flowchart of the Proposed System and Block Diagram of Hash respectively.

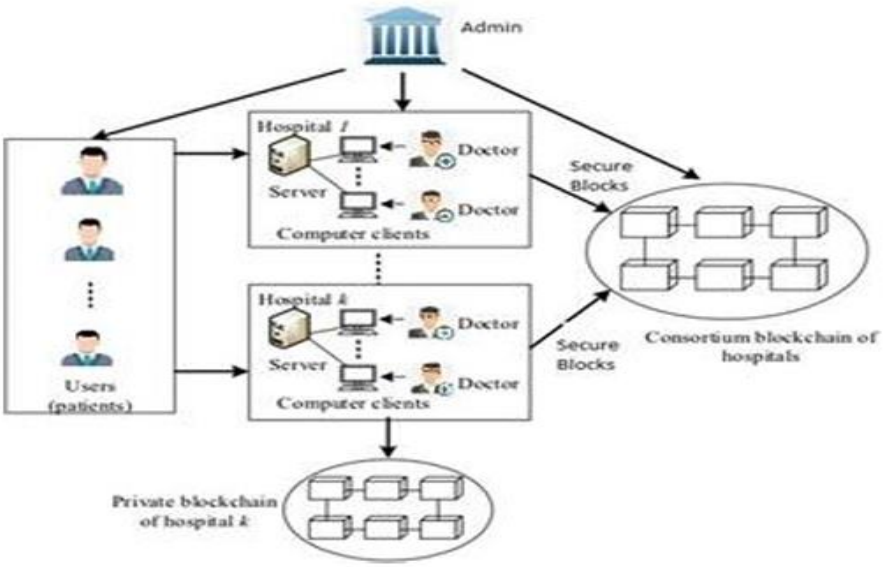

Figure 1: System Architecture

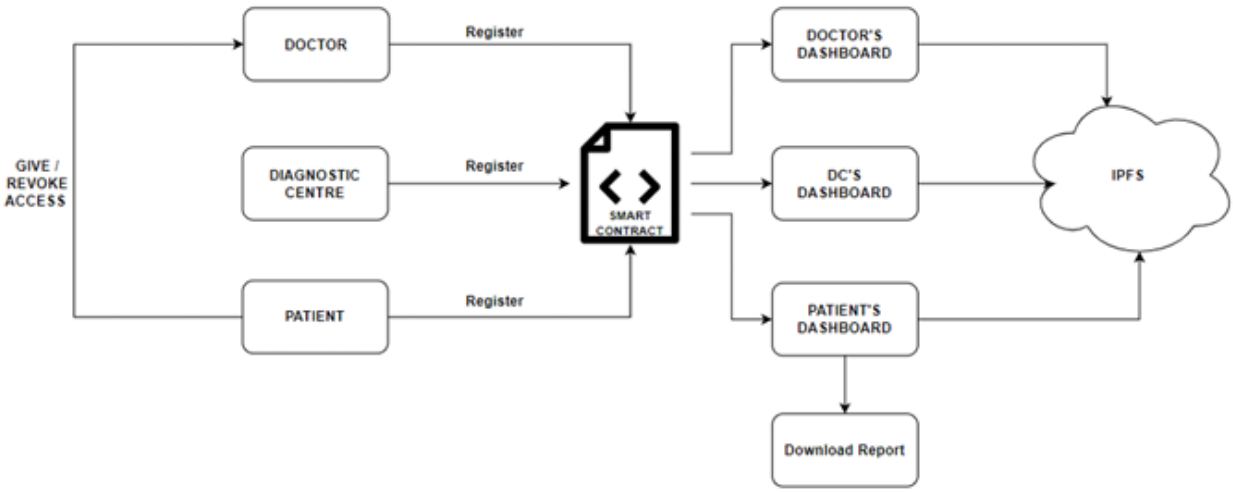

Figure 2: Flowchart of the Proposed System

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

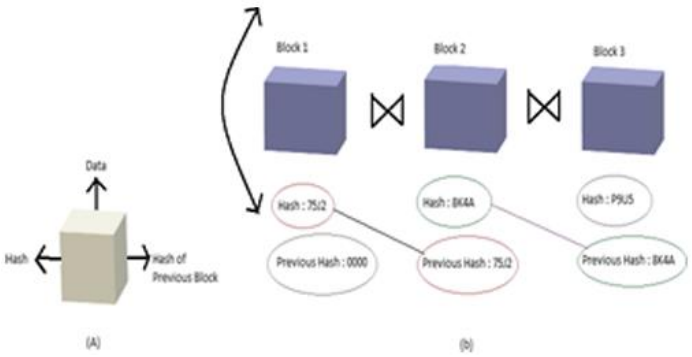

Figure 3: Block Diagram of Hash

Data is stored in the form of blocks. those blocks are connected using the hash value. All blocks have specific hash values. Every Block has a previous hash value excluding the starting one which consists of either zero or null. The next block contains a hash value of the previous block, similarly, the next blocks are connected like this. Parameters used to calculate hash values are previous hash, patient's ID, Doctor's ID, treatments, and timestamp. Considering all these parameters, Hash values are generated.

