Secure Cloud Storage Utilizing Blockchain for Productive Search

Meena Kumari K S[1] Nazia Nusrath Ul Ain[2]

[1]Assistant Professor, Department of Computer Science and Engineering
[2]Assistant Professor, Department of Information Science and Engineering
Brindavan College of Engineering Bangalore – 560063 India

Abstract: Blockchain Technology has received huge recognition, with a rapid interest in various applications, ranging from information management, cyber security, IoT, healthcare and economic services. There was an outstanding interest witnessed in utilizing applications of blockchain for the transport of secure and comfortable healthcare records. Furthermore, blockchain is transforming the customary medicinal services practices into a more reliable means, in terms of effective diagnosis and treatment through safe and secure records sharing.

Within the future, blockchain will be an era that could potentially help in personalized, true, and comfortable healthcare through merging the entire actual-time medical records of a patient's health and providing it in a secure healthcare setup. In this paper, we are applying health sensor data to the new technology which is called as blockchain and storing these health sensor data to cloud storage.

Keywords: Blockchain, Blockchain healthcare systems, Cloud Computing, Cloud Storage.

1. INTRODUCTION

Within the evolution of distributed systems, clouds have come to be a new trend and grid computing being the forerunner. Cloud computing become introduced within the industry through the companies like Microsoft, sales force, Amazon, Google and Yahoo. Cloud computing has centralized server resources in a disbursed structure such that it is able to offer on-demand service or resources on a scalable platform. Cloud computing is based on pay-on-usage version for permitting convenient and offer access to a shared pool of configurable sources [1][2]. Cloud computing applications are commonly rated below subscription model. The cloud based services not only prohibited for software applications.

Cloud storage is a service that keeps records, manages and backup remotely and made records available to customers over the network (through net). There are numerous cloud storage vendors like Drop Box, Google drive, box, Amazon, Apple Cloud and Microsoft SkyDrive [3]. Client need to pay amount according to the plan if they pass the free space restriction. Through using cloud storage service, clients need not make investments on storage devices even technical assist isn't required for maintenance, he storage, backup, disaster recovery [4]. The idea of cloud storage in not really worth while the customer is capable of store and control the data at low price when compared thru using cloud .So, the cloud have to be designed in such a way that it is price effective, autonomic computable, multi-tenant, scalable, available, manage, efficient [5].

TABLE I
Overview of Cloud Computing

Deployment Models	Essential Characteristics	Service model
Public	On Demand Service	SaaS
Private	Broad Network Access	PaaS
Hybrid	Resource Pooling Rapid Elasticity	IaaS
Community	Measured Services	

Cloud storage architecture includes the front-end, middleware, back-end. The front-end may be web-service front-end, record based the front-end, and even more conventional the front-ends. The middleware includes storage logic which implements numerous capabilities like replication, data reduction, data placement algorithms. The back-end implements the physical storage for data. The access techniques for cloud are different from conventional storage because the cloud holds different kind of data of various clients. Most of the vendors implement multiple access techniques [6].

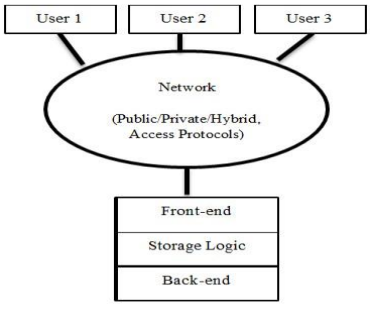


Fig. 1 General Cloud Storage Architecture

Blockchain is a dispensed framework recording and putting away exchange data. Exceptionally, blockchain is a shared, immutable file of peer-to-peer transactions built from related transaction blocks and saved in a digital ledger.

Blockchain is based on set up cryptographic strategies to permit every player in a community to engage (e.g. save, trade, and look at records), without pre-existing belief among the events. In a blockchain system, there may be no

critical authority; rather, transaction data are saved and allotted throughout all community contributors. Interactions with the blockchain become recognized to all members and require verification via the community earlier than records is brought, allowing trustless collaboration among community individuals whilst recording an immutable audit path of all interactions [9].

