JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN FOR HEALTHCARE MANAGEMENT SYSTEMS: A SURVEY ON INTEROPERABILITY AND SECURITY

[1]Jinkala Sai Sudeep , [2]Mellam Sri Harsha , [3]Pandula Shashi Kiran , [4]Surugu Bharath , [5]Mr.Manik Rao Patil

[1,2,3,4]UG Scholars , [5]Asst. Professor

[1,2,3,4]Department of Computer Science Engineering (Internet of Things)

Guru Nanak Institutions Technical Campus (Autonomous), Hyderabad, India

Abstract : This research addresses a critical necessity within healthcare systems: the secure exchange of medical information. It delves into the potential of blockchain technology to fulfill this need. Utilizing a Systematic Literature Review (SLR), the study explores the architectural mechanisms that support both interoperability and security within Blockchain-based Health Management Systems. Through this review, the study identifies a range of scenarios where these mechanisms can be effectively deployed, taking into account contextual factors, prevalent issues, and architectural considerations such as interoperability and security. Additionally, the research proposes a high-level architecture, which is subsequently validated through experimentation. One notable aspect of this proposed architecture is the emphasis on the development of a Domain Specific Language (DSL) for crafting Smart Contracts. This is achieved through the application of Model Driven Engineering (MDE) methodology. Such an approach not only facilitates the creation of Smart Contracts but also enhances their adaptability and efficiency. However, the research also acknowledges the challenges inherent in striking a balance between security and interoperability within blockchain-based healthcare solutions. This task is further complicated by the continual evolution of both technologies and healthcare systems. In providing insights into the architectural design and validation processes, this study makes significant strides towards advancing the integration of blockchain technology within healthcare. The ultimate goal is to facilitate improved data exchange and patient care while navigating the complexities inherent in the healthcare landscape.

Index Terms **:** Blockchain Technology, Health Management Systems (HMS), Interoperability, Architectural Mechanisms, Domain Specific Language (DSL), Smart Contracts (SC), Model Driven Engineering (MDE), Healthcare Data Management, Interoperability Trade-offs, Security Challenges, Decentralization, Healthcare Ecosystem, Architecture Tradeoff Analysis Method (ATAM)

I. INTRODUCTION

The introduction provides a thorough understanding of the complexities within the healthcare ecosystem, particularly concerning the exchange of medical information. It underscores the pressing need for technological solutions to enhance efficiency, safety, and transparency in managing healthcare data. The narrative emphasizes the inherent challenges of existing health information storage systems, which are often fragmented and vulnerable to risks associated with centralized data management, such as cyberattacks and breaches of confidentiality. The paper aims to investigate how Blockchain (BC) technology can be leveraged within Health Management Systems (HMS) to address these challenges and improve key aspects like interoperability and security. Recognizing BC's widespread adoption across various industries and its burgeoning significance, the paper acknowledges its potential within healthcare settings. Specifically, BC is praised for its capacity to ensure traceability, confidentiality, and the integrity of information, making it a promising solution for the healthcare sector. Central to the research is the exploration of architectural mechanisms supporting interoperability and security within Blockchain-based HMS. Additionally, the paper aims to propose and validate a high-level architecture for the development of a Domain Specific Language (DSL) using Model Driven Engineering (MDE) methodology for Smart Contracts (SC). This research question sets the foundation for the subsequent investigation and analysis. The paper's structure is outlined to encompass several sections, each serving a distinct purpose. It begins with establishing the general context and scope of the project, followed by outlining the specific objectives. The problem statement and existing challenges within the current healthcare system are then presented, with a particular focus on shortcomings related to security, storage efficiency, and interoperability. This structured approach ensures a comprehensive examination of the subject matter and guides the reader towards understanding the significance and relevance of the research.

II. LITERATURE SURVEY

The literature review encompasses a diverse array of studies that delve into encryption and security methods relevant to healthcare systems and data management.

Thamer and Alubady (2021) highlight the susceptibility of healthcare systems to cyberattacks, particularly ransomware, underscoring the urgency for effective solutions. Their study surveys strategies aimed at preventing ransomware attacks, including the utilization of Blockchain technology alongside other tools. They identify research gaps and stress the paramount importance of information security in healthcare settings.

