

Blockchain Technology for Secure Management of Patient Data in Pathology Labs

Isidro Navarro del Valle

Universidad de Salamanca, Spain

Abstract

This research identifies a system that uses blockchain technology in healthcare. This technology enables patients to access their medical records at any time and from any location. Furthermore, patients' health records are uploaded to the blockchain in secret. When a patient consults with a healthcare professional, the authorized entity filters the patient's medical report to remove sensitive information. The research employed primary data analysis to determine the usage of Smart PLS software. The filtered medical data is then saved in an off-chain database, while the data's address gets uploaded to the blockchain along with the patient's pseudo-random identifier. As a result, each patient is assigned many pseudo-random identities. In contrast to previous research, when patients' identities/reports may be connected, the proposed technique does not allow for such a connection. The total analysis indicated a direct and significant correlation between blockchain technology and security management. When a pandemic strikes (such as COVID-19), the proposed technology could be used to broadcast people's health status to certain organizations. During the COVID-19 pandemic, patients must provide documentation of their immunization series before flying overseas or nationally or participating in specific social activities.

Keywords: Block Chain Technology (BCT), Secure Management (SM), Patient Data (PD), Pathology Labs (PL)

Introduction

An organized mechanism by which information is shared among the members of a business infrastructure very transparently. In this phenomenon, all the information is secured in blocks, and all those blocks are arranged in the form of a chain. The main objective of this technology is to inform all members of business infrastructure that have access to that particular thing. This sharing of information is performed with the help of an application. This approach toward essential information is sometimes restricted but only some ofays [1, 2]. Many times, it is permission by the relevant person. Four major types of Blockchain technology are: 1. Public, 2. Private, 3. Hybrid, 4. Consortium. All these types of Blockchain technology have their particular positive and negative aspects. Those specific aspects decide their unique method of usage. These aspects are responsible for making a decision that's which one is better for you. The management of one's assets is the best example of the use of Blockchain technology. In the world of finance, Blockchain plays a very important role. It plays the same role in asset management[3]. Let's consider an example: all those companies based on Blockchain technology and related to energy usage have developed a platform that is all about trading and selling electricity among individuals. All homeowners with solar panels utilize this facility to provide the solar energy produced by the solar panel to their neighbors and charge them. A record that is inflexible and is shared among the business members. In this phenomenon, this facility is provided that all the transactions are recorded and all the assets are tracked within the network of a particular business. In these assets, involved things can be tangible, like those things that can be touched; we can take the example of house, car, cash, and land. Some of those things can be intangible, like those that cannot be touched[4]. We can consider examples of intellectual property, patents, copyright, branding, etc. The main reason Blockchain technology's popularity is its circulating character, limpidity, and protective nature. Blockchain technology proves a good solution to all these problems. During the phase of patient data management, Block chain technology plays a significant role. It

provides security to all sensitive information. Susceptibility and incompetence are also tackled by Blockchain technology in all those traditional data handling methods. If one is looking for an effective solution regarding security, then Blockchain technology is an extremely effective way that can be implied. Just like an insulating network, a new model that is all about privacy is introduced by Blockchain technology[5]. That advanced model plays a significant role in enhancing and protecting data. It utilizes secret writing techniques to verify data vigorously. The working of Blockchain technology is based on administered, public, and nonauthorized frameworks. The distribution of records by Blockchain technology helps a lot in the transfer of data, which is all about patients' medical records, in a secure way. It also enforces the shielding of all the data related to healthcare. It also organizes the chain that is all about the medicine supply. It also aids researchers who work in healthcare in unlocking codes related to genetics. Within the blockchain network, all the information is processed and managed up to the limit of various intersections. This information is inspected by multiple people within that network many times[6]. This peak level and secured transparency are very useful in various healthcare, finance, and supply chain management fields. These departments are mentioned specifically because the data's place of origin is inspected critically in these fields[7]. In recent times, healthcare systems have manipulated Blockchain technology as a well-secure, inflexible source that can record data about the history of patients. It gives surety of protecting all sensitive information but also ensures that all the information will remain unchangeable and can be traced easily. As a result of this surety, all patients and providers trust it. In Blockchain technology, secret writing is utilized and implied to protect data[8]. It has also finished the need for any central person who has any authority. The things that are provided by Blockchain technology are of inherent data integrity and confidentiality type. Several challenges are offered by Blockchain technology when discussing the level of privacy. During the pandemic, as the situation becomes very dramatic, the need for