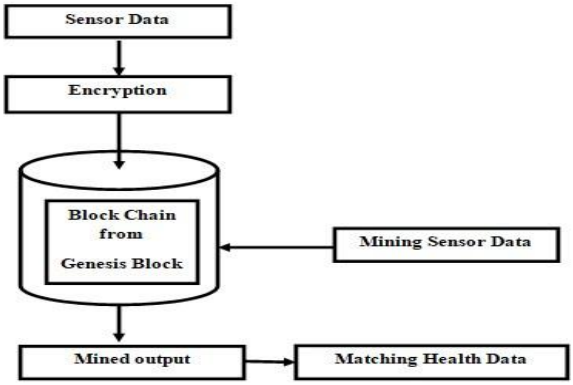


Fig. 2 System Architecture

The Implementation is carried out on the Raspberry Pi board. The Genesis Block developed for the implementation of the health care security implementation that is taken in this implementation would get the data from the Heart rate and the Blood Pressure Sensor and those values are got as the transaction and provided to the Blockchain for the development of the security process..

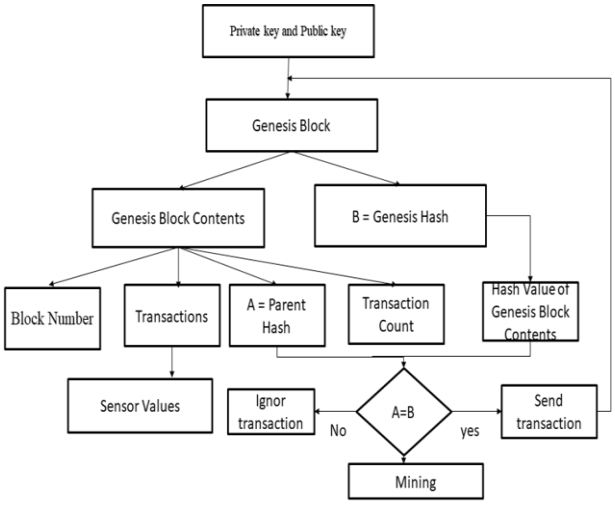


Fig. 3 The Overall Flow Chart of the Proposed Implementation

The Mining process is involved at the end of the data acquisition process to know whether there is a person with similar health condition in observed in the past. The mining is carried out using the Hash value generated from the block creation. Then the value obtained from the block is taken and compared using correlation coefficient to find out person having similar health status. Thus this implementation would reduce the cost of diagnostics of the patient by having the reference of the patient data in a decentralized manner

2. RELATED WORK

Blockchain's ability to enable higher health records sharing and ownership has been formerly described through several authors. Using a public or private blockchain to truly save medical records is one example-for instance, Yue et al. defined a "Healthcare records Gateway" (HRG) which might allow patients to control their personal health records saved on a private blockchain [7]. In addition, Ivan defined a public blockchain implementation, wherein healthcare records is encrypted but saved publicly, developing a blockchain-based private health record [8].

MedChain is another instance, wherein a permissioned network of medicine stakeholders (such as the patient) may be used to facilitate medicine-precise records sharing among patients, hospitals, and pharmacies [9]. Even as we consider that a model storing real medical records on a blockchain-permissioned or public-might have massive privateness and scalability issues, it is vital to continue to recognize the privateness and safety implications of on-chain records storage. Another technique to sharing health records leverages blockchain not for the storage of the real medical records, however for facilitating management or governance of those records [9].

Zyskind et al. have described a preferred- cause decentralized get entry to and manage supervisor for encrypted off-chain records; the blockchain layer enforces access manage guidelines, however records is saved off chain [10]. within the healthcare space, FHIRChain is a smart-agreement based system for exchanging health records based on the standard FHIR [11], wherein medical records is saved off chain, and the blockchain itself stores encrypted meta-records which function pointers to the primary records source (like an EHR) [12].

