International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST24112134

Blockchain for Healthcare Management Systems : A Survey on Interoperability and Security

Ch Gopi[1], D Saikumar[2], G Premsagar[2], MD Noouman[2]
[1]Assistant Professor, Department of IT, Guru Nanak Institutions Technical Campus, Hyderabad, India
[2]Department of IT, Guru Nanak Institutions Technical Campus, Hyderabad, India

ARTICLEINFO

Article History:
Accepted: 15 April 2024
Published: 25 April 2024

Publication Issue :
Volume 11, Issue 2
March-April-2024
Page Number :
796-805

ABSTRACT

In recent years it has been shown that the secure exchange of medical information significantly benefits people's life quality, improving their care and treatment. The interoperability of the entire healthcare ecosystem is a constant challenge, and even more, with all the risks posed to the security of healthcare information. Blockchain technology is emerging as one of the main alternatives when it comes to finding a balance in the healthcare ecosystem. However, the constant development of new Blockchain technologies and the evolution of healthcare systems make it difficult to find established proposals. From an architectural point of view, the design of blockchain-based solutions requires trade-offs e.g., security and interoperability. This paper focuses on two main objectives, in the first one, it was carried out a Systematic Literature Review for exploring architectural mechanisms used to support the interoperability and security of Blockchain-based Health Management Systems. Taking into account of results, a series of scenarios were generated where these mechanisms can be used along with their context, issues, and various architectural concerns (interoperability and security). In the second objective, a high-level architecture and its validation were proposed through an experiment for the whole process of developing a Domain Specific Language, using the Model Driven Engineering methodology for specific Smart Contracts.

Keywords: Blockchain, DSL, Health, Interoperability, MDE, Model, Security, Smart Contracts, Software Architecture.

I. INTRODUCTION

In today's globalized world, where the percentage of universal health coverage is only 50%. It is necessary for everyone to have access to quality health services (diagnosis, treatment, and prevention) in an efficient, safe, and transparent manner [1]. For this purpose, technologies that increase the coverage and quality of hospital services are being developed every day, and

without them, medical centers would be inefficient and lose credibility [2].

The large healthcare ecosystem includes several interconnected stakeholders with different and sometimes competing needs. The healthcare environment involves a high degree of comprehensive and reliable information exchange between stakeholders [3]. However, this information is highly fragmented and distributed in multiple non-integrated data storage systems, making it impossible to have adequate information to support the care process and decision-making. This occurs because each medical center manages health information in an isolated and centralized way, causing health personnel to have a small history of the patient's entire life, which leads to errors in diagnosis and treatment. Likewise, having centralized information presents multiple information risks. This is highlighted by [4], which mentions that healthcare is one of the sectors most vulnerable to cyberattacks. Denial-of-service (DoS) attacks can occur to indispose information, or a ransomware attack to hijack information, which in many cases cannot be recovered [5]. For these and other reasons, it is necessary to have mechanisms that contribute to achieving interoperability between the information systems that support the care processes [6]. In addition, security is an indispensable element for disseminating patients' medical records, since this task entails various risks that cause serious damage to reputation, insurance, and finances, among other factors in the healthcare ecosystem [7].

The healthcare field is a topic that is researched daily from different approaches, one of which is the relationship between Blockchain (BC) technology and the management of Health Management Systems (HMS), with the idea of improving aspects such as interoperability, security, traceability, confidentiality, and information integrity. BC was first introduced by Satoshi Nakamoto in a paper on Bitcoin [8]. Applications of BC have been studied in financial environments (where it began), as well as in other growing areas of ICT. Now, it is considered a mainstream technology, used in different industries and use cases, such as identity management, contracts, supply chain, insurance, healthcare, voting.

II.RELATED WORKS

The second objective, a high-level architecture and its validation were proposed through an experiment for the whole process of developing a Domain Specific Language, using the Model Driven Engineering methodology for specific Smart Contracts.