Zhang et al. (2020) introduce advancements in searchable encryption by presenting a scheme that supports Boolean keyword search in public key settings. Their paper addresses shortcomings of previous schemes and proposes a novel method that combines vectors and inner product encryption to enable efficient keyword search functionality.

Senouci et al. (2021) put forth a certificateless searchable encryption scheme designed to resist keyword guessing attacks, thus mitigating concerns regarding data breaches in cloud storage services. Their study contributes significantly to enhancing security in cloud environments by presenting an encryption scheme that is resilient against various attack scenarios.

Jiang et al. (2022) concentrate on forward security in public-key authenticated encryption with keyword search (PAEKS), introducing a new primitive called forward secure PAEKS (FS-PAEKS) to mitigate the risks of information leakage from previously issued queries. Their paper introduces an efficient FS-PAEKS scheme that supports conjunctive queries and demonstrates its practical performance in a real cloud environment.

Zeng et al. (2019) propose a searchable asymmetric encryption scheme that supports sub-linear Boolean queries for cloud applications. Their study combines symmetric and public-key encryption techniques to overcome limitations present in existing schemes and presents a novel secure inverted index for efficient data retrieval.

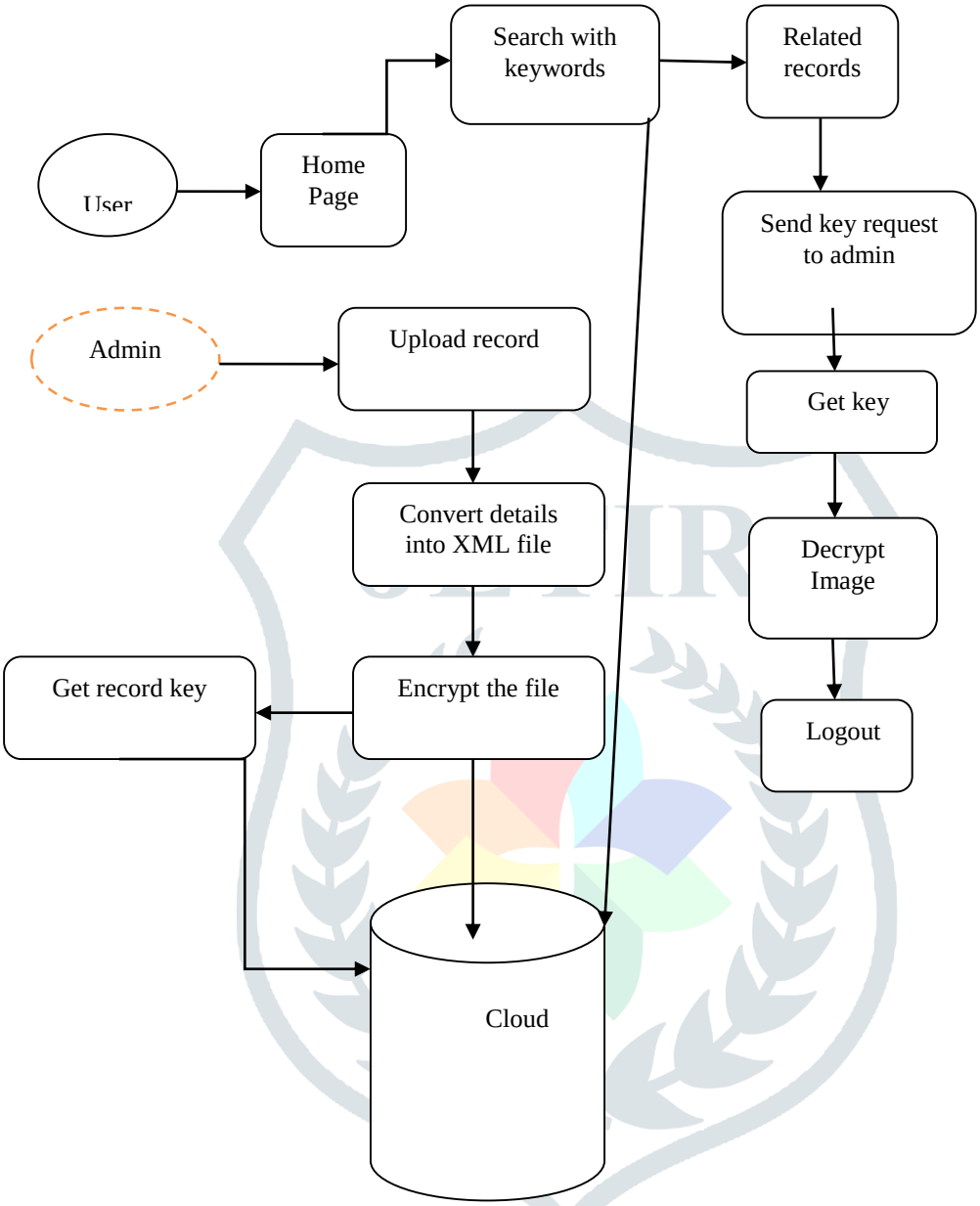
Chen et al. (2020) focus on multi-user Boolean searchable encryption for mobile clouds, addressing privacy concerns and search efficiency in mobile services. Their paper introduces a multi-user scheme for rapid Boolean query outcomes and a fast ranking search protocol to safeguard relevance scores between files and keywords.