4. Experimental And Implementation:

In this system, the main actors are Admin, Doctor, and Patient. Admin has all the rights of giving secure access to doctors and patients to check medical records. Admin adds all the details of the Doctor including Name, Email, Phone number, Password, and Degree. Also, he can check all the doctors added from the previous history. The same procedure is done for Patients to give access to their medical records. The accuracy of the system is that nobody can tamper with any data in the database including admin. All treatment details of patients can be viewed but cannot manipulate anything in it.

As we can see, Admin has provided login access to doctors. So whenever a new patient is visiting that specific doctor, he can check that patient's entire history. On that basis, the Doctor can add more treatments further for that patient and that patient will be added to that doctor's list. If somehow some data has been tampered with within the database, then the doctor cannot add any more treatment to that specific patient. This confirms that no more data can be stored in blocks until all issues are resolved. Admin has given access to the patient to check their medical history. The patient can also check their treating doctor's name and treatment with a timestamp.

This work enhances the security of the Medical Record. This work aims to encrypt the passwords and hide them in a cover image using a hash function. We implemented this work using the Web platform and using a MySQL database and PHP.

The platform has an important weak point which is storing the passwords as clear text in the database thus leaving them vulnerable to exposure to database attacks such as SQL injection attacks.

Therefore, we in this work avoid the previously mentioned weak point by saving the hash digest of the password in the database instead of saving the password itself.

Another reason for choosing the hash function to improve the weak point is its time efficiency, i.e. hash digest consumes a little bit less time in its computations. Also, the hash function always produces the same output length independent of the length of its input (e.g. passwords) which is a data storage standardization benefit.

The improvement is implemented based on one main assumption as follows:

- Creating the based on one level security which is the hash function.

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

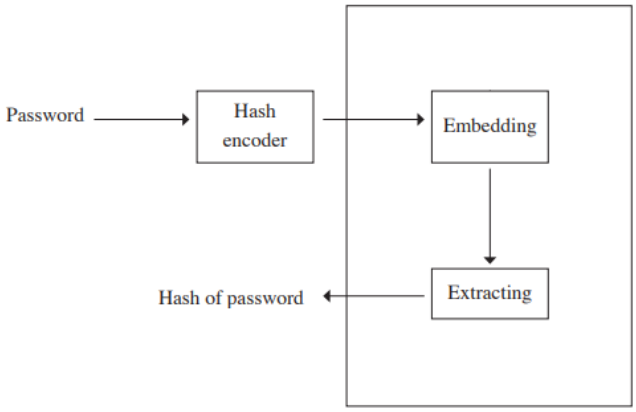

Figure 4: Assumption (Hash function)

For the first, hash implementation, The processes of the first assumption are illustrated in Fig. 4 Moreover, this assumption guarantees the confidentiality of the password and the integrity of the password by hash function as overcoming the drawback. Also, the hash function emphasizes the authenticity of the user.
The sequence of operations in the system is based on the first assumption as in the following steps:
A . If the user chooses the Signup operation:
1. Go to the Signup interface.
2. Enter your username, password, and email.
3. Press the Signup button.
4. Store data in the database.
5. Compute the hash value of the password.
6. Hide the result of the hashing algorithm.
7. Print “Registration Success…”.
8. Go to the main interface.

B . If the user chooses the Login operation:
1. Go to the Login interface.
2. Enter your username.
3. Click the sign-in button.
4. Decrypt the result from the algorithm using the username as a key.
5. Set the hashing password.
6. Find a row in the database such that the username column is equal to the entered username and the hashing password column is equal to the hashing password.
If the server finds the row in the database:
1. Print “Registration successful, you can log in".
2. Go to the access granted interface.
3. Show the username.
Otherwise:
Print “Login Failed...Try Again”.

5. Results And Discussion

Analyzing performance and assessing mistakes that arise when the program is performed in various operating settings and with various input sources is the primary goal of testing. We have created a GUI in this investigation. The primary goal of evaluating this research is to see if encryption techniques are used to safeguard user data and to determine how well the system performs when different inputs are provided. The steps involved in testing are: Testing for Validation and user acceptance testing.

