A Comprehensive Review of Blockchain-Based Electronic Health Records Management and Future Research Directions

Mr.Dr.Paritala Chiranjeevi

Associate Professor,

Department of Computer Applications

Amrita Sai Institute of Science and Technology, Paritala AP

Mogalla Phanindra Kumar

MCA Student

Department of MCA

Amrita Sai Institute of Science, and Technology, Paritala, AP

ABSTRACT_ Electronic Wellbeing Records (EHRs) are electronically-put away wellbeing data in a computerized design. EHRs are ordinarily divided between medical services partners and face power disappointment, information abuse, absence of protection, security, and review trail. Then again, blockchain is the progressive creation of the 20th century that offers a conveyed and decentralized setting to impart among hubs in a rundown of organizations without a focal power. It can address the impediments of EHRs the executives and give a more secure, got, and decentralized climate for trading EHRs information. Three classifications of blockchain-based potential arrangements have been proposed by specialists to deal with EHRs: calculated, model, and executed. This study zeroed in on a Deliberate Writing Survey (SLR) to find and dissect articles submitted either reasonable or executed to oversee EHRs utilizing blockchain. The review inspected 99 papers that were gathered from different distribution classifications. The profound specialized investigation zeroed in on assessing articles in light of protection, security, adaptability, availability, cost, agreement calculations, and the kind of blockchain utilized. The SLR found that blockchain innovation vows to give decentralization, security, and protection that customary EHRs frequently need. In addition, results got from the itemized examinations would furnish possible analysts with the kind of blockchain for future exploration. At long last, future exploration bearings, eventually, would guide excitement to join new blockchain-based frameworks to appropriately oversee EHRs.

1.INTRODUCTION

Block chain has been a trendy expression in Data and Correspondence Innovation industry as of late. The ascent of this new innovation has more prominent possibilities to tackle

information protection, security, and trustworthiness issues. The word block chain came in the forefront after the distribution of the Piece coin white paper by Satoshi Nakamoto in 2008. The key instrument behind Piece coin is to make monetary exchanges conceivable without the mediation of a confided in outsider. The innovation is primarily viewed as a conveyed Companion to Peer(P2P) network where computerized information may freely or secretly be designated to all clients on the web in a protected and undeniable manner. In conventional monetary exchanges, both source and recipient need to rely upon a Confided in Outsider (TTP), e.g., bank. It includes a couple of safety issues and functional challenges. For example, a TTP gains admittance to a client's monetary information, which demonstrates the absence of client security. Besides, the time engaged with a TTP exchange is extended as there are many in the middle of between the activity. Moreover, clients need to pay the TTP for their administration. Bit coin settles the above restrictions and causes the TTP to disappear for a fruitful exchange between two clients .

The viable Piece coin digital currency came into the market in 2009. Notwithstanding, since the code for Cycle coin was open source, different software engineers could alter and further develop Touch coin. The block chain innovation has advanced in various phases.1

_ Block chain 1.0: The utilization of Circulated Record Innovation (DLT) added to the first and most perceptible utilization of the innovation: digital forms of money. Block chain 1.0 is the first digital currency that utilizes a straightforward instrument to screen bit coin exchanges on a common record.

_ Block chain 2.0: Doing exchanges through a few lawfully restricting strategies, likewise called Brilliant Agreements, which are produced from a bunch of little PC programs, is viewed as block chain 2.0. The most conspicuous block chain in stage 2.0 is Ethereum.

_ Block chain 3.0: The following manifestation in this innovation is block chain 3.0, which centers around Decentralized Applications (D Applications) by staying away from unified foundation. Not at all like conventional applications, D Applications store and convey through decentralized capacity and decentralized server. The point of block fasten 3.0 was to advocate block chain among regular areas, government, wellbeing, and training.

_ Block chain 4.0: It gives arrangements and strategies that can satisfy a few business needs of Industry 4.0, which includes computerization, asset arranging, and mix of different execution programs. It requires upgraded trust and security which can be met by block chain.

Many studies have been distributed on the utilization of block chain in different regions. Among these papers, many were deliberate audits on the use of block chain in medical services areas .Specialists talked about block chain innovation's limits, potential applications, and future bearings in medical care, government, production network, and numerous different fields. We have proposed a complete SLR on the use of block chain to oversee EHRs.