Collectively, these studies make significant contributions to the field of information security and encryption techniques, providing valuable insights into addressing vulnerabilities and enhancing data protection in healthcare systems and cloud environments. However, there remain gaps in existing knowledge, particularly the need for more robust encryption schemes resilient against various attack scenarios and the development of efficient methods for secure data retrieval and query processing in distributed environments such as cloud and mobile services.

III. PROPOSED SYSTEM

This paper is centered around two primary objectives. Firstly, it undertakes a Systematic Literature Review to explore the architectural mechanisms employed in supporting the interoperability and security of Blockchain-based Health Management Systems (HMS). This systematic review delves into existing literature to identify and analyze the various architectural mechanisms utilized in Blockchain-based HMS. The review also aims to generate a series of scenarios wherein these mechanisms can be effectively applied, considering contextual factors, associated issues, and pertinent architectural concerns, notably interoperability and security. Following the analysis of the review results, the paper proceeds to its second objective. Here, it proposes a high-level architecture and subsequently validates it through experimentation. This proposed architecture is designed to facilitate the entire process of developing a Domain Specific Language (DSL) explicitly tailored for Smart Contracts within Blockchain-based HMS. The methodology employed for this purpose is Model Driven Engineering (MDE), which offers a systematic approach to software development, focusing on modeling and abstraction. By leveraging the MDE methodology, the paper aims to provide a structured framework for the creation of a DSL tailored for Smart Contracts, thereby enhancing the efficiency and effectiveness of Blockchain-based HMS. The validation process entails practical experimentation to ascertain the feasibility and efficacy of the proposed architecture in real-world scenarios. Overall, these two objectives collectively contribute to advancing the understanding and implementation of Blockchain technology in healthcare systems. By systematically exploring architectural mechanisms and proposing a validated high-level architecture, the paper aims to address critical concerns surrounding interoperability and security while promoting innovation and efficiency in healthcare data management.

IV. SYSTEM ARCHITECTURE



V. HARDWARE REQUIREMENTS

The hardware requirements serve as the foundational specifications for the implementation of the system and are integral to ensuring the system's functionality and performance. These requirements constitute a comprehensive and cohesive specification of the entire system, providing software engineers with essential guidance for the system design phase. Importantly, they outline what the system should entail, rather than how it should be implemented.

