IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

STUDY ON MEDICAL INFORMATION ECOSYSTEM USING MULTI-LEVEL AUTHENTICATION IN BLOCKCHAIN TECHNOLOGY

Dr.P.Senthil Pandian[1], Dr. V. Kannadhasan[2], Mr.K.Alagar Pandi[3], Dr. R. Sangeetha[4], Dr. S. Dheepthi Gunavathana[5]

[1]Associate Professor, Department of CSE, Solamalai College of Engineering, Madurai, Tamilnadu.

[2,3]Assistant Professor, Department of Mechanical Engineering, Solamalai College of Engineering, Madurai, Tamilnadu

[4,5] Assistant Professor, Department of Science and Humanities, Solamalai College of Engineering, Madurai, Tamilnadu.

Abstract:

It has been demonstrated recently that the safe interchange of medical data enhances people's quality of life by enhancing their care and treatment. With all the threats to the security of healthcare information, the interoperability of the entire healthcare ecosystem is an on going concern. When it comes to striking a balance in the healthcare environment, blockchain technology is emerging as one of the primary possibilities. Finding established solutions is challenging, nevertheless, due to the on going development of new Blockchain technology and the advancement of healthcare systems. The design of blockchain-based solutions necessitates trade-offs, such as security and interoperability, from an architectural perspective. The first goal of this article was to explore architectural methods that promote the interoperability and security of Blockchain-based Health Management Systems. This was done through a systematic literature review. The second goal of this study is to discuss the results of these two major objectives. In light of the findings, a number of use cases for the mechanisms were created, complete with context, problems, and various architectural considerations (interoperability and security). In the second goal, a high-level architecture and its validation for the entire process of creating a domain-specific language utilising the Model Driven Engineering technique for particular Smart Contracts were provided.

Keywords: Blockchain, Ecosystem, Medical Information, Multi-Level Authentication, Interoperability.

INTRODUCTION

In the modern, globalized world, where only 50% of people have access to universal health care. Everyone must have access to high-quality healthcare (diagnosis, treatment, and prevention) delivered in a timely, secure, and open manner [1]. Medical centres would be ineffective and lose their credibility without the technologies that are being developed daily for this purpose, which expand the coverage and quality of hospital services [2]. There are many interwoven stakeholders in the expansive healthcare ecosystem, each with unique and occasionally conflicting requirements.

A significant amount of thorough and reliable information interchange between stakeholders occurs in the healthcare setting [3]. The management of Health Management Systems (HMS) and the relationship between Blockchain (BC) technology are two topics that are being researched daily from various angles with the goal of enhancing interoperability, security, traceability, confidentiality, and information integrity. Satoshi Nakamoto originally mentioned BC in a paper on Bitcoin [4].

Applications of BC have been researched in both financial contexts, where it all started, and other expanding ICT fields. It is now regarded as a mainstream technology, employed in a variety of sectors and use cases, including voting, identity management, contracts, supply chain, insurance, and healthcare [5]. The architecture of software is the product of numerous design choices.

When architects recognize trade-offs between quality attributes, such security and interoperability, they make the first type of decision at the requirements level. When interoperability allows the system to share data with other systems, security issues frequently surface. A system's capacity to provide others with access to information (interoperability) could aid to enhance a business process. But it creates possible problems in the event that the data is compromised (security vulnerabilities). Although a closed system would produce an impractical outcome, it could be an alternative to achieving security [6].

One of the main goals of this work is to develop a high-level architecture along with an experiment for the construction of an architectural mechanism for the Interoperability and security of HMSs through BC technology, creating an ecosystem of trust between them. This SLR provides the theoretical underpinning and sufficient basis for that goal.

This method, which is conceptually described as a Domain Specific Language (DSL) [7], aims to help with the challenges of resolving HMS interoperability using BC technology. A DSL would make it possible to specify Smart Contracts (SC) at a high level of abstraction, enabling independence from particular technologies and facilitating the reuse of contract implementation through Model Driven Engineering. Smart Contracts are code fragments that can be executed autonomously and automatically based on predefined conditional triggers.