Azaria et al. brought MedRec, which makes use of a permissioned blockchain network to facilitate records sharing and authentication. MedRec has a unique evidence-of-work incentive method constructed round access to anonymized medical records (for studies, for instance) [13]. Subsequently, Dubovitskaya et al. also suggest a permissioned blockchain (targeted on oncologic care) which leverages off-chain cloud garage for medical records, using the blockchain to manage consent and authorization [14].

Each MedRec and Dubovitskaya's work were prototyped but do not look like operational. Moreover, it is really worth noting that within the drive toward patient driven interoperability, blockchain won't be the only answer. Private, supplier-based solutions can also take maintain. For instance, Apple recently introduced a product that might permit patients to pull their medical EHR records from collaborating institutions using APIs (based on FHIR and the Argonaut assignment specification) [15]. further, Sync four technology is a pilot attempt to allow patients to

make a contribution their EHR records to research efforts, additionally thru standard APIs, using an authorization workflow(i.e., the records need never be saved or controlled through the patient personally) [16]. Although the concept of a virtual private health record has been defined for many years, there was noticeable traction from an era and regulatory perspective in latest years.

3. BLOCKCHAIN

Blockchain is a distributed ledger technology wherein transactions are bundled into blocks which are chained together cryptographically through hash pointers. Blockchain solutions upload believe and privacy to the present net because of its tampering resistance and superior cryptography traits.

A. How Blockchain Works

The term "Blockchain" refers to the manner BC stores transaction records – in "blocks" that are linked together to form a "chain." The chain grows as the number of transactions increases. Since each entry is saved as a block on a chain, the care you receive is added for your private ledger. At its center, blockchain is a disseminated framework recording and storing transaction data. In a blockchain system, there's no central authority. Rather, transaction data are saved and distributed throughout all network members. In place of having a centrally located database that manages data, the database is distributed to the networks, and transactions are stored comfortably through cryptography. Blockchain removes the need for a middleman that historically can also facilitate such transactions. The Blockchain was designed so transactions are immutable, i.e. they can't be deleted. Therefore, Blockchains are comfortable and meddle-free via design. Records may be distributed, however not copied. In terms of digital property and transactions, you may position almost anything on a Blockchain. Different situations name for different Blockchains.

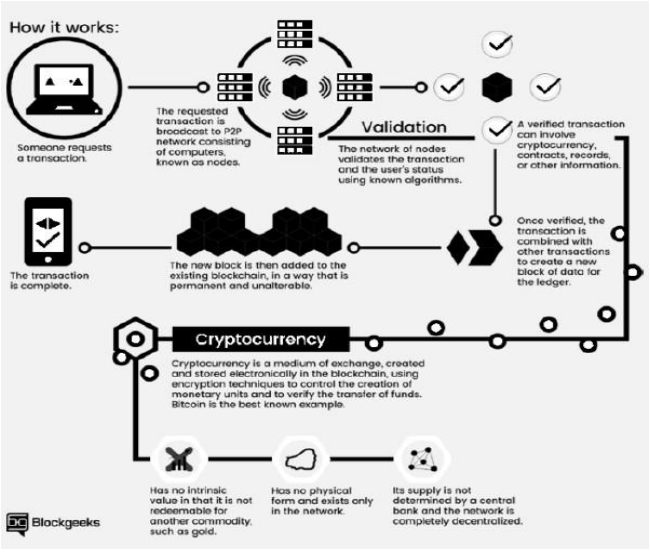


Fig. 4 How Blockchain Working

The Blockchain era presently has the subsequent features [17][18]

1) *Peer-to-Peer (P2P) network*: the primary requirement of BC is a network, an infrastructure shared via a couple of events. This may be a LAN at a small scale or the net at a big scale. All nodes participating in a BC are linked in a decentralized P2P network. Transactions are broadcast to the P2P network. Due to a few limitations of P2P networks, a few providers have provided cloud-based BCs.