2.LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company Traffic Redundancy Elimination, once these things are satisfied, then next steps are to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system we have to known the below concepts for developing the proposed system

1) A new general framework for secure public key encryption with keyword search

Public Key Encryption with Keyword Search (PEKS), introduced by Boneh et al. in Eurocrypt’04, allows users to search encrypted documents on an untrusted server without revealing any information. This notion is very useful in many applications and has attracted a lot of attention by the cryptographic research community. However, one limitation of all the existing PEKS schemes is that they cannot resist the Keyword Guessing Attack (KGA) launched by a malicious server. In this paper, we propose a new PEKS framework named Dual- Server Public Key Encryption with Keyword Search (DS-PEKS). This new framework can withstand all the attacks, including the KGA from the two untrusted

2)Searchable symmetric encryption: Improved definitions and efficient constructions

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search

over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions.

Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction.

3.PROPOSED WORK

EHR contains sensitive personal data (for example, a patient's medical history). As a result, the security and privacy of such information are critical. Medical institutes in poor countries are required to follow the government's rules. As a result, preserving and disseminating EHR data is difficult. EHR management, on the other hand, presents numerous technical challenges. Central medical servers, for example, have limited capacity, are subject to single-point failure, and are vulnerable to insider attacks. Even patients are unaware of where their sensitive data is housed or how it is shared. However, because people currently are mobile, interoperability among diverse healthcare providers can deliver better health recommendations.

3.1 IMPLEMENTATION

Server

In this module, the Admin has to login by using valid user name and password. After login successful he can do some operations such as Login, View All Hospitals and Authorize, View All Clients and Authorize, Add Block chain Code, View All Block chain Code, View All Patient Details, View All Transactions, View All SK Request and Response Details, View All SK Requests and Permit, View All Credential Attackers Details, Trace and View All Disease Records by Block chain, View No. of Same Disease in Chart, View Patient Searched Rank in chart, View Patient File Rank in chart, View No. Of Attackers on Patient.

