An Analytical Survey on Personal Health Record Access Control using Blockchain and Machine Learning

Aneesh Pillai[1] Parag Khankari[2] Shivshankar Giri[3] Vaibhav Ghatge[4] S. E. Ingale[5]
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]Modern Education Society's College Of Engineering, Pune, India

Abstract— For every citizen It is right to have a good medical treatment. Most of the time this kind of good treatments are only available in advanced countries like USA as these countries have strengthened their health care system. To provide immediate proper treatment these countries have a system of medical data vending, where doctors are seeking treatment history of already being treated, patient's data from either a patient or by a doctor through an authorized data vendor. In this process data vendor is a major component and a trustless party between seekers and data providers. However, to provide a stronger security for the data Blockchains is being introduced in the network. Many methodologies are existed to provide an access control mechanism for the demanded data to ensure the strict security for the service of data providing process. However, most of them are still working with traditional manual models, so to enhance this, this paper insists usage of machine learning mechanisms to enhance the access control mechanism with blockchains.

Keywords: BlockChain, Access Control Mechanism, Personal health Records

I. INTRODUCTION

Blockchain, generally mentioned and commonly known as a form of Distributed Ledger Technology (DLT), makes the history of any digital document unalterable and distinct through the utilization of decentralization and implementation of hashing schemes.

A simple analogy for understanding blockchain technology is analogous to creating a Google Doc for a group. Once we produce a document and share it with a bunch of individuals, the document is distributed rather than derived or transferred. This creates a decentralized distribution chain that offers everybody access to the document at an equivalent time. None of the users in the group are left out while awaiting changes from another party, whereas all modifications to the document created and the changes are being recorded all the time. The changes made on the document are logged clearly.

Of course, blockchain is a lot more difficult and complicated when compared to a Google Doc, however, the analogy is apt as a result of it illustrates 3 important concepts of the technology:

1) Digital assets security measures are distributed rather than derived or transferred.
2) The document is decentralized, permitting a full period of time access.
3) A clear ledger of changes preserves the integrity of the document, which creates trust within the plus.

Blockchain is a tamper-proof technology that is a particularly promising and revolutionary technology as a result, Blockchain can help scale back risk, stamp out fraud and bring transparency to an ascendible approach for myriad uses where security concerns are paramount.

Arguably the foremost logical use for blockchain is as a method to expedite the transfer of funds from one party to the receiver.

Blockchain additionally comes in handy once it involves observing the chains for identification of tampering. By removing paper-based trails, businesses ought to be ready to pinpoint inefficiencies among their offer chains quickly, also to find things in real-time through the Blockchain.

Blockchain may any revolutionize the retail expertise by turning into the go-to for loyalty rewards. By making a token-based system that rewards shoppers, and storing these tokens inside a blockchain, it might incentivize shoppers to come to a precise store or chain to try to their searching.

More than one billion individuals have encountered and have been victims of identity theft. Microsoft is one of the companies that want to reduce this occurrence and secure their premises. Its making digital IDs at intervals through the Microsoft appraiser app which provides the users the simplest way to regulate their digital identities and reduce fraud through Blockchain.

Blockchain can enable a high level of privacy and transparency in a transaction that can be validated at any time. For example, marijuana corporations will use blockchain as a method to record their sales and demonstrate to lawmakers that they are operating within the law and their sales are legitimated by native, state, and/or federal laws. Due to the inclusion of Blockchain, these sales act as a transparent record for the federal agency that they've paid their justifiable share of taxes to the central government and they are indeed profitable.

In a world with growing internet access, copyright and possession laws on music and alternative content have become really hazy. With blockchain, those copyright laws could be beefed up significantly for digital content downloads, guaranteeing that the creator or producer of the content being purchased gets their fair proportion of the reward and the sales.

Blockchain offers the flexibility to vote digitally, however, it's clear enough that any regulators would be able to see if one thing was modified on the network. This ensures that the elections are transparent and fair while being instantly auditable for anyone being apprehensive about the security of the system.

One of the primary goals of blockchain is to reduce the dependency on paper and eliminate it out of the equation. Since the paper trails usually increase the confusion level which is used smartly by the criminals to carry on their illicit activities. If you're buying or selling properties such as land, a house, or a car, you will have to transfer or receive a title physically on paper. Instead of handling this on paper, blockchain can store titles on its network, and perform a

All rights reserved by www.ijsrd.com

transparent scan of this transfer, which is equally valid as a crystal-clear image of legal possession.

Yet another intriguing use for blockchain may well be in tracing food from its origin to your plate. Since blockchain knowledge is immutable, you would be able to trace the transport of food merchandise from their origin to the grocery store, thereby guaranteeing the authenticity as well as eliminating any foul play on the item.