Blockchain technology becomes essential to lessen and restrict the patients from moving here and there. This restriction was extremely necessary, so the threat of infection among people from patients could be reduced. In the era when things like the Internet of Things were spreading, in this study, we are trying to cover the need for the service of a telemed laboratory in which some clinical exams are tested on patients within a hospital by using technology like the Internet of technology[9]. After this procedure, all the results are transferred to the doctors through the hospital cloud for validity and consultation. The scenario that we are going to discuss is all about the spreading of security of information that is related to patients[10]. This security is possible only with the aid and support of nurses, doctors, and technicians who are all that make sure the transfer of all information of patients to the patient's cloud so that a team can be formed that is virtual and can take care of security issues[11, 12].

Research Objective

The main purpose of the study of Blockchain Technology for Secure Management of Patient Data in pathology labs is to protect patients' information so that it cannot be leaked and patients have no trust issues during their treatment procedure. All the important steps that play a significant role in the protection procedure are also mentioned in it. The research study measures the Blockchain Technology for Secure Management of Patient Data in Pathology Labs. The research paper is divided into five different sections. The first portion describes the introduction and included the objective of the research. The second portion describes the literature review, and the third section presents those methods related to blockchain technology and secure management. The fourth portion represents the result and its description, also the last section also summarized the overall research.

LITERATURE REVIEW

Researchers claim that the need for advanced technology has increased during the COVID-19 pandemic. Since the COVID-19 pandemic, the use of information technology has reduced the interaction between humans. Telemedical-based laboratories around the world use IOT to improve the quality of medical services provided by health systems. Through the telemedicine system, a doctor can examine a patient's medical condition remotely[10]. Studies reveal that data related to a patient medical health condition is critical as it determines patient health. The information associated with patient health is shared with stakeholders of the medical system using technology-based medical devices. IoT-based devices are developed to keep the health-related data of each patient safe with little chance of error. This precise health data helps maintain patients' privacy. To ensure the safe transformation of medical data from medical institutes to stakeholders, different healthcare centres make use of blockchain systems. The blockchain system is an accurate medical framework that is widely used for health-related data management[5]. Researchers explain that remote health data provides new insight related to patient medical conditions. Doctors and patients use technology-based health-related systems because of the immense benefits of remote health systems. Using remote health-related data storage systems ensures no health data is shared with unauthorized institutes. EMRs are kept safe using remote technology systems like deep learning to secure the health-related information of patients[8]. studies claim that the modernization of the world increases the need for data safety and protection. the increase in the number of cybercrime cases has