- PROCESSOR : PENTIUM IV 2.6 GHz, Intel Core 2 Duo.
- RAM : 512 MB DD RAM
- MONITOR : 15” COLOR
- HARD DISK : 40 GB

VI. SOFTWARE REQUIREMENTS

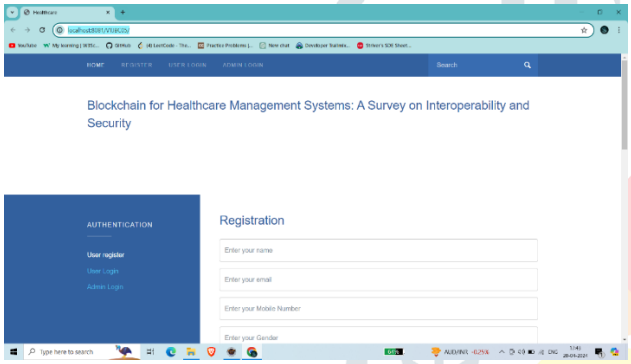
The software requirements document serves as the definitive specification of the system, outlining both the definition and specification of requirements. It delineates what the system should accomplish rather than dictating how it should achieve those objectives. Essentially, it provides a comprehensive set of functionalities and features that the system must possess to meet its intended purpose.

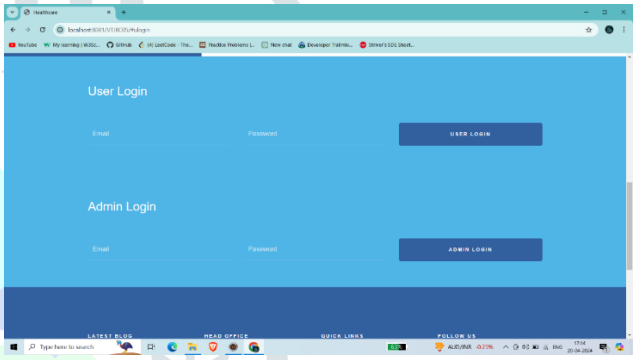
- Front End : J2EE (JSP, SERVLET)
- Back End : MY SQL 5.5
- Operating System : Windows 7
- IDE : Eclipse

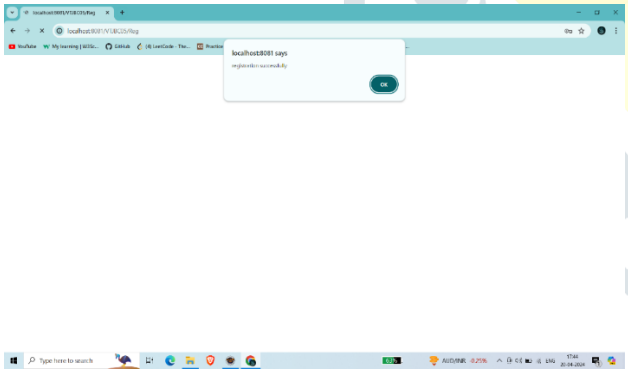
VII. FUTURE ENCHANCEMENT

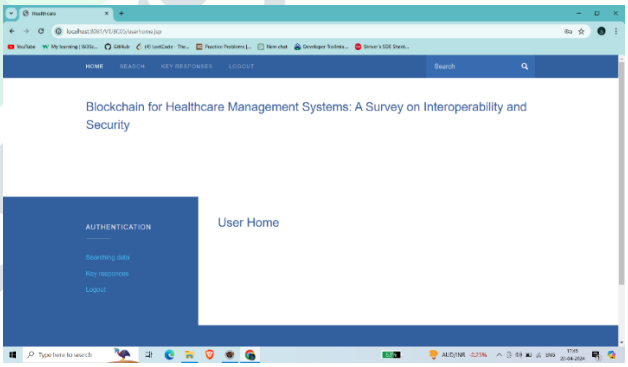
In future directions, the exploration of the metaverse is intersecting with blockchain technology (BC) from various angles, signaling potential synergies and challenges. This review underscores the assertion that interoperability will emerge as a pivotal driver shaping the evolution of the metaverse. Interoperability, in this context, refers to the seamless interaction and integration of diverse virtual environments and platforms within the metaverse. Simultaneously, the review identifies a plethora of security challenges inherent in managing health data within the metaverse. These challenges encompass concerns such as data leakage, manipulation, and loss, particularly if the metaverse relies on a centralized storage system. The risk of compromising sensitive health data underscores the urgency of implementing robust security measures within the metaverse ecosystem. However, BC technology emerges as a potential solution to address the inherent trade-off between interoperability and security within the metaverse. By leveraging the decentralized and immutable nature of blockchain, BC offers a framework for securely managing and exchanging health data across disparate virtual environments. BC's decentralized architecture mitigates the risks associated with centralized storage systems, thereby enhancing data security and integrity..