A. Validation Testing

Passwords are frequently securely stored using hash algorithms. The password that a user chooses while creating an account is hashed and kept in a database.

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

The password is hashed once again and compared to the saved hash when the user signs in (Fig.5) . The user gets access if the hashes match. In this manner, the original passwords cannot be discovered, even in the event that an attacker manages to get access to the password database. Fig.6, shows Code Hash functions(passwords).

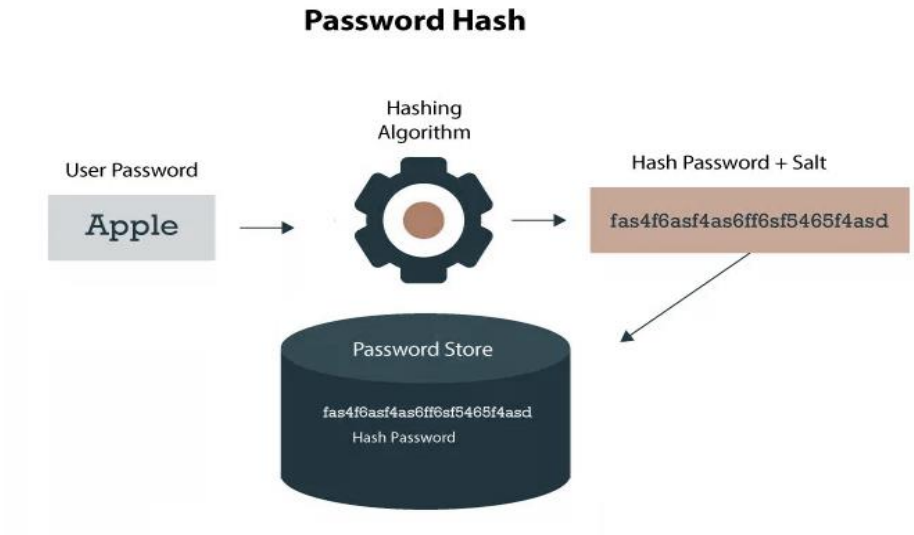

Figure 5: Hash functions (passwords).

```php
$inputPassword = $_POST['password'];

// Retrieve the stored hashed password and salt from the database
$storedHashedPassword = "hashed_password_from_database";
$storedSalt = "salt_from_database";

$hashedInputPassword = hash('sha256', $inputPassword . $storedSalt);

if ($hashedInputPassword === $storedHashedPassword) {
    // Passwords match, allow login
} else {
    // Passwords do not match, deny login
}
```

Figure 6: Code Hash functions(passwords).

A. User Acceptance Testing

The integrity, convenience, and security of the proposed medical system should conform to the characteristics of the mobility of medical records, the urgency of medical care, protection of connection function and security, and avoidance of medical conflicts. The following descriptions would prove the system satisfies the requirements. Fig. 7,shows From the database Hash functions(passwords).

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

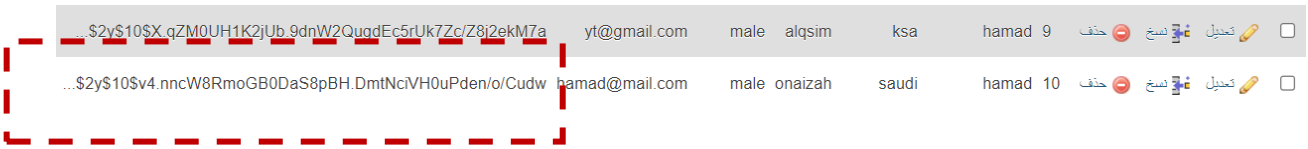

Figure 7: From the database Hash functions(passwords).