increased the need for the development of advanced data protection systems. The blockchain system protects Forensic information in most laboratories [3]. Studies suggest that the development of any nation is based on the workings of the healthcare system. The advancement of health systems means improvement in patient data storage systems. Technology-based health data storage programs are built to safeguard the personal information of patients Blockchain technology is one of the advanced medical technologies that use cloud-based programs for saving patient health data with great precision[11]. Studies reveal that blockchain technology is used in most forensic laboratories to optimize forensic-related information about the patient. Forensic laboratories work using the optimized technology of blockchain to enhance the process of their health system[13]. Scholars suggest that to ensure data safety, blockchain technology should be implemented in different fields. data transparency is maintained by the healthcare system using blockchain technology. the centralized healthcare system secures the health data[14]. The use of blockchain technology has advanced the optimization of data management systems in various laboratories. The authentication provided by blockchain technology in the medical profession makes this technology the best technology for efficient data storage[15]. Studies predict that the chances of health data getting corrupted are higher because of errors in health data. Blockchain systems are preferred in laboratories to minimize errors related to health data. Most forensic lab infrastructure uses the patient-centric system to regulate health data. The information associated with the health system is maintained using a cryptographic algorithm. This algorithm has great applications in the medical and health fields[16]. scholars suggest that the present medical system is facing a lot of data management problems. these problems cause more errors in healthcare data, thereby reducing the transparency of healthcare data. These problems are overcome using innovative technology in healthcare laboratories[17]. Studies explain that the advancement in the field of healthcare is rapidly increasing. Despite this advancement, the healthcare system faces many problems related to storage of patient-related data in bulk. to solve this problem a blockchain technology-based framework is employed in most health institutes to store health-related data in bulk. Many laboratories are famous for their biomedical research programs. to efficiently manage the data and results of these programs, the use of blockchain technology is increasing in medical laboratories[18]. Moreover, improving the efficiency of blockchain systems using artificial intelligence holds great importance. The AI system works by optimizing the data related to patient health status. The whole report related to the prescriptions and medical treatment the patient gets during his treatment journey is provided in an optimized manner by using AI in laboratories[19]. Studies suggest that MCPS systems demand higher data security for minimizing the chances of health data alternations. The complex data related to medicine are stored using a secure AI system in laboratories. using blockchain technology, it becomes easier to design a system that works on an algorithm for secure data transmission[20]. The modern blockchain technology-based system uses an IPFS system to store large amounts of health-related data with high accuracy. Through this system, the personal data of patients is fully secured; therefore, the chances of data leakage decrease [21]. Studies of scholars reveal that the majority of patient health records were lost during the covid 19 pandemic due to the inefficiency of the electronic health system. During the pandemic, the inefficiency of the health system was tackled by developing an e-health record system using blockchain technology. The one big advantage of e-health records is that all the information about the medical patient is saved with accurate reports and

results[22]. Also, when a large amount of patient data is shared between medical institutes, the chances of data getting altered increase. For analysing big data related to patients' medical situations, blockchain technology is used in medical health centres. The patient's data is securely saved using blockchain technology-based medical records[23]. Scholars predict that large data transactions related to patient health will be made easier using blockchain technology. Blockchain technology is built to automate the process of data handling and data analyzing. The implementation of blockchain technology in the health sector, especially in medical laboratories, improves the process of the health system[24]. Studies suggest that cloud-based medical technology is used for saving medical records with the help of the blockchain model. This model secures the data and makes it accessible for transmission to other health sectors[25]. Studies show that EHR is a form of electronic data storage that stores the personal medical histories of patients without errors. The EHR is a computerized electronic data format that stores big data with minimal data error chances. Blockchain technology accurately predicts the type of disease a patient is affected with and also tells the mode of disease treatment[26]. Moreover, blockchain technology acts as a novel medical model that secures data for developing a better health or medical industry[27].

Methods

The research determines that Blockchain Technology for the Secure Management of Patient Data in Pathology Labs. The research

was based on primary data analysis to determine the research used Smart PLS software related to variables. Descriptive statistical analysis, and the correlation coefficient analysis also explains the smart PLS Algorithm model between them. Blockchain technology is a decentralized and public digital ledger that keeps the records of transactions among numerous computers. This technology ensures that not even a single piece of data can be altered without modifying the subsequent records. This technology is verified, associated with the previous block, and forms the long chain. Blockchain means the record of transactions.

The blockchain method delivers a good deal of accountability as each transaction is listed and checked widely. When a record is entered in block chain it is not possible to alter the information. Thus, it secures the data without any alteration or modification. In block chain technology data are secured on networks instead of databases in this way data is safer and less prone to be hacked. Block chain technology provides an excellent medium to develop and compete with traditional companies for a business model.

Block chain methods help the vendors to uphold the outline of the medicine-related products. Many health and pharmaceutical centers use block chain technology to get rid of counterfeit medications as it helps in copying all medicines. This will help to find out the cause of falsification and maintain the privacy of the record of the patient when medical history is established. Block chain records cannot be altered and used in the hardware of hospitals due to its decentralized network.