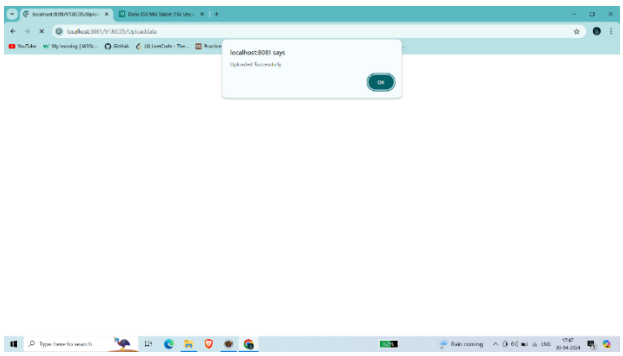
VIII. SNAPSHOTS

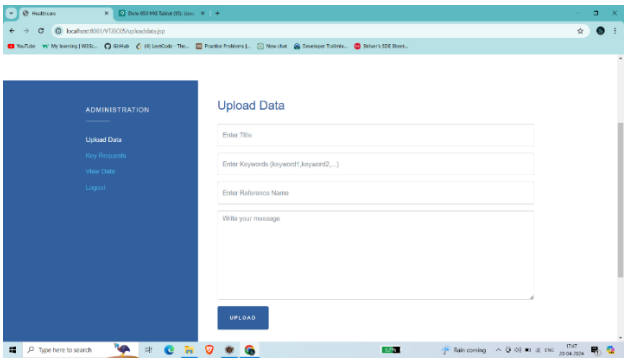


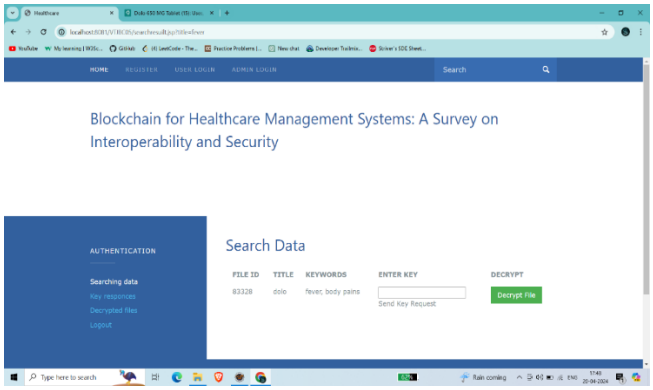


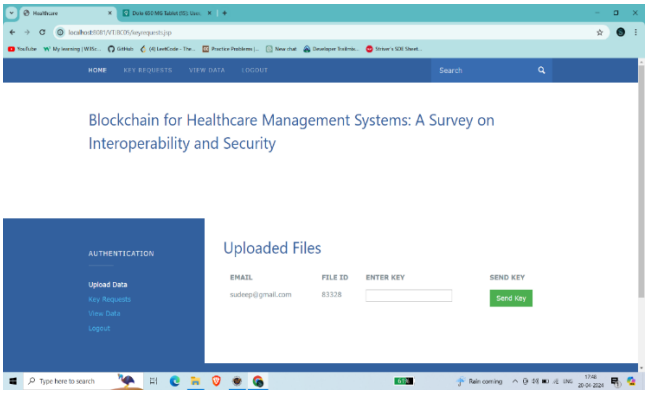


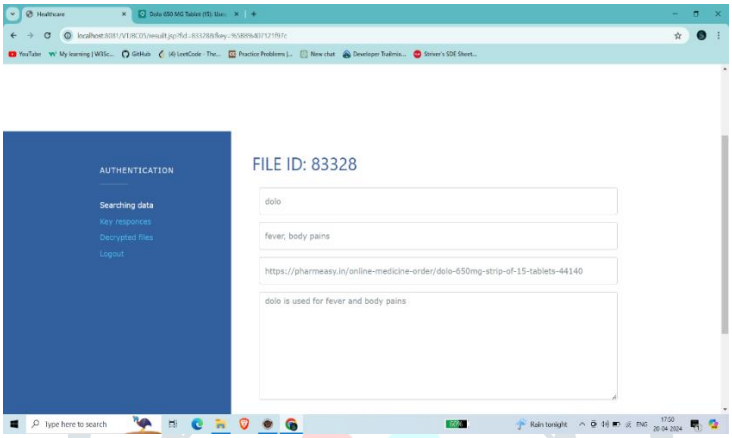












IX. CONCLUSION

In summary, this paper presents a thorough review and analysis of mechanisms and architectural elements aimed at bolstering the interoperability and security of Health Management Systems (HMS) using Blockchain (BC) technology. Through a meticulous systematic literature review, we have identified and scrutinized various solutions and tactics employed in the realm of BC technology to tackle interoperability and security challenges within healthcare environments. Our analysis encompasses 21 papers, unveiling a diverse array of architectural mechanisms, tactics, and high-level scenarios for implementing BC-based solutions in healthcare.Key findings include the identification of architectural mechanisms such as Frameworks, Gateways, Proxies, APIs, DSLs, and Model-Driven Engineering (MDE), alongside tactics for effectively balancing interoperability and security concerns. We present seven high-level scenarios, each addressing specific architectural solutions for BC integration in healthcare, and discuss the necessary trade-offs required to achieve interoperability and security goals. Furthermore, we propose an MDE Framework for blockchain interoperability and security, delineating a high-level architecture centered around the development of a Domain Specific Language (DSL) for Smart Contracts (SC). We intend to validate this architecture through an MDE experiment, refining the process and ensuring its feasibility across different BC platforms. The significance of this research lies in its potential to propel the practicality and efficacy of the BC ecosystem in healthcare. By furnishing a robust foundation and actionable insights for developers and researchers, we aim to catalyze further interest and