In each scenario, we present an overview, of the problem, analyze interoperability and security, and relate some security and interoperability tactics. We then discuss some trade-offs used to balance interoperability and security in the healthcare ecosystem using BC. We propose a MDE Framework for blockchain interoperability and security. This framework consists of a high-level architecture whose main objective is the development of a DSL for the specification of SC independent of the BC platform used, to contribute to the interoperability and security of the healthcare environment. We propose an experiment developed under the MDE methodology, to put this architecture in context and validate each of the elements required in this solution.

PROBLEM STATEMENT

Healthcare has always been fundamental to society, where everyday accidents and emergencies arise those cause ailments and diseases that must be diagnosed, treated, and managed by different services. Having these services presents technological challenges in health, such as storage, consultation, and exchange of information, where its implementation is associated with a decrease in morbidity and mortality

Considering the above, there are several standards for Electronic Medical Records (EMRs). These standards

present its characteristics, strengths, and weaknesses, which make choosing one of them an additional problem to consider. Generally, health records are stored in databases within health organizations and rarely have access from remote sites, in this case, some inconveniences of slow access to data, and data access restrictions, among others, are generated.

In this regard, several interoperability and security issues are arising from the SC analysis, design, and development phases. Interoperable access to data in the healthcare ecosystem must provide the necessary functionality for the entities involved, maintaining security, trust, and privacy. Interoperability and security are issues that must be traded off in the specific context of the functional, non-functional, and business requirements of the healthcare ecosystem. The problem of knowledge and expertise required to design software architectures in this new scenario is a derivative of the opportunities of BC in the healthcare sector. The problem lies in the knowledge around architectures, particularly interoperability, which is incipient, and conceptual and technological strategies are required to facilitate the design considering qualities in trade-off with security and interoperability

III. LITERATURE SURVEY

N. Thamer and R. Alubady, healthcare is one of the most vulnerable sectors of cyber-attacks. As it continues to expand exponentially and moves to digitally-enabled healthcare services, cyber-criminals are trying to take advantage of the weaknesses and security vulnerabilities correlated with these shifts. As a result of technical developments, a multitude of highly powerful risks such as Ransomware is facing the healthcare sector. Ransomware is cyber-attack targeting companies and household users and has increased lately due to its productive results. It conflicts have significantly improved over the last few years. The study shows an exhaustive survey on Ransomware attacks and fixes these attacks. The main aim of this study is to classify the solution strategies for Ransomware attacks in healthcare that used to prevent the Ransomware, such as Blockchain technology, Software define network technology, Machine Learning, and other tools as well as to highlight many issues faced by researchers during the process of discovering a way to solve Ransomware attacks in health care systems. In addition, the study will provide scientific benefits to researchers in the field of information security, health institutions, and security companies.

Y. Zhang, Y. Zhao, Y. Wang and Y. Li, searchable encryption with advanced query function is an important technique in today's cloud environment. To date, in the public key setting, the best query function supported by the previous schemes are conjunctive or disjunctive keyword search, which are elementary but not enough to satisfy the user's query requirements. In this paper, we make a progress for constructing a searchable public key encryption scheme with advanced query function called simple Boolean keyword search. To create our scheme, we proposed a keywords conversion method that projects the index and query keywords into a group of vectors. Based on a combination of these obtained vectors and an adaptively secure inner product encryption scheme, a public key encryption with simple Boolean keyword search scheme is proposed. We also present both theoretical and experimental analysis to show the effectiveness of this scheme. To the best of our knowledge, it is the first time to give a searchable public key encryption scheme supporting queries like $q_1\ op_1\ q_2\ op_2 \ldots op_{i-1}\ q_i\ op_i \ldots op_{n-1} qn$, where op_i is a logical operator which can be and($\vee$) or or($\wedge$) and qi is a keyword.