RELATED WORKS

The field of medical technology has advanced significantly. With a variety of hardware, software, and communication networks with the improvement of being the primary goal the level of services offered [8]. The administration of healthcare trending data is a latent difficulty, but it can serve to increase the precision of doctor diagnoses and encourage research in the healthcare industry, according to BC and healthcare experts [9]. Although there are a number of architectural solutions in the literature that address non-functional requirements like interoperability (e.g., a broker [10]), as well as security and privacy requirements (e.g., data encryption [11]), such as access control and data privacy [12], striking a balance between them is not an easy task because off-the-shelf solutions do not exist [13].

The use of data from other untrustworthy sources has led to mistrust between healthcare organization’s and healthcare professionals, including doctors and nurses, among others, and competition has been created in the sharing of sensitive information to create tangible economic goals. The information that has been disseminated also lacks integrity [14]. In light of the aforementioned, BC is more secure than other information management techniques since it ensures that the data is comprehensive and makes it possible to track the information's provenance [15]. In addition, BC is not unfamiliar with potential security risks,

vulnerabilities, and other related issues, as is the case with most technologies.

The entities involved in the healthcare ecosystem must have interoperable access to data that maintains security, trust, and privacy while also providing the necessary functionality. In the specific context of the functional, non-functional, and business requirements of the healthcare ecosystem, interoperability and security are concerns that must be balanced.

The challenge of having the knowledge and skills necessary to create software architectures in this new context is a result of BC's prospects in the healthcare industry. The issue is the lack of understanding about architectures, especially interoperability, which necessitates conceptual and technological approaches to make it easier to build while balancing interoperability and security.

A. BLOCKCHAIN

The development of numerous applications, including those in healthcare, is being driven by BCs. A BC is a type of data structure made up of blocks, which are ordered batches of data elements. The hash1 of the record that came before it is used to link the blocks and the aforementioned assures immutability [16]. A collection of decentralized nodes (peers) that keep a copy of the full chain maintain a BC. This chapter introduces these nodes, which respond to a consensus mechanism. The foundational elements of the BC technology are discussed in more detail in the books [17], [18], and [19].

B. POSITIVE STAKE PROOF

The computational burden is waived by PoS algorithms, but only a randomly chosen portion of nodes are given the chance to construct each block. Each entity's current degree of system investment, which is often described as the value or duration of asset holdings pertinent to that specific BC [20], is weighted to determine the probability of selection.

C. DPoS: PROOF OF DELEGATED PARTICIPATION

Votes are weighted according on the stake of the voter, and the block producer candidates that obtain the most votes are those who produce blocks. Only holders of the network token are eligible to vote. Users may also assign ("proxy") another user with voting authority [21].

D.PRACTICAL BYZANTINE FAULT TOLERANCE.

This technique ensures unanimity despite the participants' unpredictable behaviour. If more than two-thirds of all validation pairs offer the same response, a new block is added [22]. A significant modification of this technique is presented in [23], who provide a reputation-based Delegated Byzantine Fault Tolerance consensus (DBFT) procedure to quickly reach agreement on the authoritative BC. Proof of Authority (PoA), QuorumChain, and Raft, among others, are alternate consensus mechanisms that are less useful. There is a thorough analysis of consensus procedures in [24].

E. SMART CONTRACT

SC was first introduced by computer scientist and attorney Nick Szabo in 1996 [25]. Szabo recognized the possibility of creating software that resembled contract clauses (from written agreements between individuals), that was legally enforceable, and that decreased the likelihood of non-compliance on the part of the parties. It also recognized that the word did not involve the use of artificial intelligence, but the use of computer algorithms that would be eventually employed in all forms of contracts. Although it was a novel idea in the 1990s, the technology needed for its proper development was not accessible.