innovation in the realms of software architecture, interoperability, and security of HMS using BC technology. Looking forward, our future endeavors include characterizing different types of SC for the development of requisite meta models in our DSL. Additionally, we plan to conduct case studies to evaluate our proposed mechanisms in real-world scenarios, with a focus on patient referral processes and the management of elderly healthcare data. These case studies will undergo evaluation using the Architecture Tradeoff Analysis Method (ATAM), enabling us to assess the interoperability and security attributes of our system. In forthcoming publications, we will disseminate the results of these case studies and broaden the discourse on the trade-offs between interoperability and security in BC-based HMS within the healthcare ecosystem. Overall, this research endeavors to spur innovation and enhancement in healthcare data management through the seamless integration of blockchain technology, fostering a more secure, efficient, and interoperable healthcare ecosystem.

X. REFERENCES

[1]. Universal Health Coverage, Geneva, Switzerland, 2022.
[2]. V. P. Aggelidis and P. D. Chatzoglou, "Using a modified technology acceptance model in hospitals", Int. J. Med. Informat., vol. 78, no. 2, pp. 115-126, 2009.
[3]. A. Roehrs, C. A. da Costa and R. da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records", J. Biomed. Inform., vol. 71, pp. 70-81, Jul. 2017.
[4]. N. Spence, 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. 2018.
[5]. N. Thamer and R. Alubady, "A survey of ransomware attacks for healthcare systems: Risks challenges solutions and opportunity of research", Proc. 1st Babylon Int. Conf. Inf. Technol. Sci. (BICITS), pp. 210-216, Apr. 2021.
[6]. T. Benson, Principles of Health Interoperability HL7 and SNOMED, New York, NY, USA:Springer, pp. 1-316, 2012.
[7]. L. Coventry and 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, pp. 21260, Oct. 2008.