B. Output UI System.
Shows in Fig 8 to 19,it includes login page, registration page etc.

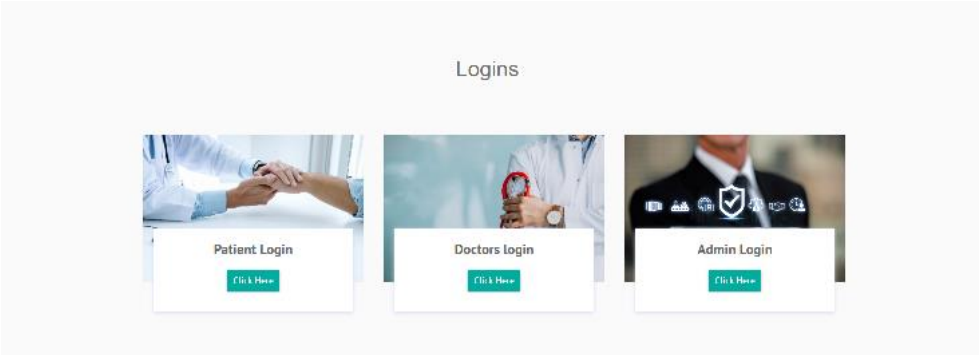

Figure 8: Login Page

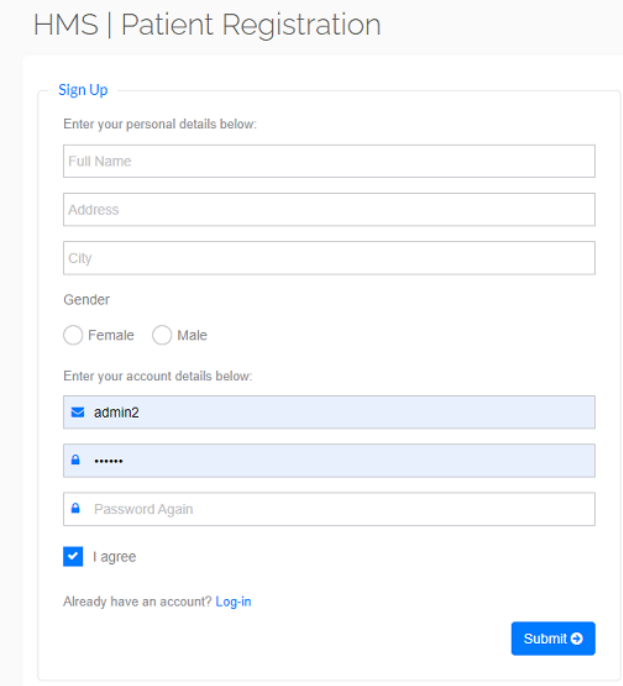

Figure 9: Patient Registration Page

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

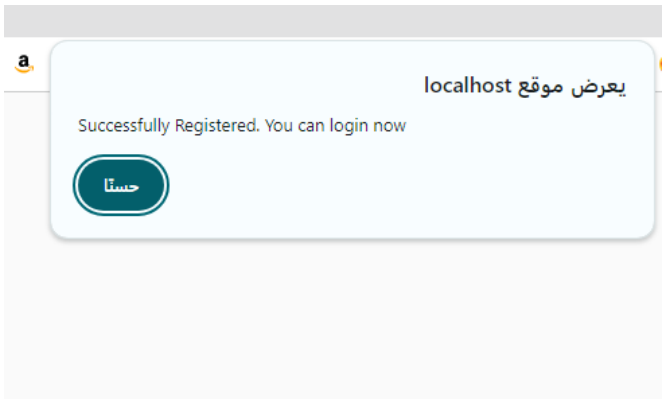

Figure 10: Login success message

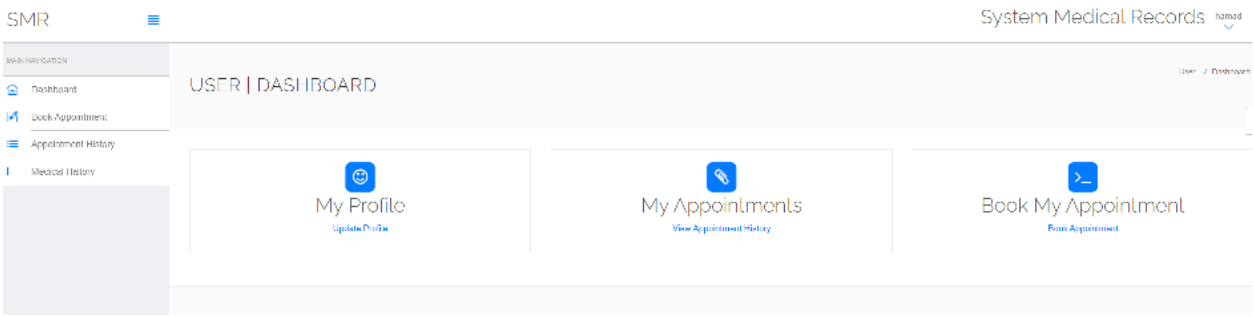

Figure 11: Dashboard Patient

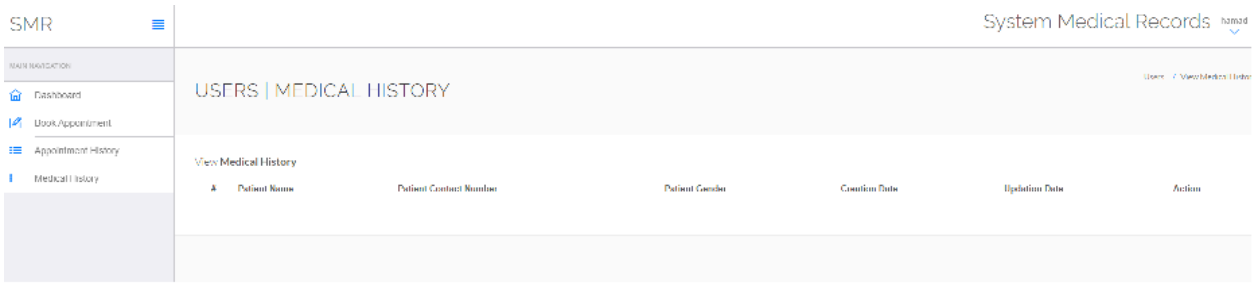

Figure 12: Medical History

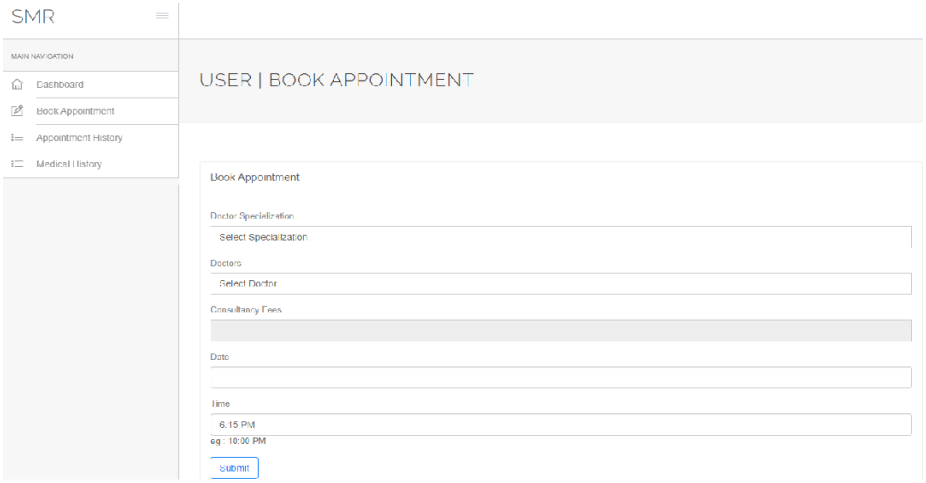