M. R. Senouci, I. Benkhaddra, A. Senouci and F. Li, as the wave of data breaches continues crashing down on companies, specially for companies that provide cloud storage services, the data security and privacy have become the main concern of most clients that use this kind of services. Certificateless public key

encryption with keyword search (CLPEKS) is a novel cryptographic primitives that if implemented correctly, provides the possibility to search over an encrypted data that has been outsourced to the cloud server, while guaranteeing the privacy of the search-keyword used in the process. Several CLPEKS schemes have been presented in the literature, but many of them are found vulnerable to offline/online keyword guessing attacks either performed by inside attackers, outside attackers or by both. To overcome these security weaknesses, we propose an efficient and secure certificateless searchable encryption scheme that is proven to be resistant against different keyword guessing attacks under both, the hardness of solving the discrete logarithm (DL) and the computational Diffie-Hellman (CDH) problems in the random oracle model. Then, by conducting a comprehensive comparison between our proposed scheme and other related schemes, we found that the proposed scheme has better overall performance in terms of communication and computation complexities, while guaranteeing security against online and offline KGA performed by either outside attackers or inside attacker.

Z. Jiang, K. Zhang, L. Wang and J. Ning, public key encryption with keyword search is a promising primitive which enables search over encrypted data in secure data outsourcing services. In traditional construction, the associated keywords may be recovered from a given trapdoor by a malicious server through keyword guessing attacks. Therefore, the notion of public-key authenticated encryption with keyword search (PAEKS) was introduced, where a sender encrypts (and authenticates) the keywords using a receiver's public key and its secret key. In this paper, we consider the forward security for PAEKS and introduce a new primitive: forward secure public-key authenticated encryption with keyword search (FS-PAEKS), which captures the information leakage risk from previously issued queries due to the updates on the outsourced data. Technically, we embed a non-interactively agreed key into the cipher-keyword generation algorithm, and bind the cipher-keyword and the trapdoor with a set converted from algorithm-generation time. Finally, we present an efficient FS-PAEKS scheme supporting conjunctive query, and prove its forward security against chosen keyword attacks and keyword guessing attacks. To illustrate practical performance, we implement our FS-PAEKS and related PAEKS schemes based on Enron dataset in real cloud environment.

M. Zeng, K. Zhang, H. Qian, X. Chen, J. Chen and Y. Mu, cloud computing is a new promising technology paradigm that can provide clients from the whole network with scalable storage resources and on-demand high-quality services. However, security concerns are raised when sensitive data are outsourced. Searchable encryption is a kind of cryptographic primitive that enables clients to selectively retrieve encrypted data, the existing schemes that support for sub-linear boolean queries are only considered in symmetric key setting, which makes a limitation for being widely deployed in many cloud applications. In order to address this issue, we propose a novel searchable asymmetric encryption scheme to support for sub-linear boolean query over encrypted data in a multi-client model that is extracted from an important observation that the outsourced database in cloud is continuously contributed and searched by multiple clients. For the purpose of introducing the scheme, we combine both the ideas of symmetric searchable encryption and public key searchable encryption and then design a novel secure inverted index. Furthermore, a detailed security analysis for our scheme is given under the simulation-based security definition. Finally, we conduct experiments for our construction on a real dataset (Enron) along with a performance analysis to show its practicality.

Z. Chen, F. Zhang, P. Zhang and H. Zhao, mobile cloud computing has become an important technology for mobile services. It overcomes physical limitations of mobile devices towards flexible and scalable mobile services. When using mobile clouds,

