Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-02 | June-2023

Build A Secure Healthcare System Based On the Metadata of Patient Information

Moatasem Mohammed Saeed Naji[1], Dr. Hayder A. Nahi[2]
[1,2]Computer Center, Al-Qasim Green University, Iraq.
haider.satar@uoqasim.edu.iq

DOI: 10.5281/zenodo.8239516

ABSTRACT

Building a secure healthcare system based on metadata involves several key steps to ensure that patient information remains confidential and secure. Metadata refers to information about data, such as the time and date of creation, author, and location, rather than the content of the data itself. In this paper, there are many steps that considered when building a secure healthcare system based on metadata: we begin with defining metadata standards: Establishing metadata standards for healthcare data can help ensure consistency and interoperability across different systems. This can include standards for data elements, data formats, and data models. Implement access controls: Access controls should be implemented to restrict access to sensitive patient data. Role-based access control can be used to limit access to specific data based on job responsibilities. Use encryption: Encryption can be used to protect patient data from unauthorized access. Data encryption should be implemented at rest and in transit to protect data at all times. Secure storage: Patient data should be stored securely, including backups and archives. Secure storage can help prevent data loss and unauthorized access. We obtain a perfect time for processing compare with other resources and perfect time for check the metadata and hyperlink of patient's information**.**

Keywords: Metadata; health-data security; healthcare system; hyperlink; EMR.

Cite as: Moatasem Mohammed Saeed Naji, Dr. Hayder A. Nahi. (2023). Build A Secure Healthcare System Based On the Metadata of Patient Information. *LC International Journal of STEM (ISSN: 2708-7123), 4*(2), 15–24. https://doi.org/10.5281/zenodo.8239516

INTRODUCTION

The healthcare system refers to the network of organizations, institutions, and individuals involved in providing healthcare services to people in a given area or country [1]. This includes hospitals, clinics, doctors, nurses, pharmacists, and other healthcare professionals. The healthcare system can be divided into different levels of care, such as primary care (where people receive basic medical care and preventive services), secondary care (specialist medical care provided by hospitals and clinics), and tertiary care (highly specialized medical care, such as surgery and intensive care) [2].

The healthcare system is usually financed via a variety of public and private sources [3], with the purpose of supplying inexpensive and affordable healthcare to all partners of the people. Yet, entrance to healthcare can differ relying on characteristics such as payment, place, and insurance coverage. Efforts are constantly being made to enhance the healthcare system, such as via the benefit of technology to enhance efficiency, decrease expenses, and security, and via the growth of unique medicines and therapies to enhance patient consequences [4].

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-02 | June-2023

An Electronic Medical Record (EMR) is a digital understanding of a patient's medical record, including details like medical requirements, therapies, drugs, allergies, and additional appropriate details. EMRs are created to be available to healthcare providers, allowing them to efficiently access and communicate patient data to enhance care coordination, decrease medical mistakes, and enhance patient security [15]. EMRs can be accessed by licensed healthcare providers from various places, constructing it more comfortable for them to cooperate and supply coordinated care to patients. Can even be utilized to develop reports and analytics, permitting healthcare institutions to determine trends and patterns in patient care, observe the efficacy of medicines, and enhance the general quality of care [16].

A secure healthcare system guarantees the confidentiality, integrity, and availability of healthcare data and patient details [5]. The healthcare enterprise works with sensitive and private information, such as medical records, economic data, and unique identifiers, constructing it as an excellent target for cyberattacks and data breaches [6]. A secure healthcare system should execute reasonable standards to guard the privacy and security of patient data and control unauthorized access, theft, or loss of data.