Figure 13: Book Appointment Patient

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

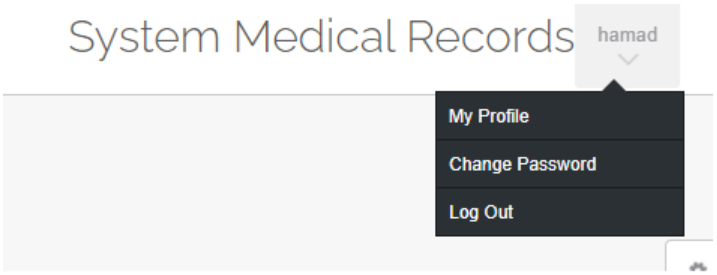

Figure 14: Settings, profile, and logout

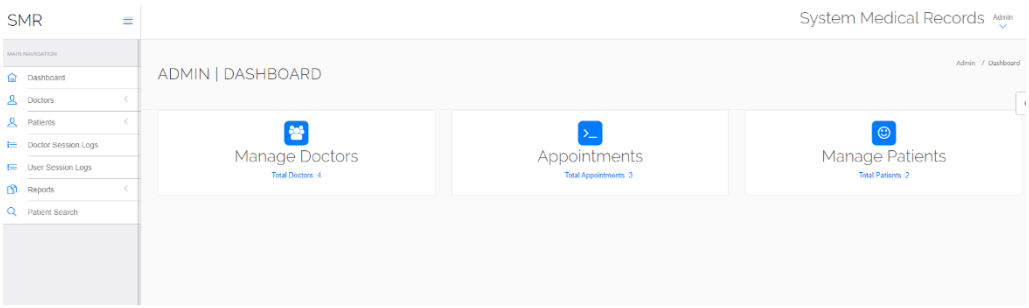

Figure 15: Dashboard Admin

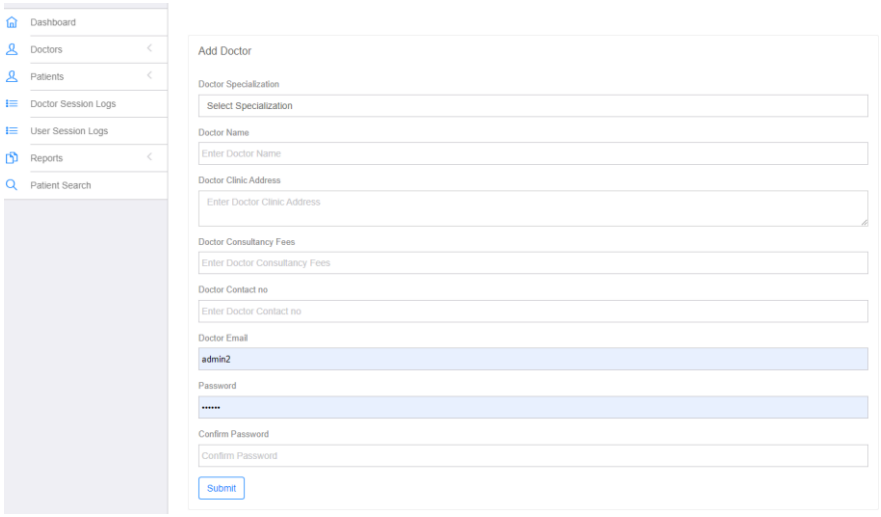

Figure 16: Add Doctor

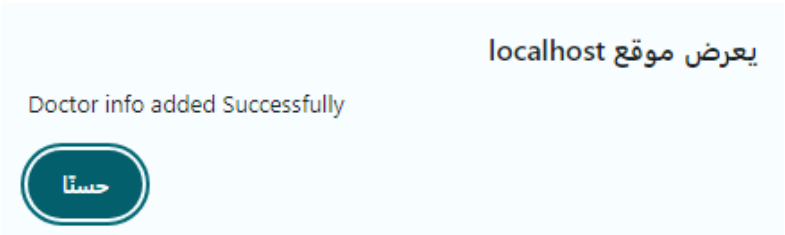

Figure 17: Success Message Add Doctor

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

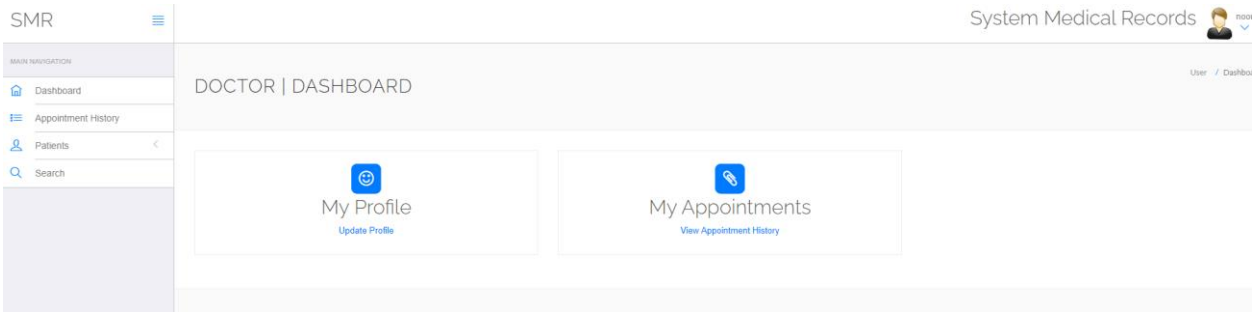

Figure 18: Dashboard Doctor

Figure 19: Store password from database