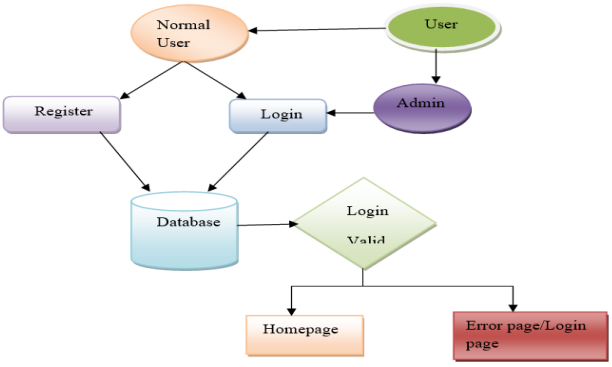
people usually upload and store their data in cloud servers, and access the data through mobile devices from anywhere. As the privacy of the sensitive data is the major concern of users, the data is often encrypted before storing in cloud servers. However, the flexibility using the data is thereby affected, such as a Boolean search over the encrypted data, or ranking search results. To address these problems, in this paper we first propose a novel multi-user Boolean keyword search scheme (MBKSS) to achieve a rapid Boolean query outcome, while eliminating query interactions between users and the data owner. To rank search results and protect the privacy of relevance scores between files and keywords, we design a new homomorphic cryptosystem with partial decryption, which could be used as a basis for constructing a fast ranking search protocol (FRSP). A comprehensive security analysis shows that the proposed MBKSS and FRSP can achieve secure Boolean search and ranking. The experimental results demonstrate that the proposed MBKSS and FRSP are efficient and suitable for mobile devices.

One feasible and promising method is to encrypt the data before storing it in cloud servers. In this case, the flexibility of data is affected. For example, a Boolean search over the encrypted data will become difficult. Suppose that there is a mobile user who wants to find a file in the encrypted data. He/she may need to download the entire database and decrypt it for searching. However, it may be impossible due to limited processing capacity and storage space in mobile devices.

IV.PROPOSED SYSTEM

This paper focuses on two main objectives, in the first one, it was carried out a Systematic Literature Review for exploring architectural mechanisms used to support the interoperability and security of Blockchain-based Health Management Systems. Taking into account of results, a series of scenarios were generated where these mechanisms can be used along with their context, issues, and various architectural concerns (interoperability and security). In the second objective, a high-level architecture and its validation were proposed through an experiment for the whole process of developing a Domain Specific Language, using the Model Driven Engineering methodology for specific Smart Contracts.

This SLR provides the theoretical underpinning and sufficient basis for one of the main purposes of this work, which consists of developing a high-level architecture together 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 mechanism, in principle proposed as a Domain Specific Language (DSL), which seeks to contribute to solving the difficulties of addressing interoperability of HMS through BC technology. A DSL would allow specifying Smart Contracts (SC) (code fragments that can be executed autonomously and automatically based on predefined conditional triggers) at a high level of abstraction, enabling independence from specific technologies and facilitating the reuse of contract implementation through Model Driven Engineering (MDE) approach.



This is the first module of our project. In this the application user's first create their account properly which are stored at the back end for verification or for providing security to the accounts. If user wants to get into his account first they have to submit their constraints such as username, password and so on…otherwise can't able to access the account. In our

project according to actions they are performing we disperse the users as admin or normal application user.

Electronic Health Record System:

Cloud-based electronic health record (EHR) systems enable medical documents to be exchanged between medical institutions; this is expected to contribute to improvements in various medical services in the future. In this project the electronic records are stored in xml files and we are store encrypted xml files to server.

The third party users have the permissions for searching the data related to electronic file to view the data the user must need a key to decrypt a file due to we are storing the files in the form of encryption in cloud. The key are stored at admin, So when we need a file data we must need get key from the admin, for that we need to send key request to admin for particular file.

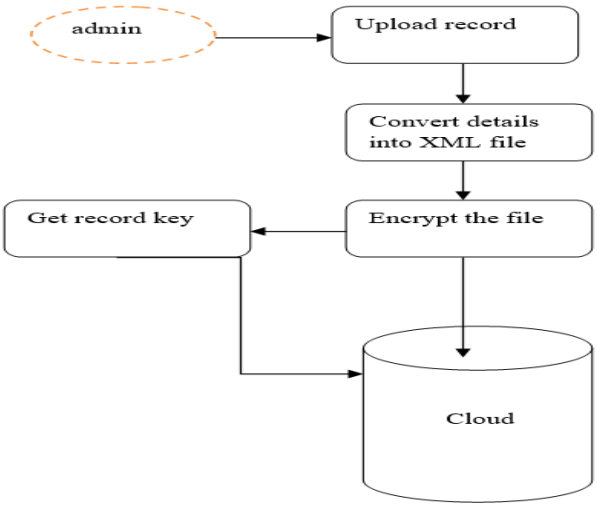


Figure 2. Electronic health record have title, reference name, keywords, data.