The are some key components of a secure healthcare system may include: Strong access controls, ensuring that only authorized individuals have access to sensitive data and information. Encryption, encrypting data to prevent unauthorized access and ensure the confidentiality of information [8]. Regular audits and assessments, regularly conducting security assessments to identify vulnerabilities and address them proactively [9]. Disaster recovery and business continuity planning, having a plan in place to ensure that critical data and systems can be restored quickly in the event of a disaster or system failure [10]. Employee training and awareness, ensuring that employees are trained on security best practices and are aware of the risks associated with handling sensitive data [11]. By implementing these measures and other appropriate security protocols, healthcare systems can help protect patient data and maintain the trust of their patients. Additionally, may analyses the contain of the information of records (metadata) to protect the system of patina data.

Metadata is data that provides information about other data [12]. It can include information such as the author, date created, date modified, file type, file size, and other characteristics of a piece of data. Metadata is used in many different contexts, including in digital media, where it can be used to organize, search, and manage large collections of files [13]. However, may be utilized in scientific investigation, where metadata can supply essential details about the approaches and outcomes of the research. Metadata can be stored in different formats, including XML, JSON, and RDF [14].

Metadata in a healthcare system typically refers to information that describes various aspects of clinical data. This can include details such as the source, type, format, and structure of the data, as well as information about how the data is processed, stored, and accessed.

Examples of metadata in a healthcare system might include:

- Patient demographic data, such as age, gender, and medical history
- Medical imaging metadata, such as the type of scan, the date it was taken, and the equipment used
- Laboratory test metadata, such as the type of test, the date it was performed, and the laboratory where it was processed

Electronic health record (EHR) metadata, such as the date and time of a patient encounter, the provider who treated the patient, and the type of Metadata is important in healthcare systems because it provides context and structure to the data, which can help ensure that it is accurate, consistent, and easy to use. Metadata can also be used to facilitate data sharing and interoperability between different healthcare systems, which can be critical for improving patient outcomes and reducing healthcare costs.

In this paper, we present a new method for examining the information entered into the health care system and analyzing its content if it is appropriate or not. As it is known, most attacks come through hyperlinks. Therefore, after analyzing the content of the patient's information, we examine the information through a specific browser to check if there is a link that contains dangerous implicit information. After accessing the data source, it is compared with the imposed condition. If it conforms

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-02 | June-2023

to the protection conditions, it is stored in a database. Data otherwise rejected as patient information service provided.

The numbering of section and sub-section is following on this template. Sizes and styles of page setup shown in this below. The example of table and figure also shown in this below.

LITERATURE REVIEW

To ensure that the information is accurate and with the patient's consent, the signature is validated. After that, a consensus procedure would be used to decide which accounting node would send the secure information to the cloud while simultaneously writing the data's destination and describe to the blockchain [17].

A prototype for exchanging data utilizing Amazon cloud computing was already developed and put into practice on a portable device. This application combines the blockchain technology and the decentralized Interplanetary File System (IPFS).The efficiency of the created mobile application for Android has been shown on the Ethereum platform. The e-healthcare system was created using an Ethereum blockchain. Like Bitcoin, Ethereum is a modern distributed blockchain technology. The most noteworthy feature of Ethereum is its flexibility and flexibility, which may be leveraged to create a blockchain-based application [18].

Moreover, a not publicly accessible network avoids the drawbacks of public blockchain, including their high levels of energy use, increase or decrease in performance, and transactional throughput is low [19]. [20] provides a careful study on the examination of privacy and security concerns when employing suitable technology in the healthcare industry. Wearable healthcare gadgets have been created and constructed specifically for this survey in order to gather patient health-related data. The patient's health status can be determined by examining this data. This survey used a crosssectional technique as its methodology. Several people who participated in this survey provided data. Among those, 50% of respondents were unaware of the privacy issue with healthcare data.

A brand-new method for sharing personal health records that uses blockchain technology to verify data integrity has been put into place [21]. This plan attempts to address problems that remained in the sharing of healthcare records, such as privacy disclosure, the restriction of keyword searches, and the losing of access control rights for releasing medical information.