Figure 1: Blockchain

Blockchain technology is an emerging field, and its success depends on the Bitcoin cryptocurrency. Blockchain method has a distributed ledger that provides an unchallengeable, clear history in the network participation (Figure 1). This technology is a new generation method that gained the trust of users, accountability and clarity. Blockchain maintains the privacy of records, and it is considered a cost-effective method. Electronic health record (HER) sharing is important for quick medical care. For example, transition and synchronization for care are important for cancer patients. It is helpful for doctors to make clinical decisions when patient history, tests, diagnosis reports and treatment data are recorded. Patients have an interest in having access to their Electronic Health Records (EHR) history to know about them and also their families get connected and control who can able to realize and use their health evidence. To

improve the quality of health it is recommended to access the history of HER so that patients personalized treatment can be developed. Electronic Health records are very confidential and sensitive; according to some studies, the patient must have access to their health data and they can also decide who will see and access this data. Currently, it is an exciting time for health care and information technology due to advancements in genetic research and the accuracy of medicine. With the help of technology, healthcare researchers find novel strategies for the prevention of diseases and efficient treatment according to an individual own genetic makeup, regime and atmosphere. Additionally, Information technology merges with healthcare technology that produces large databases of health records and provides tools to access health records and engage individuals extra in their healthcare environment. Merging health technology with IT would bring

revolution in the health IT field. Blockchain technology is an advanced technology that has the potential to withstand the challenges that exist in the health IT system and allows healthcare providers, healthcare individuals and medical researchers to secure their electronic data of health. Blockchain stores the digital assets and information, and the network executing the blockchain has the type of information confined to the transaction. The information inserted in the blockchain is encrypted and digitally guaranteed while maintaining legitimacy and correctness. Information is stored in a block and each block comprises of cryptographic hash preceding the block in linear and chronological order. Blockchain method for health care needs to be public and include scientific solutions for constancy, safety and accuracy. One of the advanced examples of blockchain is the cutting-edge technology used in pathology labs. The efforts to standardize the pathology lab and reduce the load of manual work have upsurge over the past few decades. It aims to enhance the digital accuracy and health care outcomes of patients. It is tough to handle the anatomic samples of pathology and it leads to the loss of incorrect data and causes analytic, legitimate and moral consequences. For storing any data there is a need for controlled temperature, humidity and safe traceable systems. From collection to storage, it is important to maintain a safe and controlled chain method for biological samples and maintain value, traceability and alteration. Automation system efforts by improving efficiency and compliance provide automatic labeling, archiving, and search processes advancement in surgical pathology and the health care of patients depends on progressive technologies and standard methods. New technology includes digital pathology approaches to improve diagnostic accuracy, privacy of data and compatibility. The molecular biology field requires precision of results and standardized approaches before execution. Thus, quality assurance and control system play an important role and provide accurate and reliable results. The core responsibility of the pathologist is to maintain the privacy of patient information and diagnoses. Digital technology is a typical approach used in which multiple pathologists and diagnostic programs upload the data from one source. It is important to share the patient's medical information and diagnostic report with the right people. Likewise, the only pathologist who accesses the pathology platform can view the data images, make alternations and make analysis. However, in some cases, the images and slides can also be shared with other pathologists, experts and patients themselves. The patient can be able to remove access to his information from physicians and management. A decentralized

blockchain method is applied to solve all pathology lab-related problems by securing the patient's information. Making the specific sets of related images that are diagnosed by doctors creates uniform data storage. The blockchain method helps in the security and integrity of the patient's data. The data confidentiality of the data means that it is not exposed to others.