2) *Cascaded Encryption*: A BC makes use of encryption to guard transaction records. Blocks are encrypted in a cascaded way, i.e. the encryption result of the previous block is utilized in encrypting the current block. The BC is secured through public key cryptography, with each peer producing its personal public-private key pairs.
3) *Distributed Database*: A BC is digitally distributed throughout some of computers. Each party on a BC has access to the whole database and no single party controls the records or the information. Since BC is decentralized, there's no need for relevant authorizes such as banks.
4) *Transparency with Pseudonymity*: every node or participant on a blockchain has a completely unique 30-plus-individual alphanumeric deal with that identifies it. Users can select to stay anonymous or provide evidence in their identity to others.
5) *Irreversibility of data*: as soon as a transaction is entered within the database and the accounts are updated, the data can't be altered. Data at the database is permanent, chronologically ordered, and available to all others at the network.

B. Types of Blockchain

Blockchain can be public or private relying on the permission level [20], however here we widely classify it to 3 different levels of granularity.

1) *Public Blockchain*: A public blockchain is permission-less and all people can easily take part and validate the transactions. Transactions are public and anonymous/pseudonymous. The blockchain is maintained by using the public network, so there's the highest level of decentralized trust. Bitcoin is the pioneer public blockchain. Bitcoin, Ethereum, Waves [21], dash [22], and Bitshares [23] are few examples of public blockchains.

2) *Federated blockchain*: federated blockchain is a permissioned blockchain working below the leadership of a set often called the consortium. Predefined consortium nodes manage the consensus. The transactions might also or might

not be public. A few examples include R3 Corda [24], EWF (energy) [25], and B3i (insurance) [26].

3) *Private Blockchain*: A private blockchain is a permissioned blockchain centralized to at least one governing organization. Transactions are verified internally and might or might not be public readable. Private blockchains normally have quicker block times and may process better transaction throughput. But, those are vulnerable to security breaches. The value of private blockchain may be visible as a trust transformer in which trust is based on an algorithm instead of an authority. Monax [27], Hyper-Ledger with Saw-tooth [38], private Ethereum are a few examples of private blockchains.

C. Applications of Blockchain

Blockchain has the ability for addressing enormous healthcare problems. Here are the most likely applications [29]:

1) *Medical records management*: The healthcare industry is drowning in records patient clinical records, complicated billing, medical trials, medical research, and so on. The purpose of BC is to provide patients and their provider's one-stop access to their whole medical records throughout all vendors. Blockchain is capable of securely, privately and comprehensively track affected person health information. It makes digital medical information more efficient, disinter mediated, and secure. This way care companies may have the entire medical records of the affected person. For fitness care to achieve the blessings of a blockchain-based totally medical document, it should furnish get admission to everybody that could need patient's records [30].
2) *Drug improvement*: Blockchains can facilitate new drug improvement via making patient outcomes more widely available. The issue of counterfeit drugs has become more and more pressing in view of the economic value of the global black market and the risk to human life that comes from taking counterfeit tablets. Blockchain technology is a superb counter to threats which are rapidly approaching (integrity-based assaults) and it is a superb ahead-searching device we would deploy to address them. BC may even allow drug builders to run medical trials and share clinical samples more securely [31].
3) *Clinical trials*: using blockchain could make medical trials dependable at each step via maintaining track and time-stamping at each section of the trial. Another blockchain use-case will be the adoption of digital informed consent in medical trials. BC improves responsibility and transparency within the medical trial reporting process.
4) *Records safety*: Blockchain technology has the ability to be the infrastructure that is needed to maintain health records private and comfortable. BC requires nobody central administrator and it has unprecedented safety advantages because data are distributed throughout a network which is always in sync. Other packages include counterfeit drug prevention and detection, validation and payment of claims, medical trial outcomes, final results-based payments, reimbursement of healthcare offerings, exchange of health records, and deliver chains [32]. Although blockchain offers many possibilities for healthcare, it isn't completely mature yet. Numerous technical challenges should be addressed earlier than a healthcare blockchain can be adopted nationwide [33].