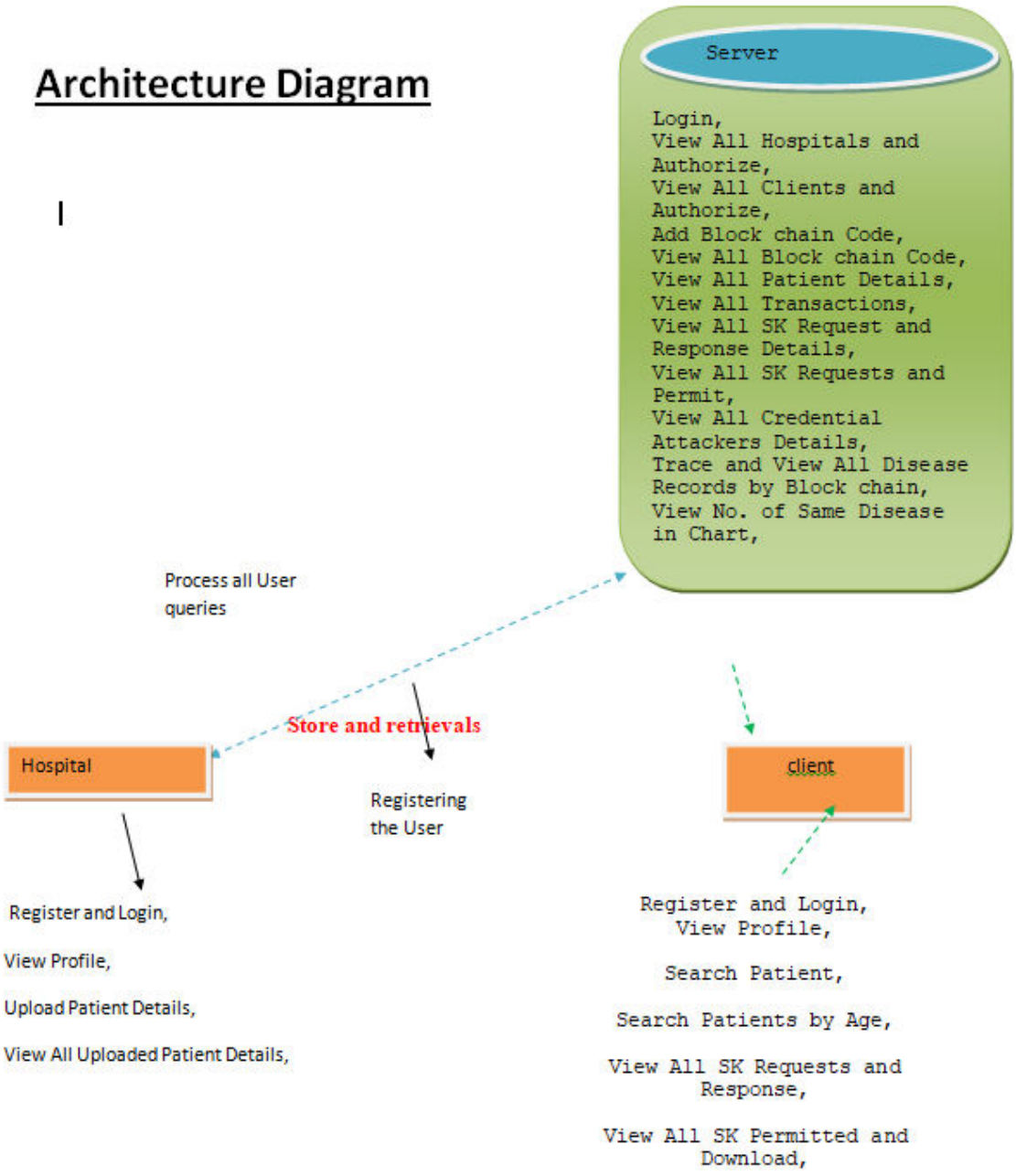
Client

In this module, there are n numbers of users are present. User should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Register and Login, View Profile, Search Patient, Search Patients by Age, View All SK Requests and Response, View All SK Permitted and Download,

Hospital

In this module, there are n numbers of users are present. Hospital user should register with group option before doing some operations. After registration successful he has to wait for admin to authorize him and after admin authorized him. He can login by using authorized user name and password. Login successful he will do some operations like Register and Login, View Profile,

Upload Patient Details, View All Uploaded Patient Details,



4.CONCLUSION

This study responds to the subject of the present status of the workmanship in block chain-based EHR the executives examination and future bearings. We showed the conveyance of block chain types and stages embraced by the evaluated articles. The possible advantages of block chain to oversee EHRs have met partners' assumptions in the medical services areas, while we additionally found that few difficulties require further examination. For example, cross-line sharing of EHR information might be hampered by differing and frequently

clashing regulation. In addition, the security strategies likewise fluctuate in light of the particular unofficial law. Subsequently, further examination on guideline, normalization, and cross-line openness of EHRs is vital.

In any case, After careful examination of chosen articles, we presumed that the most conspicuous block chain stage for EHR the board is Ethereum (private) and Hyper record Texture on the grounds that these two stages meet practically every one of the prerequisites. We likewise found that taking care of enormous EHR information for a huge scope with block chain has constraints, for example, restricted capacity limit, calculation cost, and correspondence cost. In any case, there are expected answers for conquer these limits, like man-made reasoning, IOMT, and edge processing.

The review might act as a source of perspective for future examination in this _eld. The collection of every single related paper, their commitments, and constraints will assist the expected specialists with planning another engineering or model. Also, future exploration headings to join blockchain could assist with proposing additional astonishing answers for the current issues.

REFERENCES

S. Nakamoto, ``Bitcoin: A peer-to-peer electronic cash system," *Decen- tralized Bus. Rev.*, 2008, Art. no. 21260.

A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, ``Implementing blockchains for ef_cient health care: Systematic review," *J. Med. Internet Res.*, vol. 21, no. 2, Feb. 2019, Art. no. e12439.

M. Hölbl, M. Kompara, A. Kami²ali¢, and L. N. Zlatolas, ``A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, Oct. 2018.

C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, ``Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, p. 56, Apr. 2019.