Key Features of Blockchain Technology

Blockchain technology is based on a set of distinct qualities that set it apart from traditional databases. The following are its most essential and distinguishing features: 1. Distribution of power and authority to several entities or individuals. Decentralisation is an essential aspect of blockchain technology. Blockchain utilises a distributed ledger to record transactions, in contrast to centralised databases that are managed and certified by a central authority like a bank. Therefore, the ledger is managed, authenticated, and revised by a network of transparent participants referred to as nodes. Every node is dispersed over a network and possesses a complete replica of the whole blockchain. 2. The characteristics of immutability and security. Blockchain employs cryptographic methods to provide strong security, document transactions, and thwart manipulation. Data is stored in interconnected blocks using cryptographic hashes. If someone wishes to tamper with or alter a block, they must change every consecutive block, rendering tampering computationally impossible. This key blockchain security characteristic assures the immutability of information, making blockchain a great platform for storing sensitive data and completing secure transactions. 3. Ensure openness and traceability. The inherent openness of blockchain technology ensures that all network users have access to the same information. For example, each transaction is recorded in a public ledger accessible to all participants. Transparency boosts confidence and network accountability by allowing errors to be recognized and corrected right away. Furthermore, the blockchain's ability to track the origin and transit of assets makes audits easier and reduces the danger of fraudulent activity. 4. Smart contracts. These contracts are automated agreements embedded in software that carry out the terms of the contract automatically. Smart contract programs are stored on the blockchain and execute their operations when certain conditions are met. These contracts eliminate the need for middlemen, simplify transactions, save money, and speed up closings. They are engaged in a variety of industries, including supply chain management, insurance, and banking.

Descriptive Statistical Analysis

Table 1: Result of Descriptive Statistical Analysis

Name	Mean	Median	Scale Min	Scale Max	Standard Deviation	Excess Kurtosis	Skewness	Cramér-Von Mises P Value
BCT1	1.531	1.000	1.000	3.000	0.610	-0.404	0.716	0.000
BCT2	1.551	2.000	1.000	3.000	0.537	-1.139	0.198	0.000
BCT3	1.469	1.000	1.000	3.000	0.538	-0.915	0.530	0.000
SM1	1.490	1.000	1.000	3.000	0.539	-1.002	0.445	0.000
SM2	1.490	1.000	1.000	3.000	0.576	-0.453	0.703	0.000
SM3	1.408	1.000	1.000	3.000	0.531	-0.509	0.803	0.000
SM4	1.510	1.000	1.000	3.000	0.576	-0.554	0.621	0.000
PL1	1.531	1.000	1.000	3.000	0.610	-0.404	0.716	0.000
PL2	1.510	1.000	1.000	3.000	0.610	-0.305	0.794	0.000
PL3	1.306	1.000	1.000	3.000	0.542	1.868	1.633	0.000
PL4	1.469	1.000	1.000	3.000	0.575	-0.329	0.788	0.000
PL5	1.388	1.000	1.000	3.000	0.527	-0.315	0.902	0.000

The results of table 1 the descriptive statistical analysis reveal the mean value, the lowest rate, the maximum rate, as well as the standard deviation rate and probability value of each independent and

dependent variable. BCT1, 2, and 3 are all considered independent variables based on the results, with mean values of 1.531, 1.551, and 1.469. All of them have positive average rates. The standard deviation

rate is 61%, with 53% deviating from the mean value. The results show that the skewness value is 71%, with a 19% skewness rate between them. According to the results, SM1,2,3, and 4 are considered mediator variables, and the mean values are 1.490, 1.408, and 1.510.

There is now a positive average rate. The standard deviation value is 53%, indicating a 57% departure from the mean value. According to the descriptive statistic, PL1,2,3,4, and 5 are all considered as dependent variables, with average rates of 1.510, 1.306, 1.469, and 1.388, respectively. The standard deviation rate is 61%, 54%, 57%, and 52% away from the mean value. According to the results, the aggregate significant value is 0.000, indicating a 100% significance rate between them.

Resources

Pathologists and laboratory professionals in charge of patient data privacy and security should have access to the following helpful resources. 1. Checklists for laboratory accreditation by the College of American Pathologists (CAP). These checklists contain a unique section for laboratory computer services that covers all important features of LISs and laboratory computer services, such as patient data protection and security. Furthermore, particular requirements for

telepathology services in terms of patient data confidentiality and security are discussed. 2. The Centres for Medicare and Medicaid Services provided instructional resources and recommendations on HIPAA compliance, privacy and security, and health insurance reform. 3. CLSI provides technical standards and implementation techniques for securing in vitro diagnostic (IVD) systems, including devices, analytical equipment, and data management systems, placed in healthcare organisations. The AUTO11-A-IT Security of IVD Instruments and Software Systems document is designed for suppliers, users (for example, laboratory workers), and healthcare organisations' IT management. 4. The International Society of Blood Transfusion's Information Security Task Force released standards for ensuring information security in transfusion medicine. These rules cover the application of HIPAA Security Standards in Transfusion Medicine. The results shown in table 2 illustrate that correlation coefficient analysis between variables, including dependent and independent variables, reveals both negative and positive interrelationships. Pathology informaticists must ensure that patient data in the pathology laboratory remains discreet and secure, ideally in partnership with their information services division. As a result, informaticists must be aware of the pathology laboratory's security dangers and privacy rules, as well as the potential technology solutions to solve these issues