D. Benefits of Blockchain

TABLE II
Benefits of Blockchain

Features	Examples
Digital Access Rules	Clinical informational stored off-chain or on-chain is associated with the public key of a patient. The patient can utilize properties of the blockchain, similar smart contracts, to assign access rules for the data. For instance, authorizing release to an investigation for a fixed period.
Data Aggregation	A patient associates with various institutional interfaces with institution-specific logins and gives that organization their blockchain public key along with approval to securely transmit data (or metadata) to the blockchain. Done over the various institution, clinical information can be amassed using the technology
Data liquidity	Profoundly time-sensitive clinical data—for instance, advanced care planning "code status" or medication sensitivities, can be circulated on an open blockchain, guaranteeing prepared, liquid access to this data as suitable.
Patient Identity	Patients can deal with their public keys may be through a multi-sig wallet or cell phone and utilize the public-key foundation (PKI) to build up their identity for recovering clinical information from the blockchain, just as adding new data (like home monitoring gadgets). PKI guarantees providers and establishments can trust that the patient is generating the data.
Data immutability	Clinical data (or metadata) is securely scattered over various entities, ensuring trustworthiness cutting down the risk of loss, and offering a survey trail. The Append-only model of blockchain guarantees access to data.

E. Challenges of Blockchain

TABLE III
Challenges of Blockchain

Challenge	Mitigation
Transaction volume of clinical data	Focus data exchange on summarized clinical data. Permissioned blockchains for local geologies to handle huge transaction volumes without time-intensive endorsement. New advancements and research in blockchain scaling frameworks
Security and Privacy	Permissioned, member-only blockchain consortium to limit open presentation. Data storage off-chain, with on-chain centered around authorizations or other meta-information. Patient-friendly "app" ecosystem of channels to manage public keys and permissions.
Patient engagement Incentives	Continued federal incentives to inflate API coverage. Association of open data with regard to reimbursement. Competitive pressure of API-enabled systems to urge non-enabled framework in API establishments.

4. POSSIBLE FUTURE DIRECTIONS

Blockchain has exhibited its potential in industry and academia. The possible future directions with respect to four areas: blockchain testing, big data analytics, stop the affinity to centralization, and blockchain application

A. Blockchain testing

Recently different kinds of blockchain appear and over 700 crypto currencies are listed in [34] up to now. However, some developers might falsify their blockchain performance to attract investors driven by the huge profit. Besides that, when users want to combine blockchain into business, they have to know which blockchain fits their requirements. So blockchain testing mechanism needs to be in place to test different blockchain. Blockchain testing could be separated into two phases: standardization phase and testing phase. In standardization phase, all criteria have to be made and agreed. When a blockchain is born, it could be tested with the agreed criteria to valid if the blockchain works fine as developers claim. As for testing phase, blockchain testing needs to be performed with different criteria. For example, an user who is in charge of online retail business cares about the throughput of the blockchain, so the examination needs to test the average time from a user send a transaction to the transaction is packed into the blockchain, capacity for a blockchain block and etc.

B. Stop the tendency to centralization

Blockchain is designed as a decentralized system. However, there is a trend that miners are centralized in the mining pool. Up to now, the top 5 mining pools together owns larger than 51% of the total hash power in the Bitcoin network [35]. Apart from that, selfish mining strategy showed that pools with over 25% of total computing power could get more revenue than fair share. Rational miners would be attracted into the selfish pool and finally the pool could easily exceed 51% of the total power. As the blockchain is not intended to serve a few organizations, some methods should be proposed to solve this problem.