E. Chukwu and L. Garg, ``A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," *Access*, vol. 8, pp. 21196_21214, 2020.

S. Khezr, A.Yassine, and R. Benlamri, ``Blockchain technology in healthcare:

A comprehensive review and directions for future research," *Appl. Sci.*, vol. 9, no. 9, p. 1736, 2019.

I. Ahmed, M. Ahmad, G. Jeon, and F. Piccialli, ``A framework for pandemic prediction using big data analytics," *Big Data Res.*, vol. 25, Jul. 2021, Art. no. 100190.

R. Vaishya, M. Javaid, I. H. Khan, and A. Haleem, ``Arti_cial intelligence (AI) applications for COVID-19 pandemic," *Diabetes Metabolic Syndrome: Clin. Res. Rev.*, vol. 14, no. 4, pp. 337_339, Jul. 2020.

L. Houston, Y. Probst, and A. Humphries, ``Measuring data quality through a source data veri_cation audit in a clinical research setting," *Stud. Health Technol. Inform.*, vol. 214, pp. 13_107, Jan. 2015.

M. Muthuppalaniappan and K. Stevenson, ``Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health," *Int. J. Qual. Health Care*, vol. 33, no. 1, Feb. 2021.

M. S. Rahman, I. Khalil, P. C. Mahawaga Arachchige, A. Bouras, and X. Yi, ``A novel architecture for tamper proof electronic health record management system using blockchain wrapper," in *Proc. ACM Int. Symp. Blockchain Secure Crit. Infrastruct. (BSCI)*, 2019, pp. 97_105.

H. Wu, Y. Shang, L. Wang, L. Shi, K. Jiang, and J. Dong, ``A patient-centric interoperable framework for health information exchange via blockchain," in *Proc. 2nd Int. Conf. Blockchain Technol. Appl.*, Dec. 2019, pp. 76_80.

S.Wu and J. Du, ``Electronic medical record security sharing model based on blockchain," in *Proc. 3rd Int. Conf. Cryptogr., Secur. Privacy (ICCSP)*, 2019, pp. 13_17.

A. Fernandes, V. Rocha, A. F. D. Conceicao, and F. Horita, ``Scalable architecture for sharing EHR using the hyperledger blockchain," in *Proc. Int. Conf. Softw. Archit. Companion (ICSA-C)*, Mar. 2020, pp. 130_138.

A. A. Mamun, A. Al Mamun, S. R. Hasan, S. R. Hasan, M. S. Bhuiyan, M. S. Bhuiyan, M. S. Kaiser, M. S. Kaiser, M. Abu Yousuf, and M. A. Yousuf, ``Secure and transparent KYC for banking system using IPFS and blockchain technology," in *Proc. IEEE Region 10 Symp. (TEN- SYMP)*, 2020, pp. 348_351.

Wikipedia. *Cryptographic Nonce*. Accessed: Jan. 10, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Cryptographic_nonce

V. Buterin. (2016). *What is Ethereum*. [Online]. Available: http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html

Litecoin. *Litecoin_Open Source P2P Digital Currency*. Accessed: Jan. 8, 2021. [Online]. Available: https://litecoin.org/

E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, and K. Christidis, ``Hyperledger fabric: A distributed operating system for permissioned

blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1_15.

F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, ``Ripple: Overview and outlook," in *Proc. Int. Conf. Trust Trustworthy Comput.* Heraklion, Greece: Springer, 2015, pp. 163_180.

Quorum. *Build on Quorum, the Complete Open Source Blockchain Platform for Business*. Accessed: Jan. 7, 2021. [Online]. Available: https://consensys.net/quorum/

R. G. Brown, ``The corda platform: An introduction," *Retrieved*, vol. 27, p. 2018, May 2018.

S. Nadal and S. King, ``PPCoin: Peer-to-peer crypto-currency with proofof- stake," *Self Published Paper*, vol. 19, 2012.

F. Saleh, ``Blockchain without waste: Proof-of-stake," in *The Review of Financial Studies*. Oxford, U.K.: Oxford Univ. Press, 2018.

G. Wood, ``Polkadot: Vision for a heterogeneous multi-chain framework," Parity Technol., London, U.K., White Paper 21, 2016.