Correlation Coefficient

Table 2: Result of Correlation Coefficient

	BCT1	BCT2	BCT3	SM1	SM2	SM3	SM4	PL1	PL2	PL3	PL4	PL5
BCT1	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
BCT2	-0.020	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
BCT3	0.112	-0.330	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
SM1	0.079	0.407	-0.159	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
SM2	-0.159	-0.345	0.180	-0.576	1.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
SM3	-0.102	0.428	-0.527	0.086	-0.186	1.000	0.000	0.000	0.000	0.000	0.000	0.000
SM4	0.101	0.345	0.149	0.115	-0.200	-0.014	1.000	0.000	0.000	0.000	0.000	0.000
PL1	-0.154	0.042	0.236	0.079	-0.159	0.024	0.043	1.000	0.000	0.000	0.000	0.000
PL2	-0.179	-0.111	-0.108	-0.325	0.160	-0.076	-0.160	-0.015	1.000	0.000	0.000	0.000
PL3	0.003	-0.229	0.137	-0.094	-0.023	-0.150	-0.043	0.003	-0.102	1.000	0.000	0.000
PL4	0.279	0.088	0.079	0.312	-0.386	0.041	0.016	0.105	-0.043	-0.264	1.000	0.000
PL5	0.058	-0.106	0.221	0.265	-0.289	-0.128	-0.047	0.439	-0.107	0.299	0.140	1.000

Smart PLS Algorithm Model

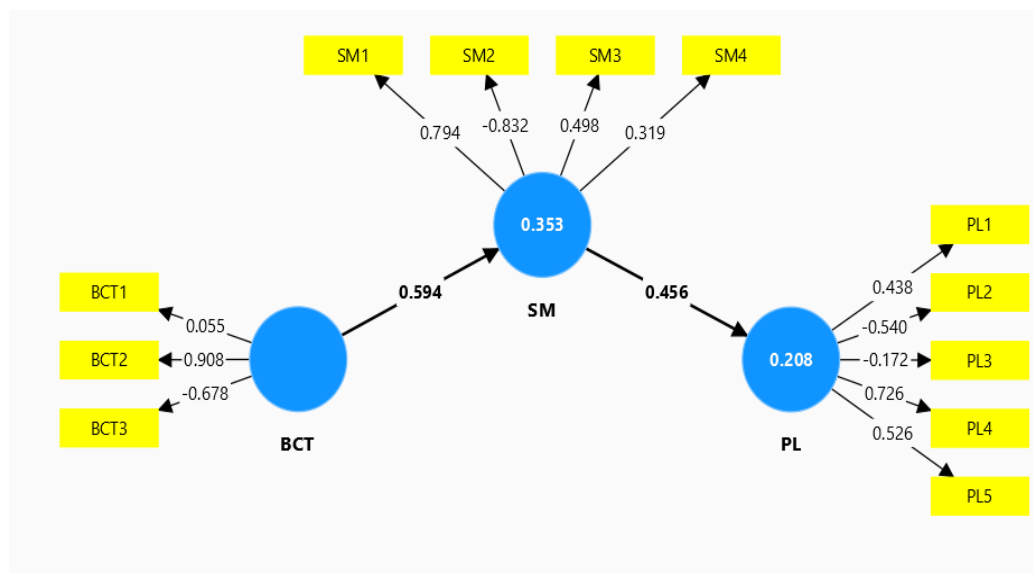


Figure 2: Smart PLS Algorithm Model

The above model of figure 2 is smart PLS Algorithm model its shows relation between BCT, SM and PL according to the above model

BCT shows that 0.055, 0.908 and -0.678 shows 5%, 90% and 67% significantly rate between them. the SM shows that 79%, 83%, 49% and

31% positive and significant relation according to the result its shows 59% positive and significant link in between BCT and SM. The PL describe that 45% positive and significant relation between them.