C. Big data analytics

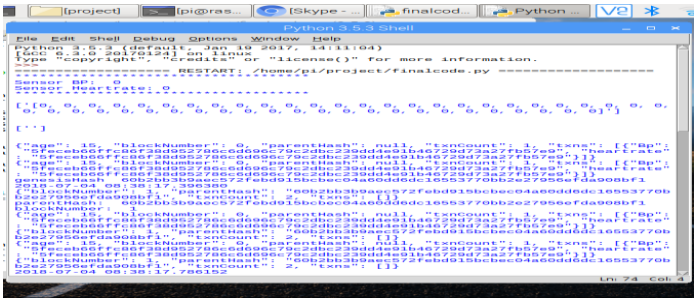
Blockchain could be well combined with big data. Here we roughly categorized the combination into two types: data management and data analytics. As for data management, blockchain could be used to store important data as it is distributed and secure. Blockchain could also ensure the data is original. For example, if blockchain is used to store patient's health information, the information could not be tampered and it is hard to steal those private information. When it comes to data analytics, transactions on blockchain could be used for big data analytics. For example, user trading patterns might be extracted. Users can predict their potential partners' trading behavior's with the analysis.

D. Blockchain applications

Currently most blockchains are used in the financial domain, more and more applications for different fields are appearing. Traditional industries could take blockchain into consideration and apply blockchain into their fields to enhance their systems. For example, user reputations could be stored on blockchain. At the same time, the up-and-coming industry could make use of blockchain to improve performance. For example, Arcade City [36], a ridesharing start-up offers an open marketplace where riders connect directly with drivers by leveraging blockchain technology. A smart contract is a computerized transaction protocol that executes the terms of a contract [37]. It has been proposed for long time and now this concept can be implemented with blockchain. In blockchain, smart contract is a code fragment that could be executed by miners automatically. Smart contract has transformative potential in various fields like financial services and IoT.

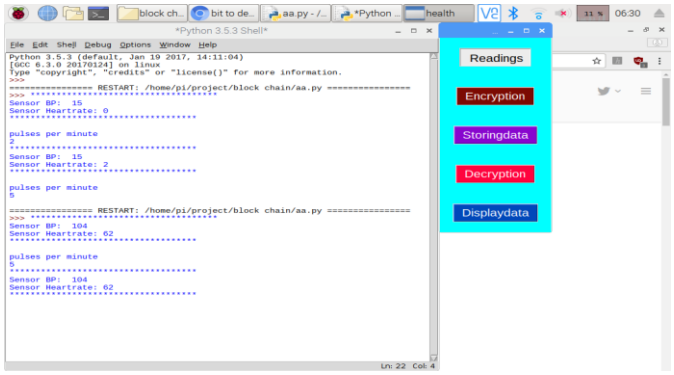
5. RESULT

Result of blockchain before sensors connecting and before mining



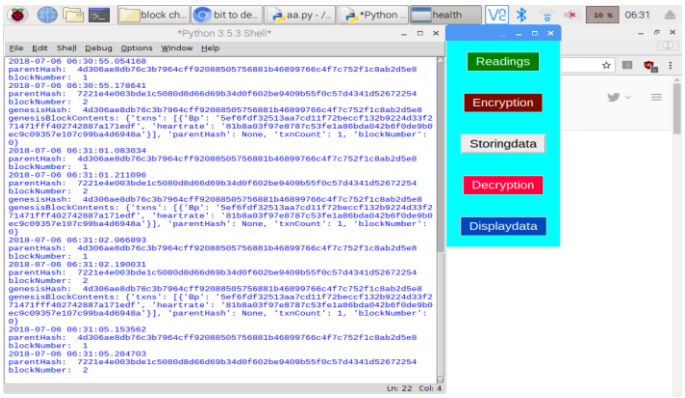
Screen 1

By using GUI the result will get like this and sensor reading values



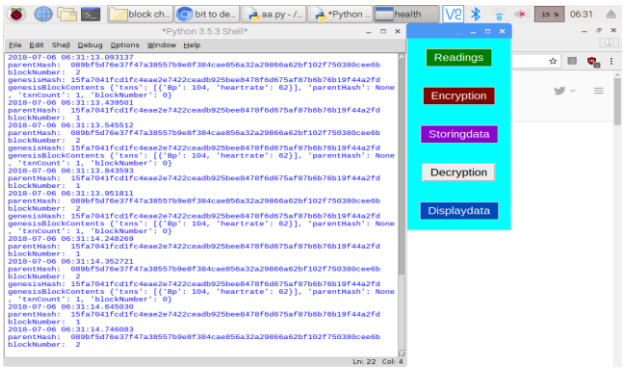
Screen 2

In Encryption, we have to create an account and private key by using that we are sending the data to blocks. We are using encryption to secure the data. Encryption output with GUI as shown in below image