METHODOLOGY

Model-driven engineering (MDE) is a branch of software engineering that focuses on the methodical application of software models to increase output and various other qualities of software, such as

maintainability and system compatibility. Additionally, it increases automation and offers a higher level of abstraction [26]. Some key ideas that might be regarded as the MDE paradigm's foundational components are as follows

• A model depicts a software system's component in full or in part.

DSLs are used to represent these models.

• A DSL is technically represented by a metamodel.

• Model transformations or model translation are the usual methods for automating processes.

The purpose of SLR is to examine the architectural mechanisms being used to enhance the security and interoperability of HMSs utilizing BC, as well as the architectural features that underpin these mechanisms. The complete refinement procedure is summarized in Figure 1 and is explained below: Initially, 318 documents were found when searching the chosen databases. There is only one copy of each paper in the records because it was discovered that 109 of them are stored across multiple databases, eliminating duplicates in the process. Thus, 209 papers needed to be examined for the following phase.

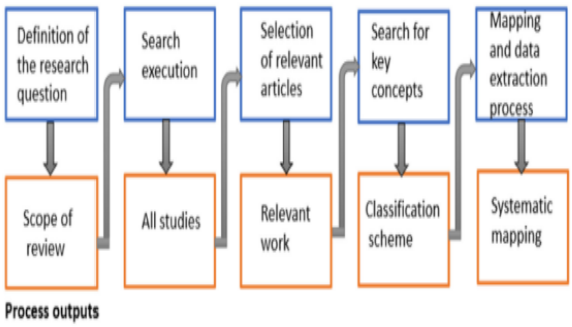

Figure 1 Refinement Procedure

MULTI-LEVEL AUTHENTICATION

The group of interoperability strategies is shown in Figure 8. Locate and Manage Interfaces are the two categories into which they fall in this instance. In our instance, every tactic was relevant to the Manage Interfaces subcategory. Having examined the strategies, we can relate them to the RQ2 results as a whole. The key stakeholders circling around BC software engineering technology are depicted visually in Figure 2. The International Organization for Standardization (ISO)/IEC/IEEE 42010-2011, Systems and Software Engineering-Architecture Description, methodology has been accepted by our company. A system-of-systems model is developed in this instance, identifying the key stakeholders who are concerned in this study.

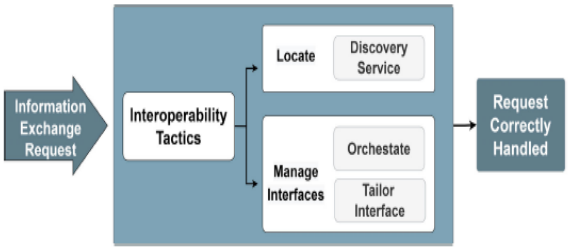

Figure 2 Multi-Level Authentication

Architectural strategies, such as the primary domains and subdomains to define and specify the BC technology components, are utilized to support these concerns. The final 21 papers on the IEEE 42010 framework were mapped into the aforementioned elements, which were then given n [27]. Right side shows some of the BC-related technologies that were previously reviewed in the distance.

The four forms of BC used in permissioned and restricted domains. The varied data are maintained within the healthcare solutions in both on-chain and off-chain data, which are the two categories that make up the data domain. The sorts of networks utilized in these fields are listed in the network domain. The work of Wang et al. [28] offers a novel BC-based method for safe and auditable private data sharing in smart grids as a complement to this notion. The use of on-chain and off-chain SC for a trusted execution environment (TEE) with atomic operation guarantee for the private processing of user data and reduction of computational cost in the BC are also discussed.

SYNTHESIS AND DISCUSSION

We sought to do a comprehensive analysis of the two previous RQs, where we proposed a categorization into 7 different situations in which BC is being utilised to affect the interoperability and security

of HMS following the analysis of the evaluated publications. Patterns of resemblance (such as the mechanisms utilised for the solutions or how BC is used in each solution) were found in order to present these situations, and the architectural strategies were examined in RQ2. Give BC application architects and designers and field researchers a clearer perspective while considering potential solutions for the healthcare industry is shown in Figure 3 as Security tactics.