Conclusion

Traditional database methods provide several challenges for collecting financial activities. Consider selling a property. Once the money is exchanged, the buyer acquires ownership of the property. The buyer and seller can record monetary transactions individually, but neither is reliable. The vendor can easily claim that they did not get the money when they did, and the buyer might claim that they did not pay when they received it. To avoid legal problems, a reputable third party must monitor and approve transactions. The existence of this central authority complicates the transaction by introducing a single point of risk. If the central database becomes hacked, both parties may suffer. Blockchain solves these issues by providing a decentralised, tamper-proof framework for recording transactions. The research was based on primary data analysis to identify the research study, which employed smart PLS software to create useful results such as descriptive statistics and correlation coefficients to describe the clever PLS Algorithm model between them. In the case of a real estate transaction, blockchain generates a single ledger for both buyers and sellers. All transactions require both party's consent and are automatically recorded in both ledgers in real-time. Any inaccuracies in prior

transactions will affect the entire ledger. These qualities of blockchain technology have led to its adoption in a variety of industries, including the development of digital currencies like Bitcoin. Given that pathology laboratories manage a high number of patient data for clinical and maybe research purposes, data protection and security rules and procedures are essential. Contemporary pathology laboratories must handle security concerns as their information systems and workstations become more connected to the Internet, as well as meet the need for wireless and mobile device connectivity. Maintaining HIPAA and HITECH compliance is critical for labs, especially in the US.

The most current modifications to the HIPAA Privacy and Security Rules were announced in January 2013 and took effect on March 26, 2013. They enacted HITECH, tightened privacy safeguards under the Genetic Information Nondiscrimination Act, and made several measures, most notably impacting BAs. According to recent reforms, BAs may now face immediate civil fines if proven to have violated privacy or security. Nowadays, LISs are rarely used for data retrieval or reference (except by actual, core laboratory professionals). Laboratory data is routinely uploaded to multiple Electronic Medical Records, and even if the LIS is the most secure environment, there is still a chance that the data may be compromised due to systems beyond the laboratory's control. As a result, the company must make a complete and unalterable commitment to protecting sensitive health data.