V.TECHNIQUE USED OR ALGORITHM USED

KC-RBAC Model

The KC-RBAC model is proposed to protect patient privacy in the medical information systems of a hospital with static restrictions. The proposed KC-RBAC can identify the real purposes of system users by referring to the biomedical domain knowledge.

Different system users in the hospital information systems have different roles in a variety of hospital processes. However, even for users with the same role in the system, their intentions to use the information systems may be different and vary in different contexts. As shown in, in a HIS's deployed RBAC model, the system user can access all information and data authorized to his or her role. While in a KC-RBAC system, the accessing rights of a user addition all yare restricted by using context which is supported by knowledge.

The KC-RBAC model can finally extract the necessary data from the system when hospital employees request patient information.

An MDE Framework for Blockchain Interoperability and Security

In this chapter, taking into account the gap that exists in the literature regarding the security and interoperability of BC platforms, and which were evidenced with the RSL, we propose a novel framework consisting of a high-level architecture, whose main objective is the development of a DSL for the specification of SC independent of the BC platform used, to contribute to the interoperability and security of the healthcare environment. In addition, we propose an experiment developed under the MDE methodology, to contextualize this architecture and validate each of the elements required in this solution. An important aspect of modeling and implementing SC is to define the business process and the rules governing the agreements under which the corresponding actions are executed. Unfortunately, these models use a combination of technical and business-centric terminologies that are different depending on the underlying BC platform targeted by the SC. Most SC are simple programs that define a set of rules that govern the contractual agreement process between the contracting parties (A contractual agreement is a self-executing and verifiable software code). Despite being simple, the development of SC is challenging. This is due to the complexity and heterogeneity of the

underlying platforms used to create and implement SC [96]. Different BC platforms use different terminologies and require contract models to be specified according to the syntax defined by the platform.

To address this problem, in this paper, we follow the MDE methodology, which allows for defining improved productivity and some other aspects of software quality, such as maintainability and interoperability between systems. In addition, it provides a higher level of abstraction and raises the level of automation. Consequently, as can be seen in Figure 17 shows a diagram of the proposed architecture, this is a principle mechanism proposed as a Domain Specific Language (DSL) [14], it seeks to contribute to solving the difficulties to address interoperability of HMS through BC technology. A DSL would allow SC to be specified at a high level of abstraction, enabling independence from specific technologies and facilitating the reuse of contract implementation through an MDE approach [15]. In addition, there would be multiple advantages for designers and programmers of SC, independent of the platform on which they are executed. A DSL will allow the designer to abstract SC from different BC implementations with different consensus mechanisms. Additionally, it will contribute to the generation of mature and grounded standards for the modeling of SC used in BC.

XML Security for Medical Document Security

Since the proposing of homomorphic properties, Fully Homomorphic Encryption (FHE) has been considered as the Holy Grail in cryptography. After Gentry's breakthrough on lattice-based FHE [11], a general solution has been shown to allow homomorphic evaluations over ciphertext domain. However, applying existing general fully homomorphic encryption scheme to image processing applications would be far from practical, due to their huge computation complexity. Different from FHE, SHE schemes can only support limited times of homomorphic operations. Considering the design targets of secure image processing mechanisms, SHE schemes seem to be suitable for some image processing applications. Here, we first briefly introduce the framework of the state-of-the-art practical SHE scheme before discussing its merits and drawbacks.