Figure 3 Security tactics

A firm foundation for the project may be built by using this information to establish the general layout of the software so that specifics can be added to define the large picture. How to add certain techniques as well in order to accomplish the needed quality characteristics, in this case the interoperability and security of the intended solutions. As noted earlier, we will incorporate the relevant architectural mechanisms in these high-level diagrams.

The architectural facets described in the response to RQ2. We depend on Mezaros et al.'s [95] methodology for describing architectural elements. This technique relates the final 21 items using a general diagram, a summary, the problem statement, a discussion of interoperability and security issues, and an explanation of some tactics (not all are covered due to the length of the article).

For doctors, researchers, and the general public to have their dependable health information history while they go about their daily lives, healthcare data management needs to be technologically upgraded in order to give accurate, reliable, and verifiable data [29]. The use of BC and API increases interoperability and integration with numerous HMS, speeds up their technology adoption, and improves healthcare delivery effectiveness.

The focus of healthcare interoperability has typically been on data interchange between commercial organizations, like several HMS. Recently, the focus has been on patient-driven information exchange, in which the patient acts as the intermediary and driver of the transmission of medical information [30]. It is possible for third parties to access the recorded data to carry out various research actions, such as big data analytics, autonomous learning, and artificial intelligence [31] by having APIs that manage information Read (e.g., registering medical entities that are authorized to create and support transactions) from all participants in the healthcare ecosystem.

These APIs can be included into a variety of analytics platforms, giving users access to data being recorded in real-time from the internal systems of the healthcare organization while the patient undergoes their consultation processes [32]. The zero-knowledge protocol (ST5), in which one party (the tester) verifies to the other party (the verifier) without disclosing any information other than the fact that the specific claim is true, is one of the strategies used to maintain privacy. Additionally, to identify specific users, these services employ a strong user authentication system (ST11). A SC is a section of code that runs automatically and autonomously as a result of boolean triggers that have been set up in advance. These agreements do away with the requirement for a middleman to share data and help build confidence between all parties connected through BC. In these kinds of situations, where the identification of surgeons and patients is vital and delicate, CAs (ST4) are a crucial technique.

CONCLUSION

In order to increase the interoperability and security of HMS utilising BC, we conducted a systematic literature review on the mechanisms and architectural components in this work. A total of 21 papers—corresponding to the same number of interoperability and security solutions in the BC technology field—have been methodically analysed, contrasted, and debated. This study offers fascinating views by methodologically examining each of the solutions. The first is to clearly reveal the architectural mechanisms utilised to enable BC solutions in healthcare environments, which include Frameworks, Gateways, Proxies, and among others, MDE, API, and DSLs.

The second step is to evaluate, describe, and categories the architectural strategies applied to HMS's usage of BC to address interoperability and security issues. In order to address the architectural level solutions using BC in the healthcare industry, we generate seven high-level scenarios.

For each of these, we describe the context, a problem, analyses interoperability and security issues, and then describe and analyses some trade-offs used to balance interoperability and security of the healthcare ecosystem using BC. Our findings enable us to draw the conclusion that the prerequisites are satisfied for investigating the architectural components employing BC, centred on the interoperability and security of healthcare environments, allowing a wide range of novel use cases.

As a result, we anticipate that interest in this field of study will significantly rise. By enabling the work of academics and developers, this study aims to improve the BC ecosystem. We anticipate that this study will serve as a robust and trustworthy foundation for future work in the fields of software design, interoperability, and security of HMS employing BC. Finally, we can state that this type of solution uses Model-Driven Engineering (MDE) to maximize productivity and enhance the quality, maintenance, and interoperability of the entire healthcare ecosystem.