Blockchain may also be the right implementation on the cloud platform. Even if cloud storage systems are designed to be a go-to supply for information and other personal documentation, they don't seem to be protected against hackers, or maybe infrastructure issues where the blockchain paradigm can help a lot.

Blockchain applications at first were restricted to the cryptocurrencies and monetary transactions. The invention of smart contracts helped in the development of a lot of driver applications, like aid, IoT and offer chain. A few Research articles reviewed several analysis studies that supported blockchain and smart contracts, concluded that they have a tendency to concentrate on conferred applications for providing an economical and secure access management mechanism. Access management is much-needed security and should be a part of most applications. Blockchain specific characteristics like unchangeableness, durability, suitability, and responsibility proclaim that considering blockchain as a supplementary answer for access management systems is the right choice.

AI is that the new electricity and information is the new oil. These words are typically quoted throughout conference keynotes and on social media. Thomas Edison invented the electric bulb in 1878 and fast forward to 2019 – we cannot imagine our life without electricity. it's become an important part of our life. on an equivalent line, the initial AI applications were easy applications like a prediction. Nowadays we tend to witness extremely customized applications like book or film show recommendations, intelligent traffic route navigators, talking personal assistants, upbeat apps, early disease prediction, etc. to come up with extremely correct and personal recommendations, we want access to an oversized quantity of personal information, and this can be why technological giants like Google, Facebook, Amazon, and Microsoft dominate the AI market these days. "We don't have higher algorithms than anyone else; we tend to simply have additional information," admitted Google's director of Research - Peter Norvig. Hyper-personalization comes with an enormous value – loss of privacy. Events just like the Cambridge Analytics Scandal raised considerations regarding confidentiality and information privacy. Several international agencies are currently forming laws and laws for the protection of personal information like GDPR in Europe. Therefore, the application of Artifical Intelligence is highly useful and needs to be regulated.

This paper dedicates section 2 for analysis of past work as literature survey and section 3 concludes the paper with feasible statement of the literature study.

II. LITERATURE SURVEY

This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors work as follows.

W. Dai [1] explains, in both public sections and private sections decision making is necessary because it has the capacity to hold and process huge amounts of data easily which is crucial. There are numerous obstacles in conventional data trading platforms because of fraudulent buyers/ data brokers. The risks and the potential attack vectors can be represented in three sections such as ILR which denotes "Information Leakage during Running", RF denotes" Repudiation and Fraud", DF denotes" Data Forwarding". ILR arises during the implementation of the data analysis on the blockchain node. RF is an example of fraudulent activities performed by the purchaser. DF vendor is the original data that is forwarded to a third-party.

G. Magyar [2] introduces blockchain for the Health information ecosystem for solving the most prevalent issues concerning the lifelong recorded patient health data. The privacy of the patients is an emerging issue in hospitalization as the attacker and growing data hunger of the research can cause a plethora of attacks. Thus, the author introduces how the blockchain technique can assist solutions for the preservation of data, storing data, and availability at the same time. The accessibility of the data in a blockchain can be permissioned or permission less. Maintenance of security, validity, and integrity of the blockchain with the well-known legal entity comes under the permissioned blockchain. In a permission less blockchain, the security and integrity preserved under independent peers.

Dr. M. Kumar [3] estimates that effective network monitoring and auditing can help the administrator to recognize the compounded attack pattern and the attacker's plan of actions. Tamper-proof rigid chain of records is created by the BlockChain. Once the block is written it cannot be changed. The use of a cryptographic technique to compute cryptographic hashes is provided for each block and also the value of the previous block is stored in the current block, this how a chain is created by the blockchain software. The four major functional components of the proposed system are Log Generators Devices, Local Log Server, Log Monitoring Client, Logging Cloud Server. Thus it gives a safe log storage platform for a long time.

Z. Guan [4] narrates that the amount of data in the world is increasing dramatically every day. Due to the development of information and communication, technology has taken the data storage capability to the next level. In the paper, the author has introduced two new schemes for fair and efficient data trading schemes that do not rely on any third party using the blockchain. The first scheme executes direct raw data exchange for large amounts of data. The second scheme executes data statistics trading. To evaluate their performance both the schemes are developed with smart contracts, and conduct comprehensive experiments. The results of the proposed paper indicate that the proposed methodology is highly efficient in trading data.

M. Chowdhury [5] proposes the techniques for safeguarding critical and sensitive private information like personal data such as electronic medical records and

All rights reserved by www.ijsrd.com

academic records. This personal information is usually provided across many data governance groups systems. To secure the data of an individual the technique can store, manage and deploy in a highly secure way using the service of Personal Data Store (PDS). Currently, most traditional organizations such as hospitals, universities, banks, etc. utilize web-enabled systems that host clients' data. Freshly, online social networks e.g., Facebook, Twitter, and LinkedIn reform the human's attitude regarding data sharing.