In future directions, the metaverse is being studied from different approaches along with BC, for example, in the work of [98], which is a literature review that focuses on the study of Metaverse and BC, in this, it is mentioned that interoperability will be the main driver of the metaverse. In the same work, it is mentioned that there are multiple security challenges for the management of health data in the metaverse. There is also the risk of data leakage, manipulation, or loss if the metaverse relies on a central storage system. In this and many cases, BC technology could provide an important role in finding a trade-off between interoperability and security within the metaverse.

VI.CONCLUSION

In this paper, we conducted a Systematic Literature Review on mechanisms and architectural elements aimed at improving the interoperability and security of HMS using BC. We have systematically analyzed, compared, and discussed 21 papers, corresponding to the same number of interoperability and security solutions in the field of BC technology. By methodologically exploring each of the solutions, this study provides interesting reflections, the first thing is to expose in a clear way the architectural mechanisms used to support solutions using BC in healthcare environments, among these are Frameworks, Gateways, Proxies, API, DSL's, MDE, among others. The second thing is to analyze, describe and classify architectural tactics used to solve interoperability and security concerns of HMS using BC. As a third point,

we generate 7 high-level scenarios, which represent 7 ways to address the architectural level solutions using BC in the healthcare field, in each of these we describe its context, a problem, analyze interoperability and security concerns, and then describe and analyze some trade-offs used to balance the interoperability and security of the healthcare ecosystem using BC. As a fourth point, We present a MDE Framework for blockchain interoperability and security. This framework consists of a high-level architecture that has as a central element the creation of a DSL that will be used for the translation of SC independently of the BC platform, to validate this architecture, we design an MDE experiment, which will allow us to validate the whole MDE process, This experiment seeks to look at the feasibility and determine if we are working at the right abstraction levels for the generation of SC between different BC platforms. In addition, it will allow us to make adjustments to the process and strengthen the components that are well-defined.

Our results allow us to conclude that the conditions are met to investigate the architectural elements using BC, around the interoperability and security of healthcare environments, allowing a multitude of new use cases. Thus, we expect that interest in this area of research will increase considerably. This work is aimed at making the BC ecosystem more practical, facilitating the work of developers and researchers. We hope that this study will provide a solid and reliable starting point for developers and researchers to work in the research area of software architecture, interoperability, and security of HMS using BC. Finally, we can say that Model-Driven Engineering (MDE) is being used in this type of solution to optimize productivity and improve software quality, maintenance, and interoperability of the entire healthcare ecosystem.

In the near future, we will perform characterization of the different types of SC, for the generation of the metamodels required in the development process of our DSL, then we will proceed with the development process of all the components of the DSL. After this, and to make adjustments and improvements to our experiment, put it in a real context, make measurements, and evaluate our mechanism, we will generate two case studies, the first one is related to the process of patient referral between hospitals that use within their HMS the BC technology, the second study will be related to the management by BC and SC of a dataset of examinations of the functionality of the elderly, this dataset is the result of the 4ie project.8 Each of these case studies will be evaluated following the Architecture Tradeoff Analysis Method (ATAM) [97], which will allow us to evaluate our software architecture based on the quality attributes of interoperability and security, considered in our system. In future installments, we will publish the results of the case studies and expand the discussion on the trade-offs to be had between interoperability and security of HMS using BC within the healthcare ecosystem.

II. 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]. Ravindra Changala, "Brain Tumor Detection and Classification Using Deep Learning Models on MRI Scans", EAI Endorsed Transactions on Pervasive Health and Technology, Volume 10, March 2024.

[6]. Ravindra Changala, "Sentiment Analysis in Social Media Using Deep Learning Techniques", International Journal of Intelligent Systems and Applications in Engineering, 2024, 12(3), 1588–1597.

[7]. 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.

[8]. T. Benson, Principles of Health Interoperability HL7 and SNOMED, New York, NY, USA:Springer, pp. 1-316, 2012.

[9]. Ravindra Changala, "Integration of IoT and DNN Model to Support the Precision Crop", International Journal of Intelligent Systems and Applications in Engineering, Vol.12 No.16S (2024).