References

- [1] M. Faisal, H. Sadia, T. Ahmed, and N. Javed, "Blockchain technology for healthcare record management," *Pervasive Healthcare: A Compendium of Critical Factors for Success*, pp. 255-286, 2022.
- [2] E. Ahmet and E. Adem, "The Impact of Laboratory Accreditation in Patient Safety and Quality Care," *J Bras Patol Med Lab*, vol. 59, pp. 16-23, 2023.
- [3] S. Patil, S. Kadam, and J. Katti, "Security enhancement of forensic evidences using blockchain," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, 2021: IEEE, pp. 263-268.
- [4] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustworthy electronic medical records sharing using blockchain," in *AMIA annual symposium proceedings*, 2017, vol. 2017: American Medical Informatics Association, p. 650.
- [5] A. K. Jakhar, M. Singh, R. Sharma, W. Viriyasitavat, G. Dhiman, and S. Goel, "A blockchain-based privacy-preserving and access-control framework for electronic health records management," *Multimedia Tools and Applications*, pp. 1-35, 2024.
- [6] H. Subramanian and S. Subramanian, "Improving diagnosis through digital pathology: Proof-of-concept implementation using smart contracts and decentralized file storage," *Journal of medical Internet research*, vol. 24, no. 3, p. e34207, 2022.
- [7] H. Jennath, V. Anoop, and S. Asharaf, "Blockchain for healthcare: securing patient data and enabling trusted artificial intelligence," 2020.
- [8] S. Saif, S. Biswas, and S. Chattopadhyay, "Intelligent, secure big health data management using deep learning and blockchain technology: an overview," *Deep Learning Techniques for Biomedical and Health Informatics*, pp. 187-209, 2020.
- [9] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," *Multimedia Tools and Applications*, vol. 79, no. 15, pp. 9711-9733, 2020.
- [10] A. Celesti, A. Ruggeri, M. Fazio, A. Galletta, M. Villari, and A. Romano, "Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds," *Sensors*, vol. 20, no. 9, p. 2590, 2020.
- [11] M. Gupta, R. Jain, M. Kumari, and G. Narula, "Securing healthcare data by using blockchain," *Applications of blockchain in healthcare*, pp. 93-114, 2021.
- [12] J. K. Bonifacio-Mundaca, G. C. Ramirez-Ubillus, and V. Z. Mechán-Mendez, "Immature platelets and reticulocytes fractions as a predictor of hematopoietic stem cell implantation," *J Bras Patol Med Lab*, vol. 59, pp. 1-6, 2023.
- [13] S. M. Tiwari, S. B. Dubey, N. Lal, and A. Tripathi, "Digital Support of Forensic Laboratories under Optimized Block Chain Network," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, 2021: IEEE, pp. 258-262.
- [14] M. Swetha, S. Pushpa, M. Muneshwara, and T. Manjunath, "Blockchain enabled secure healthcare Systems," in *2020 IEEE International Conference on Machine Learning and Applied Network Technologies (ICMLANT)*, 2020: IEEE, pp. 1-6.
- [15] K. Misztal, T. Szulczek, and A. Kubica-Misztal, "Securing Data of Biotechnological Laboratories Using Blockchain Technology," in *International Conference on Computer Information Systems and Industrial Management*, 2020: Springer, pp. 88-96.
- [16] S. M. Idrees, I. Aijaz, P. Agarwal, and R. Jameel, "Blockchain-based smart and secure healthcare system," in *Transforming cybersecurity solutions using Blockchain*. Springer, 2021, pp. 165-183.
- [17] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Computing and Applications*, pp. 1-16, 2022.
- [18] M. T. Alam and K. Raza, "Blockchain technology in healthcare: making digital healthcare reliable, more accurate, and revolutionary," in *Translational Bioinformatics in Healthcare and Medicine*. Elsevier, 2021, pp. 81-96.
- [19] V. Chamola, A. Goyal, P. Sharma, V. Hassija, H. T. T. Binh, and V. Saxena, "Artificial intelligence-assisted blockchain-based framework for smart and secure EMR management," *Neural Computing and Applications*, vol. 35, no. 31, pp. 22959-22969, 2023.
- [20] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, "Design of a secure medical data sharing scheme based on blockchain," *Journal of medical systems*, vol. 44, no. 2, p. 52, 2020.

- [21] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," *Journal of Parallel and distributed computing*, vol. 164, pp. 152-167, 2022.
- [22] B. Mallikarjuna, D. Kiranmayee, V. Saritha, and P. V. Krishna, "Development of efficient e-health records using iot and blockchain technology," in *ICC 2021-IEEE International Conference on Communications*, 2021: IEEE, pp. 1-7.
- [23] V. S. Marichamy and V. Natarajan, "Blockchain based securing medical records in big data analytics," *Data & Knowledge Engineering*, vol. 144, p. 102122, 2023.
- [24] E. Saha, P. Rathore, and A. Gigi, "Utilizing blockchain technology to manage functional areas in healthcare systems," in *The Big Data-Driven Digital Economy: Artificial and Computational Intelligence*. Springer, 2021, pp. 125-139.
- [25] S. Sharma, A. Mishra, and D. Singhai, "Secure cloud storage architecture for digital medical record in cloud environment using blockchain," in *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, 2020.
- [26] K. Shruthi and A. Poomima, "Medical Data Asset Management and an Approach for Disease Prediction using Blockchain and Machine Learning," *International Journal of Engineering Trends and Technology*, vol. 71, no. 4, pp. 491-514, 2023.
- [27] A. A. Khan *et al.*, "Healthcare ledger management: A blockchain and machine learning-enabled novel and secure architecture for medical industry," *Hum. Cent. Comput. Inf. Sci*, vol. 12, p. 55, 2022.



This is an open-access article distributed under the terms of the Creative Commons Attribution License.