In [22], a Decentralized Application (DApp) framework implementation leveraging a permission networks blockchain technology network's backend Distributed File System (DFS) is presented.

Based on an investigation of socio-technical troubles with Healthcare Information Management Systems (HIMS), it was discovered that there are issues with lack of privacy, absence of data translucency, integrity, lacking privacy, and security mistakes in the supply chain and medicine of medications, and a shortage of understanding interpretation. Also, this evaluation offers potential blockchain-based solutions for problems with identity and threat administration, auditing characteristics, and privacy with security jointly. Also, it offers some suggestions for further HIMS study and development [23].

There is a strategy aims to enhance organization-to-organization interoperability in support of the Nationwide Interoperability Roadmap and national healthcare distribution priorities the same as Patient-Centered Outcomes Research (PCOR), as well as to come up with an approach for privacy-preserving healthcare predictive modeling via a distributed application architecture network such as bitcoin and other cryptocurrencies [24].

METHODOLOGY

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-02 | June-2023

This section contains the methodology utilized in this work and the proposed method based on metadata of the patients' information. we began with building a healthcare system that receives patient information as a string, then analysed the information to get secure records. “Fig. 1”, shows the procedure flow of the suggested framework for healthcare metadata storage and check from hyperlink attack.

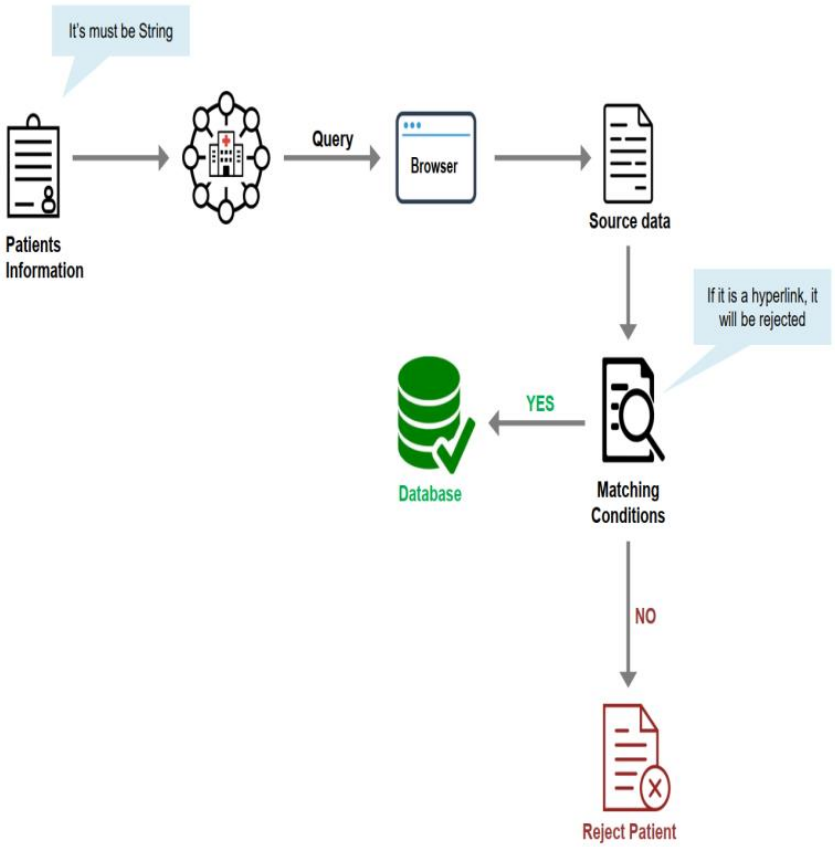

Figure 1. Proposed framework

from the above procedure can extract the steps concerned with the flow and storage of patient’s information and private data are presented below:

Step 1: Designing a comprehensive healthcare system requires careful planning and consideration of many factors, including the needs of the population, available resources, and existing infrastructure. Here are some steps to build a healthcare system.