References:

[1] Universal Health Coverage, World Health Organization, Geneva, Switzerland, 2022.

[2] P. D. Chatzoglou, ‘‘Using a modified technology acceptance model in hospitals,’’ Int. J. Med. Informat., vol. 78, no. 2, pp. 115–126, 2019.

[3] C. A. da Costa, and R. da Rosa Righi, ‘‘OmniPHR:Adistributed architecture model to integrate personal health records,’’ J. Biomed. Inform., vol. 71, pp. 70–81, Jul. 2019.

[4] M. N. Bhardwaj, and D. Paul, ‘‘Ransomware in healthcare facilities: A harbinger of the future?’’ Perspect. Health Inf. Manage., vol. 10, pp. 1–22, Jul. 2019.

[5] R. Alubady, ‘‘A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research,’’ in Proc. 1st Babylon Int. Conf. Inf. Technol. Sci. (BICITS), Apr. 2019.

[6] L. Coventry, Principles of Health Interoperability HL7 and SNOMED, 2nd ed. New York, NY, USA: Springer, 2019, pp. 1–316.

[7] D. Branley, ‘‘Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,’’ Maturitas, vol. 113, pp. 48–52, Jul. 2018.

[8] S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Decentralized Bus. Rev., vol. 5, p. 21260, Oct. 2018.

[9] E. Vaughn, J. Shelton, and A. Cahana, How Blockchain Technology Can Enhance EHR Operability. St. Petersburg, FL, USA: Ark Invest, 2018.

[10] Kuo, ‘‘Opportunities and challenges of cloud computing to improve health care services,’’ J. Med. Internet Res., vol. 13, no. 3, p. e67, Sep. 2018.

[11] P. Clements, and R. Kazman, Software Architecture in Practice. London, U.K.: Pearson, 2018.

[12] Brereton, ‘‘A systematic review of systematic review process research in software engineering,’’ Inf. Softw. Technol., vol. 55, no. 12, pp. 2049–2075, 2018.

[13] R. Feldt, S. Mujtaba, and M. Mattsson, ‘‘Systematic mapping studies in software engineering,’’ in Proc. 12th Int. Conf. Eval. Assessment Softw. Eng., 2017, pp. 68–77.

[14] J. Bézivin, F. Jouault, and P. Valduriez, ‘‘Model-based DSL frameworks,’’ in Proc. Companion 21st ACM SIGPLAN Symp. Object- Oriented Program. Syst., Lang., Appl., 2017, pp. 602–616.

[15] J. Cabot, M. Wimmer, and L. Baresi, Model-Driven Software Engineering in Practice, 2nd ed. San Rafael, CA, USA: Morgan & Claypool, 2017.

[16] Q. Mahmoud, and J. Eklund, ‘‘Blockchain technology in healthcare: A systematic review,’’ Healthcare, vol. 7, no. 2, p. 56, 2017.

[17] J. Hurtado, ‘‘The role of the blockchain technology in the elderly care solutions: A systematic mapping study,’’ in Proc. Int. Workshop Gerontechnol. Cham, Switzerland: Springer, 2017, pp. 23–34.

[18] A. Ekblaw, T. Vieira, and A. Lippman, ‘‘MedRec: Using blockchain for medical data access and permission management,’’ in Proc. 2nd Int. Conf. Open Big Data (OBD), Aug. 2016, pp. 25–30.

[19] S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, ‘‘Blockchain technology in the healthcare industry: Trends and opportunities,’’ J. Ind. Inf. Integr., vol. 22, Jun. 2016, Art. no. 100217.

[20] H. T. S. Alrikabi, and M. R. Aziz, ‘‘Combination of hiding and encryption for data security,’’ Int. J. Interact. Mobile Technol., vol. 14, pp. 34–47, Jan. 2016.

[21] H. Materwala, ‘‘BlockHR: A blockchain-based framework for health records management,’’ in Proc. 12th Int. Conf. Comput. Modeling Simulation, Jun. 2016, pp. 164–168.