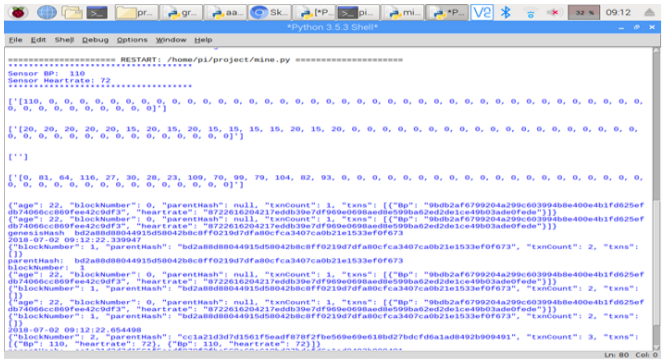
Screen 3

With encryption, we secured the data by using decryption we are taking that secure to out (private data to public data). Decryption using GUI

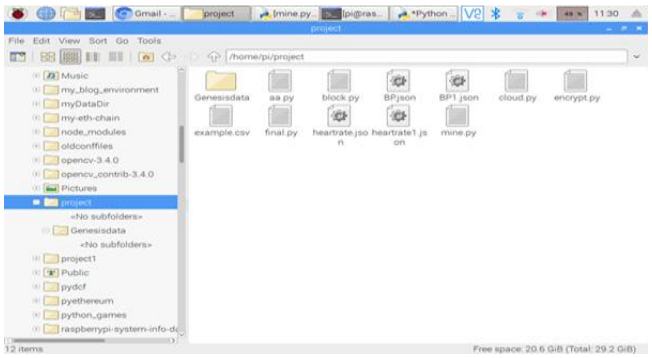


Screen 4

After mining, the block number will get increase and one more block adding to blockchain as shown in below figure



After completion of mining, the blockchain will add to genesis block and block number will get an increase. After every mining, one new block will be added to the main genesis block. In that blockchain we are sending sensors data, person age, and block number. Genesis block and CSV file will store in the project folder automatically. That result as shown in the below figure.



Screen 6

6. CONCLUSION

Blockchain technology has the ability to solve numerous problems plaguing the healthcare industry nowadays. Simply sharing the data isn't enough. The proposed approach, using personal Blockchain technology, can play an important role in allowing the data immutable, secure, and share inside a decentralized network. In this work, the blocks are described as excessive-stage 3-scenarios and their protocols are crucial to use this new technology within the health-care system. Finally, the overall performance of imperceptibility and robustness values on every block of the distributed ledger is measured. Every idea provides a few information and the reasons behind the technical path. It is hoped that this paper will stimulate further research and improvement to assist the patients as well as the overall health-care system.

REFERENCES

[1] John Viega, McAffee, Cloud Computing and the Common Man," published on the IEEE Journal ON Cloud Computing Security, pp. 106-108, August 2009.

[2] George Reese, "Cloud Application Architectures", First edition, O'Reilly Media, April 2011, ISBN 9780596156367, pp. 2-4, 99-118.

[3] http://www.baylor.edu/business/mis/nonprofits /doc.php/1 97132. Pdf

[4] R.Aronika Paul Rajan, S.Shanmugapriya. (2012, May- Jun).Evolution of Cloud Storage as Cloud Computing Infrastructure service IOSRJCE (1).pp-38-45

[5] Gurudatt Kulkarni, Rani Waghmar, Rajnikant Palwe, Vidya Waykule, Hemant Bankar, Kudilik Koli. Cloud Storage Architecture, IEEE International Conference on Telecommunication systems services and applications (TSSA).

[6] M.Tim Jones.(2010)."Anatomy of Cloud Storage Infrastructure ".IBM Available https://www.ibm.com/d Eveloperworks/cloud/library/cl-cloud storage.