[10]. Ravindra Changala, "UI/UX Design for Online Learning Approach by Predictive Student Experience", 7th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2023 - Proceedings, 2023, pp. 794–799, IEEE Xplore

[11]. 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.

[12]. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", Decentralized Bus. Rev., vol. 5, pp. 21260, Oct. 2008.

[13]. C. Burniske, E. Vaughn, J. Shelton and A. Cahana, How Blockchain Technology Can Enhance EHR Operability, St. Petersburg, FL, USA:Ark Invest, 2016.

[14]. Ravindra Changala, "Optimization of Irrigation and Herbicides Using Artificial Intelligence in Agriculture", International Journal of Intelligent Systems and Applications in Engineering, 2023, 11(3), pp. 503–518.

[15]. Ravindra Changala, Development of Predictive Model for Medical Domains to Predict Chronic Diseases (Diabetes) Using Machine Learning Algorithms And Classification Techniques, ARPN Journal of Engineering and Applied Sciences, Volume 14, Issue 6, 2019.

[16]. 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.

[17]. L. Bass, P. Clements and R. Kazman, Software Architecture in Practice, London, U.K.:Pearson, 2012.

[18]. 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.

[19]. Ravindra Changala, “Evaluation and Analysis of Discovered Patterns Using Pattern Classification Methods in Text Mining” in ARPN Journal of Engineering and Applied Sciences, Volume 13, Issue 11, Pages 3706-3717 with ISSN:1819-6608 in June 2018.

[20]. Ravindra Changala “A Survey on Development of Pattern Evolving Model for Discovery of Patterns in Text Mining Using Data Mining Techniques” in Journal of Theoretical and Applied Information Technology, August 2017. Vol.95. No.16, ISSN: 1817-3195, pp.3974-3987.

[21]. 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.

[22]. 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.

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

[24]. Ravindra Changala, Framework for Virtualized Network Functions (VNFs) in Cloud of Things

Based on Network Traffic Services, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume 11, Issue 11s, August 2023.

[25]. Ravindra Changala, Block Chain and Machine Learning Models to Evaluate Faults in the Smart Manufacturing System, International Journal of Scientific Research in Science and Technology, Volume 10, Issue 5, ISSN: 2395-6011, Page Number 247-255, September-October-2023.

[26]. C. Agbo, Q. Mahmoud and J. Eklund, "Blockchain technology in healthcare: A systematic review", Healthcare, vol. 7, no. 2, pp. 56, 2019.

[27]. 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.

[28]. Ravindra Changala, A Novel Prediction Model to Analyze Evolutionary Trends and Patterns in Forecasting of Crime Data Using Data Mining and Big Data Analytics, Mukt Shabd Journal, Volume XI, Issue X, October 2022, ISSN NO: 2347-3150.

[29]. Ravindra Changala, MapReduce Framework to Improve the Efficiency of Large Scale Item Sets in IoT Using Parallel Mining of Representative Patterns in Big Data, International Journal of Scientific Research in Science and Technology, ISSN: 2395-6011, Volume 9, Issue 6, Page Number: 151-161, November 2022.

[30]. 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.

[31]. 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.

[32]. Ravindra Changala, “Secured Activity Based Authentication System” in " in Journal of innovations in computer science and engineering (JICSE), Volume 6, Issue 1,Pages 1-4, September 2016.ISSN: 2455-3506.

[33]. Ravindra Changala, “Automated Health Care Management System Using Big Data Technology”, at Journal of Network Communications and Emerging Technologies (JNCET), Volume 6, Issue 4, April (2016), 2016, pp.37-40,ISSN: 2395-5317, ©EverScience Publications.

[34]. Ravindra Changala, "Retrieval of Valid Information from Clustered and Distributed Databases" in Journal of innovations in computer science and engineering (JICSE), Volume 6, Issue 1, Pages 21-25, September 2016.ISSN: 2455-3506.

[35]. 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.