M. Shen [6] presents the technique of the privacy-preserving SVM training scheme named secure SVM, which gets to grips with challenges of data privacy and data integrity by using blockchain techniques. For efficient and accurate privacy-preserving methodology an SVM training algorithm is developed by using a Homomorphic cryptosystem Paillier. The main contributions of the paper are that the authors appoint blockchain techniques to enable secure and reliable IoT data sharing. They have developed a secure SVM training algorithm by designing and securing building blocks, such as secure polynomial multiplication and secure comparison. With relatively high accuracy, SVM classifiers have been trained. Considerable experiments have depicted good efficiency of the proposed scheme

U. Uchibeke [7] elaborates heterogeneous data is generated ranging from agriculture, business, banking to education, medicine and healthcare has been rapidly developed. Opportunities that were not available before have been opened now due to the Big Data concept. At the same time data is continuously increasing since more flexible data processing software is available. In Cloud Computing Technology most of the new big data solutions are developed. Significant interest in such cost-effective and reliable, scalable and distributed computing of large datasets is because of cloud computing environments.

S. Ramamoorthy [8] proposed that the data centers perpetuate the data storage devices which stock the data collected from the more than one member's user groups in cloud computing. The storage as a service (SaaS) is a sample for storage space provided by the cloud to its end users. The real-time examples of cloud storage space are Amazon Simpl Storage Systems (S3), EMC Mozy, Rackspace. The proposed paper aims to secure cloud data by developing the new technique using blockchain technology. To ensure the data security among the community cloud users the Hybrid approach to combine the BlockChain(BC). The malevolent data access and modifications the blockchains allow the user to trace.

W. Liang [9] explains the wide application of industrial IoT also leads to great duress. Due to this industrial Internet of Things (IIoT), productivity efficiency has been greatly upgraded. The security problems in data transmission, many organizations have held secure data transmission techniques in industrial IoT. The power blockchain technique is traceable, consensus, anti-tampering and unlocked. A chain collected of well-ordered data blocks and each block contains a time-stamp and a block mark. The power data security should be validated. Data transmission method can be used in the IoT industry, such as power, energy.

P. Urien [10] provides the solution to the double-spending issues utilizing a peer-to-peer distributed timestamp server to create a computational proof of the chronological order of undertaking. Blockchain platform for enabling the security relies on three main pillars: Transactions, Block mining, Distributed Ledger. CryptoCurrency Smart Card (CCSC) developed over a JC3.04. Traditional platform with the detailed interface. There are two cases to be detailed, the first one deals with the deployment of the CCSC software in less cost and less power due to the fact that the object is sponsored by an open hardware (Arduino) platform, and included sensor data transactions and second deals with the cloud of CCSC java cards plugged to RACS servers.

C. Cai [11] estimates that the blockchains are emerging as novel tools that are functional for financial organizations and different other application scenarios such as for health care systems. There are two types of blockchain: public, consortium. Such public blockchain is recommended by services needed for the process logs to be publicly released for testing. Financial software like mortgage system generally seek good privacy protection and thus turn to consortium blockchain instead. Unique challenges differentiate with traditional applications by using the blockchain technique. The proposed system is secure and trustworthy blockchain applications at their workplaces.

S. Sharma [12] proposes Blockchain as one of the most progressing and resourceful technologies of cloud security. The use of cryptographic data structures for the making of Blockchain is enormously thought-provoking. Blockchain and contrast the different platforms on which blockchain can be developed. Developing a secure environment of cloud computing is proposed in Blockchain applications. To identify the owners, the Blockchain digital identity gives additional control over personal information. Enforces security and integrity of the data on cloud platforms which confirms that Blockchain is the most powerful technique.

X. Zheng [13] explains wearable technology and wireless sensing, people are using various types of mobile and wearable devices, such as smartphones, smartwatch, smart band, and smart glasses, etc only because of the rapid development of mobile computing. By using wearable technology and wireless sensing devices we get a huge amount of data regarding health such as remote diagnosis, disease monitoring, and elderly people monitoring. These data which are collected are valuable resources for healthcare research and business applications. Thus the author has provided an efficient way to collect high-quality personal health data commercial purposes.

C. Liu [14] narrates the growth of smart portable mobile terminals MTs, such as smartphones, UAVs, which are fitted with sensors such as camera, gyroscope, and GPS), has assisted a new type of data collection technique for industrial IoT (IIoT). A cloud-based server and a collection of MTs are provided in a typical MCS system. The author proposed a connected application that combines energy-efficient data collection and secure data sharing among MTs activated by blockchain. The proposed experiments produce effective results when compared with traditional data storage.