1. Conduct a Needs Assessment: Conduct a comprehensive assessment of the healthcare needs of the population. Identify the health problems that need to be addressed, such as chronic diseases, infectious diseases, and maternal and child health.
2. Develop a Healthcare Plan: Based on the assessment, develop a healthcare plan that outlines the goals, objectives, and strategies for addressing the identified health issues. The plan should also address resource allocation and financing mechanisms for the healthcare system.
3. Establish Healthcare Infrastructure: Establish a healthcare infrastructure that includes hospitals, clinics, and primary care centers. Develop a plan to ensure that these facilities are equipped with the necessary medical equipment, supplies, and trained staff.
4. Develop a Healthcare Workforce: Design a healthcare force that contains physicians, nurses, and additional healthcare specialists. Establish training programs and professional development

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-02 | June-2023

opportunities to guarantee that healthcare workers have the essential talents and proficiency to supply high-quality care.

5. Found Healthcare Financing Programs: Found financing to guarantee that healthcare services are available and inexpensive to all members of the population.
6. Design Healthcare Policies: Design healthcare procedures that enable the delivery of high-quality care and address problems such as patient protection, medical principles, and quality advancement.
7. Observe and Evaluate the Healthcare System: Design a strategy or techniques for controlling and evaluating the healthcare system to guarantee that it is meeting the needs of the population and achieving its goals.

Step 2: Information documents the system via different input channels, such as sensors, or data feeds.

Step 3: Review the content of information through the browser to analyze the metadata of a hyperlink that typically possesses the following.

1. URL (Uniform Resource Locator): Address of the web page or file that the hyperlink indicates to.
2. Anchor text: This is the clickable text that appears as the hyperlink on the page.
3. Title attribute: The optional feature that supplies further details about the hyperlink when the mouse cursor drifts above it.
4. Rel attribute: Defines the association between the existing document and the linked document.
5. Target attribute: Specifies the frame in which the linked document ought to open.
6. Type attribute: Specifies the kind of file that the hyperlink indicates, such as an image.
7. Language attribute: Specifies the language of the linked document.
8. Class attribute: Refers a class name for the hyperlink, which utilized to style it with CSS.
9. ID attribute: Indicates a unique identifier for the hyperlink, which utilized to reference it with JavaScript.

A hyperlink check algorithm is a process utilized to confirm the reality and integrity of hyperlinks on a web page. This algorithm generally implicates the subsequent steps.

1. Parsing: The algorithm parses the HTML code of the web page to identify all the hyperlinks present.
2. Retrieval: The algorithm retrieves the content of each hyperlink by sending HTTP requests to the corresponding URLs.
3. Status code check: The algorithm checks the HTTP status code of the response received for each URL. If the status code indicates an error (e.g., 404 Not Found), the link is considered broken.
4. Content check: The algorithm might check the content of the retrieved page to guarantee that it compares to the desired content. For instance, if a hyperlink is considered to show a PDF file, the algorithm may verify that the retrieved content is really a PDF file.
5. Recursion: The algorithm may recursively follow links on the retrieved pages to check their validity as well.
6. Reporting: The algorithm generates a report that summarizes the status of each hyperlink on the web page, indicating whether it is valid or broken.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-02 | June-2023

Step 4: uses the requests library to check if a hyperlink returns a valid status code as in below Algorithm (1):

Algorithm 1, check a hyperlink

Input : text: string
Output: Boolean referring if a URL was detected in the text or not

1. Import the "re" module for regular expression operations.
2. Collect a regular expression design for URLs utilizing the "re.compile" function and hold it in a variable called "url_pattern".
3. Use the "search" method of the "url_pattern" object to search for a match in the "text" parameter.
4. If a match is found, store it in a variable called "match", otherwise store "None".
5. Convert the value of "match" to a boolean using the "bool" function and return it

.

Step 5: Extract source data based on step (4).
Step 6: Compare the result from step (5) with conditions then save in the database.