[22Kotzanikolaou, T. K. Dasaklis, and M. Burmester, ‘‘A hierarchical multi blockchain for fine grained access to medical data,’’ IEEE Access, vol. 8, pp. 134393–134412, 2016.

[23] A. A. Vazirani, D. Brindley, and E. Meinert, ‘‘Design choices and trade-offs in health care blockchain implementations: Systematic review,’’ J. Med. Internet Res., vol. 21, no. 5, May 2016, Art. no. e12426.

[24] J. M. Moral Ferrer, D. Tapscott, A. Tapscott, A. I. D. Santos, V. Koulaidis, J. P. Schmidt, M. Sharples, J. Domingue, and N. Smolenski, ‘‘Blockchain en educación: Cadenas rompiendo moldes,’’ Learn., Media Social Interact., vol. 3, no. 2, pp. 95–97, 2016.

[25] M. Pichler, T. Beranic, L. Brezocnik, M. Turkanovic, G. Lentini, F. Polettini, A. Lué, A. C. Vitale, G. Doukhan, and C. Belet, ‘‘Framework for assessing the smartness maturity level of villages,’’ in Proc. Eur. Conf. Adv. Databases Inf. Syst. Cham, Switzerland: Springer, 2016, pp. 501–512.

[26] E. F. Coutinho, ‘‘A pattern adherence analysis to a blockchain web application,’’ in Proc. IEEE Int. Conf. Softw. Archit. Companion (ICSA-C), Mar. 2015, pp. 103–109.

[27] H.-H. Kung, J. G. Udayasankaran, B. Kijsanayotin, A. B. Marcelo, L. R. Chao, and C.-Y. Hsu, ‘‘An architecture and management platform for blockchain-based personal health record exchange: Development and usability study,’’ J. Med. Internet Res., vol. 22, no. 6, Jun. 2015, Art. no. e16748.

[28] S. Mishra, and M. Hamdaqa, ‘‘iContractBot: A chatbot for smart Contracts’ specification and code generation,’’ in Proc. IEEE/ACM 3rd Int. Workshop Bots Softw. Eng. (BotSE), Jun. 2015, pp. 35–38.

[29] C. Cartofeanu, and S. Gao, ‘‘Smart contract applications within blockchain technology: A systematic mapping study,’’ Telematics Informat., vol. 35, no. 8, pp. 2337–2354, 2015.

[30] X. Dai, and J. Xiao, ‘‘Towards a novel architecture for enabling interoperability amongst multiple blockchains,’’ in Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jul. 2015, pp. 1203–1211.

[31] J. Ni, N. Zhang, and X. Shen, ‘‘Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions,’’ IEEE Commun. Surveys Tuts., vol. 24, no. 1, pp. 160–209, 1st Quart., 2015.

[32] Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and A. Liu, ‘‘A survey of blockchain technology applied to smart cities: Research issues and challenges,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2015.

[33] A. Vasconcelos, S. Guerreiro, and M. Correia, ‘‘A survey on blockchain interoperability: Past, present, and future trends,’’ ACM Comput. Surv., vol. 54, no. 8, pp. 1–41, Nov. 2015.

[34] A. A. Temghart, F. Sifou, and F. AlShahwan, ‘‘Adecentralized blockchain-based architecture for a secure cloud-enabled IoT,’’ J. Mobile Multimedia, vol. 2020, pp. 389–412, Nov. 2015.

[35] J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F. Wang, ‘‘Blockchain-powered parallel healthcare systems based on the ACP approach,’’ IEEE Trans. Computat. Social Syst., vol. 5, no. 4, pp. 942–950, Dec. 2015.

[36] Dr.P.Senthil Pandian, Dr.S.Muneeswaran, Valli Mayil, “Identifying software development IOT effort in human and machine using global wavelet method” in Global Journal of Engineering and Technology Advances, 2023.