[9]. C. Burniske, E. Vaughn, J. Shelton and A. Cahana, How Blockchain Technology Can Enhance EHR Operability, St. Petersburg, FL, USA:Ark Invest, 2016.
[10]. A. M.-H. Kuo, "Opportunities and challenges of cloud computing to improve health care services", J. Med. Internet Res., vol. 13, no. 3, pp. e67, Sep. 2011.
[11]. L. Bass, P. Clements and R. Kazman, Software Architecture in Practice, London, U.K.:Pearson, 2012.
[12]. B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering", Inf. Softw. Technol., vol. 55, no. 12, pp. 2049-2075, 2013.
[13]. K. Petersen, R. Feldt, S. Mujtaba and M. Mattsson, "Systematic mapping studies in software engineering", Proc. 12th Int. Conf. Eval. Assessment Softw. Eng., pp. 68-77, 2008.
[14]. I. Kurtev, J. Bézivin, F. Jouault and P. Valduriez, "Model-based DSL frameworks", Proc. Companion 21st ACM SIGPLAN Symp. Object-Oriented Program. Syst. Lang. Appl., pp. 602-616, 2006.
[15]. M. Brambilla, J. Cabot, M. Wimmer and L. Baresi, Model-Driven Software Engineering in Practice, San Rafael, CA, USA:Morgan & Claypool, 2017.
[16]. C. Agbo, Q. Mahmoud and J. Eklund, "Blockchain technology in healthcare: A systematic review", Healthcare, vol. 7, no. 2, pp. 56, 2019.
[17]. E. Dulce and J. Hurtado, "The role of the blockchain technology in the elderly care solutions: A systematic mapping study", Proc. Int. Workshop Gerontechnol., pp. 23-34, 2021.
[18]. A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using blockchain for medical data access and permission management", Proc. 2nd Int. Conf. Open Big Data (OBD), pp. 25-30, Aug. 2016.
[19]. H. M. Hussien, 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. 2021.
[20]. A. I. Aljazaery, 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. 2020.
[21]. L. Ismail and H. Materwala, "BlockHR: A blockchain-based framework for health records management", Proc. 12th Int. Conf. Comput. Modeling Simulation, pp. 164-168, Jun. 2020.
[22]. V. Malamas, P. Kotzanikolaou, T. K. Dasaklis and M. Burmester, "A hierarchical multi blockchain for fine grained access to medical data", IEEE Access, vol. 8, pp. 134393-134412, 2020.
[23]. O. O'Donoghue, 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 2019.
[24]. A. R. Bartolomé, J. M. Moral Ferrer, D. Tapscott, A. Tapscott, A. I. D. Santos, V. Koulaidis, et al., "Blockchain en educación: Cadenas rompiendo moldes", Learn. Media Social Interact., vol. 3, no. 2, pp. 95-97, 2018.
[25]. J. Martinez-Gil, M. Pichler, T. Beranic, L. Brezocnik, M. Turkanovic, G. Lentini, et al., "Framework for assessing the smartness maturity level of villages", Proc. Eur. Conf. Adv. Databases Inf. Syst., pp. 501-512, 2019.
[26]. A. W. Abreu and E. F. Coutinho, "A pattern adherence analysis to a blockchain web application", Proc. IEEE Int. Conf. Softw. Archit. Companion (ICSA-C), pp. 103-109, Mar. 2020.
[27]. H.-A. Lee, H.-H. Kung, J. G. Udayasankaran, B. Kijsanayotin, A. B. Marcelo, L. R. Chao, et al., "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. 2020.
[28]. I. Qasse, S. Mishra and M. Hamdaqa, "iContractBot: A chatbot for smart Contracts' specification and code generation", Proc. IEEE/ACM 3rd Int. Workshop Bots Softw. Eng. (BotSE), pp. 35-38, Jun. 2021.
[29]. D. Macrinici, C. Cartofeanu and S. Gao, "Smart contract applications within blockchain technology: A systematic mapping study", Telematics Informat., vol. 35, no. 8, pp. 2337-2354, 2018.
[30]. H. Jin, X. Dai and J. Xiao, "Towards a novel architecture for enabling interoperability amongst multiple blockchains", Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS), pp. 1203-1211, Jul. 2018.