The fig.18 shows the Dashboard for all three Profiles where all the registered Profiles will be shown with all data provided by the user. Fig.19,shows Hash function application.

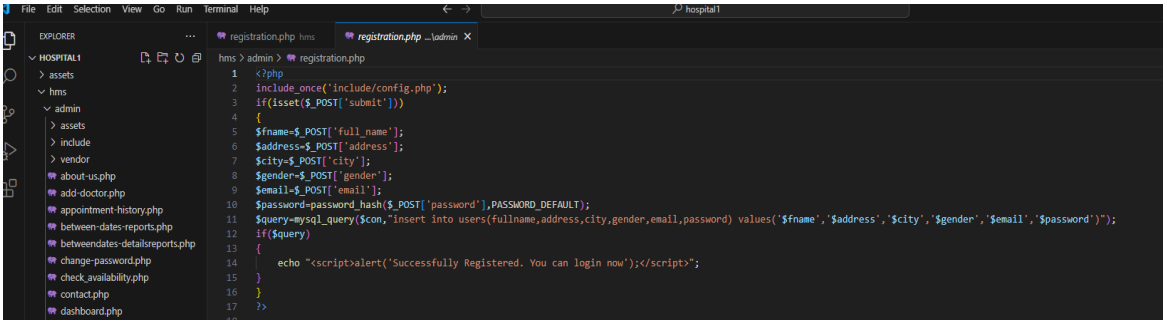

Figure 20: Hash function application

5.1 Discussion

A. Security Analysis

Patients can safely exchange their medical record data with their physicians thanks to the suggested method. This is due to the fact that our method employs re-encryption to ensure user protection while significantly decentralizing every part of the system.