RESULT AND DISCUSSION

Secure Healthcare System

A secure healthcare system can help protect patient data from various types of security threats, including cyberattacks, data breaches, and unauthorized access Table (1). This can lead to better patient outcomes, improved patient safety, and increased trust and confidence in the healthcare system.

Table 1. Results of a secure healthcare system.

Results of a secure healthcare system	Benefits for healthcare providers	Benefits for patients
Protection of patient data	Avoid data breaches and protect sensitive patient information	Ensure privacy and confidentiality of personal health information
Improved patient safety	Reduce the risk of errors and adverse events, and improve the overall quality of care	Experience better health outcomes and avoid medical errors
Better compliance with regulations	Avoid costly fines and penalties for non-compliance with regulations such as HIPAA and GDPR	Have confidence that their personal health information is being protected according to legal requirements
Increased trust and confidence	Build trust and loyalty with patients and improve patient satisfaction	Feel more comfortable sharing personal health information and engaging in healthcare decisions
Cost savings	Reduce the risk of data breaches and other security incidents, which can result in significant cost savings	Avoid the financial and emotional costs of medical errors and adverse events

Generally, a secure healthcare system can have significant benefits for both healthcare providers and patients, including improved patient outcomes, better compliance with regulations, increased trust and confidence, and cost savings.
The time depleted for the access of information of patients in a database utilizing the suggested system is compared with current single database systems and the outcome has been illustrated in“Fig. 2”,

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-02 | June-2023

Single Database

In a single database, the patient information ought to be held in a cloud as centralized storage. The patient that necessarily arrival to its records should present an EHR demand to the cloud where it's taken time is stated as *x*. Then, after obtaining the EHR demand, explore all of the detailed records and then send the content to the patient when it's taken time shall state as *y*. Therefore, the time depleted for records retrieval is computed based on the below "(1)",

$$\text{Depleted Time(sec)}=y-x \qquad (1)$$

The outcomes demonstrate that in a single database, the time depleted is more elevated than that of the proposed system approach which has been demonstrated in "Fig. 2".

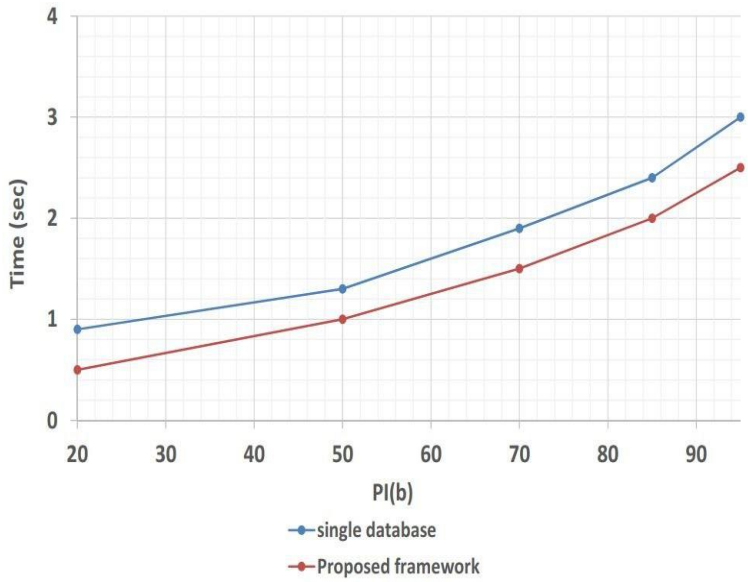

Figure 2. Comparison of depleted time between single database and Suggested Framework.

Table 2 compares the attributes of the proposed technique with those of a few other alternatives. The comparison obviously demonstrates that the suggested approach outperforms the currents approach and may supply a unassailable and protected way to store and share patient information in electronic health records based on various network types.

Table 2,Proposed framework comparison with some existing approaches.