M. Singh [15] estimates that the Blockchain technique is now attracting too much attention from software scientists since it has been created. It has largely two fields that are going to be determined by creating a decentralized system that removes central servers and provides peer-to-peer

All rights reserved by www.ijsrd.com

interaction and second by creating a fully transparent and open to all database. Components of a Blockchain are Network of Nodes, Distributed database system, Shared ledger, Cryptography. Blockchain can be mainly deployed in 3 domains Public, Consortium area and Private. Thus proposed blockchain is a solution to IoT Security.

III. Conclusion

This paper specially concentrating on providing the privacy for the healthcare data using the Artificial intelligence and Blockchain concept. For this reason, this paper studies the past developed system to identify their limitations. This study reveals some facts like most of the systems are using the access control mechanism in manual mode and very fewer are weaved in the model of health care sector in real time. By keeping this fact in the mind this paper proposes a model for providing the automatic access control using the machine learning models like Fuzzy Artificial neural network and random forest classification which is powered with the blockchain concept for the secure data transmission over the network.

References

[1] Weiqi Dai, Chunkai Dai, Kim-Kwang Raymond Choo, Changze Cui, Deiqing Zou, and Hai Jin," SDTE: A Secure Blockchain-based Data Trading Ecosystem " IEEE Transactions on Information Forensics and Security, 2020.
[2] Gábor Magyar," Blockchain: solving the privacy and research availability tradeoff for EHR data" 2017 IEEE 30th Jubilee Neumann Colloquium • November 24-25, 2017 • Budapest, Hungary, 2017.
[3] Dr. Manish Kumar, Ashish Kumar Singh, V Suresh Kumar," Secure Log Storage Using Blockchain and Cloud Infrastructure" 12, 2018, IISC, Bengaluru sBengaluru, India, 2018.
[4] Zhangshuang Guan, Xiaobei Shao and Zhiguo Wan," Secure, Fair and Efficient Data Trading without Third Party Using Blockchain" 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, 2018.
[5] Mohammad Jabed Morshed Chowdhury, Alan Colman, Muhammad Ashad Kabir, Jun Han and Paul Sarda," Blockchain as a Notarization Service for Data Sharing with Personal Data Store" 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering, 2018.
[6] Meng Shen, Member, Xiangyun Tang, Liehuang Zhu, Xiaojiang Du, and Mohsen Guizani," Privacy-Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities ": DOI 10.1109/JIOT.2019.2901840, IEEE Internet of Things Journal, 2019.
[7] Uchi Ugobame Uchibeke, Sara Hosseinzadeh Kassani , Kevin A. Schneider," Blockchain access control Ecosystem for Big Data security" 2018 IEEE Confs on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, Congress on Cybermatics, 2018.
[8] S. Ramamoorthy, B.Baranidharan," CloudBC-A Secure Cloud Data acess Management system" 978-1-5386-9371-1/19/$31.00c, IEEE, 2019.
[9] W. Liang, M. Tang, J. Long, X. Peng, J. Xu and K. C. Li, "A Secure Fabric Blockchain-based Data Transmission Technique for Industrial Internet-of-Things" 1551-3203 (c) 2018 IEEE, 2018.
[10] Pascal Urien," Towards Secure Elements for Trusted Transactions in Blockchain and Blochchain IoT (BIoT) Platforms. " Second Conference on Mobile and Secure Services, 26-27 February 2016.
[11] Chengjun Cai, Huayi Duan, and Cong Wang," Tutorial: Building Secure and Trustworthy Blockchain Applications" 2018 IEEE Secure Development Conference, 2018.
[12] Shweta Gaur Sharma, Dr. Laxmi Ahuja," Building Secure Infrastructure for Cloud Computing using Blockchain" IEEE Xplore Compliant Part Number: CFP18K74-ART; ISBN: 978-1-5386-2842-3, 2018.
[13] Xiaochen ZhengRaghava Rao Mukkamala, Ravi Vatrapu, Joaqun Ordieres-Mer,'' Blockchain-based Personal Health Data Sharing System Using Cloud Storage" 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), 2018.
[14] Chi Harold Liu, Senior Member, Qiuxia Lin, Shilin Wen," Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning " 1551-3203 (c), IEEE, 2018.
[15] Madhusudan Singh, Abhiraj Singh, Shiho Kim," Blockchain: A Game Changer for Securing IoT Data" Designing, Developing, and Facilitating Smart Cities, Springer International Publishing, 2017.

All rights reserved by www.ijsrd.com