B. Generalization

Despite focusing on a particular use case, the suggested solution is applicable to a broad spectrum of other

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

issues.
The patient can be thought of as a broad information source. Since the source will now be the organization in charge of deciding who can and cannot access the information, this is a better option than using the hospital as the source.

C. Restrictions and Difficulties

There are several obstacles that hinder the suggested blockchain-based password-protected patient-centered SMR system solution. i.e. Key personnel: The key management design of blockchain systems lacks user-friendliness and flexibility in the event that patients forget their credentials, even if it is unreliable when employing the hash function to authenticate patients.

6. Conclusion

This study enhances the security of the authentication system in devices. The weak point studied in previous research is storing the passwords as clear text in the database. Thus, leaving passwords vulnerable to exposure to database attacks such as SQL injection attacks. Therefore, this work avoids the previously mentioned weak point by saving the Hash digest of the password in the database instead of saving the plain password itself, i.e. adopting the hash function. Our improvements are based on the two main assumptions. Creating the based on one level security which is the hash function. The results showed that the combination of all security methods gives the best attributes, i.e. confidentiality, integrity, and authentication. Blockchain technology is proving to be a valuable solution for solving security challenges, thanks to its unique features of decentralization, immutability, and transparency. In this paper, we studied and identified the security vulnerabilities of three main classic healthcare applications (medical records management, traceability of medicines, and research and clinical trials). We then demonstrated how blockchain technology can effectively address these vulnerabilities. Later, we explored the most common attacks against blockchain technology and discussed suitable mitigation strategies for these attacks in the three main healthcare applications presented. Finally, we discussed how blockchain technology is impacting and transforming the healthcare sector.

References

[1] .Vanin, F.N.d.S.; Policarpo, L.M.; Righi, R.d.R.; Heck, S.M.; da Silva, V.F.; Goldim, J.; da Costa, C.A. A Blockchain-Based End-to-End Data Protection Model for Personal Health Records Sharing: A Fully Homomorphic Encryption Approach. Sensors 2023, 23, 14. https://www.mdpi.com/1424-8220/20/22/6538

[2] . Ali, A.; Al-rimy, B.A.S.; Alsubaei, F.S.; Almazroi, A.A.; Almazroi, A.A. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. Sensors 2023, 23, 6762. https://www.mdpi.com/1424-8220/23/15/6762

[3] . Pilares, I.C.A.; Azam, S.; Akbulut, S.; Jonkman, M.; Shanmugam, B. Addressing the Challenges of Electronic Health Records Using Blockchain and IPFS. Sensors 2022, 22, 4032. https://pubmed.ncbi.nlm.nih.gov/35684652/

[4] . Ismail, L.; Materwala, H.; Hennebelle, A. A Scoping Review of Integrated Blockchain-Cloud (BcC) Architecture for Healthcare: Applications, Challenges and Solutions. Sensors 2021, 21, 3753. https://www.mdpi.com/1424-8220/21/11/3753

[5] . Shahid, A.; Nguyen, T.-A.N.; Kechadi, M.-T. Big Data Warehouse for Healthcare-Sensitive Data Applications. Sensors 2021, 21, 2353. https://www.mdpi.com/1424-8220/21/7/2353

[6] .Ahmed, M.; Dar, A.R.; Helfert, M.; Khan, A.; Kim, J. Data Provenance in Healthcare: Approaches, Challenges, and Future Directions. Sensors 2023, 23, 6495. https://www.mdpi.com/1424-8220/23/14/6495

[7] .Sadhu, P.K.; Yanambaka, V.P.; Abdelgawad, A.; Yelamarthi, K. Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions. Sensors 2022, 22, 5517. https://www.mdpi.com/1424-8220/22/15/5517

[8] .Psarra, E.; Apostolou, D.; Verginadis, Y.; Patiniotakis, I.; Mentzas, G. Context-Based, Predictive Access Control to Electronic Health Records. Electronics 2022, 11, 3040. https://doi.org/10.3390/electronics11193040

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024

[9] .Ktari, J.; Frikha, T.; Ben Amor, N.; Louraidh, L.; Elmannai, H.; Hamdi, M. IoMT-Based Platform for E-Health Monitoring Based on the Blockchain. Electronics 2022, 11, 2314. https://doi.org/10.3390/ electronics11152314

[10] .M. Budman, B. Hurley, A. Khan, and N. Gangopadhyay, "Deloitte's 2019 Global Blockchain Survey," 2019. [Online]. Available: https://www2.deloitte.com/content/dam/insights/ us/articles/2019-global-Blockchain-survey/DI_2019-globalBlockchain-survey.pdf (accessed May 03, 2023).