Characteristic	[25]	[26]	[27]	[28]	Suggested System
Authentication	Y		Y	Y	Y
Access	Y			Y	Y
Policy	Y	Y	Y	Y	Y
Integrity	Y	Y	Y	Y	Y
Availability		Y		Y	Y
Resilience and Perseverance		Y			Y

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-02 | June-2023

Increase the Security

Specific strategies have been relied upon to increase the security of the system

- **Encryption:** Utilized encryption to safeguard sensitive patient information, like medical records and identifying information. This enables the encryption of data at repose, and transmission, in addition to mobile devices. Through the equation (2) below we were able to check the effectiveness of encryption.

$$\text{Impact of Encryption} = (EE + R + I + PD + C) / 5 \qquad (2)$$

Where :
EE: Effectiveness of Encryption (strength of Encryption) , *R*: Reduction in Security Breaches and Data Loss (the Predictable decrease in the number of security violations). , *I:* Improvement in Patient Trust and Confidence(Predictable improvement). , *PD:* Protection of Sensitive Patient Data. , *C*: Compliance with Industry Regulations (the degree to which the encryption solution satisfies).

- **Multi-factor authentication:** Executed to prevent unauthorized access to the information of the system. This allows a variety of passwords, security passes, and biometric authentication. Through the equation (3) below we were able to check the effectiveness of Multi-factor authentication.

$$\text{Impact of Multi-factor Authentication} = (EMA + R + I + MR) / 4 \qquad (3)$$

Where:
EMA: Effectiveness of Multi-factor Authentication. , *R*: Reduction in Security Breaches and Data Loss., *I:* Improvement in Patient Trust and Confidence., MR: Management of Risk.

The below Table (3) indicted the corresponding result of encryption and multi-factor authentication on the security of a proposed system.

Table 3. Comparison between encryption and multi-factor authentication on the security

Security Strategy	Effectiveness	Reduction in Security Breaches and Data Loss	Improvement in Patient Trust and Confidence	Protection of Sensitive Patient Data	Compliance with Industry Regulations	Impact
Encryption	9	8	7	9	10	8.6
Multi-factor authentication	8	9	8	8	9	8.3

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-02 | June-2023

CONCLUSION

A secure healthcare system is critical for protecting patients' confidential information and ensuring that their medical records are safe from unauthorized access or theft. The importance of security in healthcare cannot be overstated, as medical data breaches can lead to serious consequences, including identity theft, financial loss, and harm to patient health. In this paper, we proposed a new approach to protect systems of healthcare from hyperlinks attacks based on the metadata of patient's information that used as input information. We obtain a perfect system and model based on many sides such as authentication, access and policy.

REFERENCES

[1] Wendt, C., Frisina, L., & Rothgang, H. (2009). Healthcare system types: a conceptual framework for comparison. Social Policy & Administration, 43(1), 70-90.

[2] Starfield, B., Shi, L., & Macinko, J. (2005). Contribution of primary care to health systems and health. The milbank quarterly, 83(3), 457-502.

[3] Tuohy, C. H., Flood, C. M., & Stabile, M. (2004). How does private finance affect public health care systems? Marshaling the evidence from OECD nations. Journal of health politics, policy and law, 29(3), 359-396.

[4] Figueras, J., Robinson, R., & Jakubowski, E. (2005). Purchasing to improve health systems performance. McGraw-Hill Education (UK).

[5] Chakraborty, S., Aich, S., & Kim, H. C. (2019, February). A secure healthcare system design framework using blockchain technology. In 2019 21st International Conference on Advanced Communication Technology (ICACT) (pp. 260-264). IEEE.

[6] Ghafur, S., Grass, E., Jennings, N. R., & Darzi, A. (2019). The challenges of cybersecurity in health care: the UK National Health Service as a case study. The Lancet Digital Health, 1(1), e10-e12.

[7] Herbek, S., Eisl, H. A., Hurch, M., Schator, A., Sabutsch, S., Rauchegger, G., ... & Repas, S. (2012). The Electronic Health Record in Austria: a strong network between health care and patients. European Surgery, 44, 155-163.

[8] Anand, A., Singh, A. K., Lv, Z., & Bhatnagar, G. (2020). Compression-then-encryption-based secure watermarking technique for smart healthcare system. IEEE MultiMedia, 27(4), 133-143.

[9] Zingg, W., Holmes, A., Dettenkofer, M., Goetting, T., Secci, F., Clack, L., ... & Pittet, D. (2015). Hospital organisation, management, and structure for prevention of health-care-associated infection: a systematic review and expert consensus. The Lancet Infectious Diseases, 15(2), 212-224.

[10] Mansoori, B., Rosipko, B., Erhard, K. K., & Sunshine, J. L. (2014). Design and implementation of disaster recovery and business continuity solution for radiology PACS. Journal of digital imaging, 27, 19-25.

[11] Popa, I., Ştefan, S. C., Morărescu, C., & Cicea, C. (2018). Research regarding the influence of knowledge management practices on employee satisfaction in the Romanian healthcare system. Amfiteatru Economic, 20(49), 553-566.

Logical Creations Education Research Institute
LC INTERNATIONAL JOURNAL OF STEM
E-ISSN: 2708-7123
Web: www.lcjstem.com | Email: editor@lcjstem.com
Volume-04 | Issue-02 | June-2023

[12] Baca, M. (Ed.). (2016). Introduction to metadata. Getty Publications.

[13] Millerand, F., & Bowker, G. C. (2009). Metadata standards. Standards and their stories: How quantifying, classifying, and formalizing practices shape everyday life, 149-165.

[14] Haider, N., & Hossain, F. (2018). CSV2RDF: Generating RDF data from CSV file using semantic web technologies. Journal of Theoretical and Applied Information Technology, 96(20), 6889-6902.

[15] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). Ieee.

[16] Bertino, E., Deng, R. H., Huang, X., & Zhou, J. (2015). Security and privacy of electronic health information systems. International Journal of Information Security, 14, 485-486.

[17] Wang, H., & Song, Y. (2018). Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. Journal of medical systems, 42(8), 152.

[18] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure ehrs sharing of mobile cloud based e-health systems. IEEE access, 7, 66792-66806.

[19] Ismail, L., Materwala, H., & Zeadally, S. (2019). Lightweight blockchain for healthcare. IEEE Access, 7, 149935-149951.

[20] Cilliers, L. (2020). Wearable devices in healthcare: Privacy and information security issues. Health information management journal, 49(2-3), 150-156.

[21] Wang, S., Zhang, D., & Zhang, Y. (2019). Blockchain-based personal health records sharing scheme with data integrity verifiable. IEEE Access, 7, 102887-102901.

[22] Linn, L. A., & Koo, M. B. (2016, September). Blockchain for health data and its potential use in health it and health care related research. In ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST (pp. 1-10).

[23] Khatoon, A. (2020). A blockchain-based smart contract system for healthcare management. Electronics, 9(1), 94.

[24] Litchfield, A., & Khan, A. (2019). A review of issues in healthcare information management systems and blockchain solutions. In International Conference on Information Resources Management (Vol. 1). Association for Information Systems (AIS).

[25] Ying, Z., Wei, L., Li, Q., Liu, X., & Cui, J. (2018). A lightweight policy preserving EHR sharing scheme in the cloud. IEEE Access, 6, 53698-53708.

[26] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017, October). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC) (pp. 1-5). IEEE.

[27] Ramani, V., Kumar, T., Bracken, A., Liyanage, M., & Ylianttila, M. (2018, December). Secure and efficient data accessibility in blockchain based healthcare systems. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 206-212). IEEE.

[28] Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE access, 5, 14757-14767.