[11].Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing Blockchains for healthcare," in 2017 Int. Conf. Electr. Comput. Technol. Appl. (ICECTA), Nov. 2017, pp. 1–4. doi: 10.1109/ICECTA.2017.8252043.

[12].P. J. Korsten, "Healthcare rallies for Blockchains: Keeping patients at the center," 2017. [Online]. Available: https:// www.linkedin.com/pulse/healthcare-rallies-Blockchainskeeping-patients-center-korsten/ (accessed May 03, 2023).

[13].S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research," Appl. Sci., vol. 9, no. 9, Art. no. 9, Jan. 2019, doi: 10.3390/app9091736.

[14].G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using Blockchain technology," Sustain. Cities Soc., vol. 39, pp. 283–297, May 2018, doi: 10.1016/j.scs.2018.02.014.

[15].K. Clauson, E. Breeden, C. Davidson, and T. Mackey, "Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare," Blockchain Healthc. Today, vol. 1, Mar. 2018, doi: 10.30953/bhty.v1.20.

[16].G. Carter, D. White, A. Nalla, H. Shahriar, and S. Sneha, "Toward Application of Blockchain for Improved Health Records Management and Patient Care," Blockchain Healthc. Today, vol. 2, Jun. 2019, doi: 10.30953/bhty.v2.37.

[17].J. Frizzo-Barker, P. A. Chow-White, P. R. Adams, J. Mentanko, D. Ha, and S. Green, "Blockchain as a disruptive technology for business: A systematic review," Int. J. Inf. Manag., vol. 51, p. 102029, Apr. 2020, doi: 10.1016/j. ijinfomgt.2019.10.014. [27] H. S. A. Fang, T. H. Tan, Y. F. C. Tan, and C. J. M. Tan, "Blockchain Personal Health Records: Systematic Review," J. Med. Internet Res., vol. 23, no. 4, p. e25094, Apr. 2021, doi: 10.2196/25094.

[18].G. Meyer and F. McCraw,"Healthcare: Blockchain's Curative Potential for Healthcare Efficiency and Quality," Cognizant, 2017> [Online]. Available: https://dokumen.tips/documents/ healthcare-Blockchainas-curative-potential-for-healthcareefficiency-2020-04-05.html (accessed May 03, 2023).

[19].N. Nchinda, A. Cameron, K. Retzepi, and A. Lippman, "MedRec: A Network for Personal Information Distribution," in 2019 Int. Conf. Comput. Netw. Commun. (ICNC), Feb. 2019, pp. 637–641. doi: 10.1109/ICCNC.2019.8685631.

[20].P. Tagde et al., "Blockchain and artificial intelligence technology in e-Health," Environ. Sci. Pollut. Res., vol. 28, no. 38, pp. 52810–52831, Oct. 2021, doi: 10.1007/s11356- 021-16223-0.

[21].M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in 2016 IEEE 18th Int. Conf. e-Health Netw. Appl. Serv. (Healthcom), Sep. 2016, pp. 1–3. doi10.1109/HealthCom.2016.7749510.

[22]R. Yousuf, Z. Jeelani, D. A. Khan, O. Bhat, and T. A. Teli, "Consensus Algorithms in Blockchain-Based Cryptocurrencies," in 2021 Int. Conf. Adv. Electr. Comput. Commun. Sustain. Technol. (ICAECT), Feb. 2021, pp. 1–6. doi: 10.1109/ICAECT49130.2021.9392489.

[23].M. Krichen, M. Lahami, and Q. A. Al–Haija, "Formal Methods for the Verification of Smart Contracts: A Review," in 2022 15th Int. Conf. Secur. Inf. Netw. (SIN), Nov. 2022, pp. 01–08. doi: 10.1109/SIN56466.2022.9970534.

[24].R. Yousuf, D. A. Khan, and Z. Jeelani, Security and Privacy Concerns for Blockchain While Handling Healthcare Data,Florida, USA: CRC Press, 2021.

[25].T. Teli, R. Yousuf, and D. Khan, "Ensuring Secure Data Sharing in IoT Domains Using Blockchain," in Cyber Security and Digital Forensics, M. Ghonge, S. Pramanik,

Doi : https://doi.org/10.54216/JCIM.140104
Received: January 18, 2024 Revised: March 05, 2024 Accepted: May 23, 2024