[7] Yue X,Wang H, Jin D, LiM, JiangW. Healthcare data gateways: Found healthcare intelligence on Blockchain with novel privacy risk control. J Med Syst 201640218.https://doi.org/10.1007/s10916-016-0574-6.

[8] Ivan Drew. Moving toward a blockchain-based method for the secure storage of patient records, NIST/ONC; 2016.

[9] GordonWJ, Landman A. Secure, decentralized, interoperable medication reconciliation using the Blockchain. NIST/ONC; 2016.

[10] Zyskind Guy, Nathan Oz, Pentland Alex. Decentralizing privacy using blockchain to protect personal data. IEEE Secur Priv Work 20152015180–4.

[11] Health Level Seven International (HL7). Introducin HL7 FHIR n.d. http://www.hl7.org/fhir/summary.html accessed January 9, 2017.

[12] Zhang Peng, White Jules, Schmidt Douglas C, Lenz Gunther, Trent Rosenbloom S. FHIRChain: Applying Blockchain to securely and scalably share clinical data – semantic scholar; 2018.

[13] Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: Using blockchain for medical data access and permission management. 2016 2nd Int. Conf. Open Big Data OBD; 2016. p. 25–30. https://doi.org/10.1109/OBD.2016.11.

[14] Dubovitskaya A, Xu Z, Ryu S, Schumacher M,Wang F. Secure and trustable electronic medical records sharing using blockchain ArXiv170906528 Cs; 2017.

[15] Apple. Apple announces effortless solution bringin health records to iPhone. https://www.apple.com/newsroom/2018/01/apple- nannounces- effortless-solutionbringing-health-records-to- iPhone/; 2018, Accessed date: 7 May 2018.

[16] Sync 4 Science n.d. http://syncfor.science/ accessed May 31, 2018

[17] M. Iansiti and K. R. Lakhani, "The truth about Blockchain," *Harvard Business Review*, Jan./Feb. 2017.https://hbr.org/2017/01/the-truth-about-blockchain

[18] W. T. Tsai et al., "A system view of financial blockchains," *Proceedings of IEEE Symposium on Service-Oriented System Engineering*, 2016, pp. 450- 457.

[19] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In Big Data (BigData Congress), 2017 IEEE International Congress on, pages 557–564. IEEE, 2017.

[20] Waves whitepaper, 2018(accessed Nov 15, 2018). https://blog:wavesplatform:com/waves-whitepaper-164dd6ca6a23.

[21] Diaz Duffield. Dash: A Payments-FocusedCryptocurrency, 2018(accessed Nov 15, 2018).https://github:com/dashpay/dash/wiki/Whitepaper.

[22] The BitShares Blockchain, 2018(accessed Nov15, 2018).https://www:bitshares:foundation/papers/BitSharesBlockchain:pdf.

[23] Richard Gendal Brown. Introducing r3 corda: A distributed ledger designed for financial services, 2016, 2017.

[24] Energy web foundation, 2018(accessed Nov 15, 2018). http://energyweb:org.

[25] B3i insurance, 2018(accessed Nov 15, 2018). https://b3i:tech/.

[26] Monax - blockchain explainer, 2018(accessed Nov 15, 2018). https://monax:io/learn/blockchains.

[27] Hyperledger sawtooth, 2018(accessed Nov 15, 2018). https://sawtooth:hyperledger:org.

[28] "Blockchain in health care: The good, the bad and the ugly," https://www.forbes.com/sites/forbestech council/2018/04/13/blockchain-in-health-care-the-good-the-bad-and-the-ugly/#c00ec6462787

[29] "What the hell is blockchain and what does it mean for healthcare and pharma?" http://medicalfuturist. Com/what-the-hell-is-blockchain-what-does-it-mean-for-healthcare-and-pharma/

[30] S. Attili, "Today's healthcare challenges and how blockchain can help solve them – Join IBM for a HIMSS17 breakfast briefing," https://www.ibm.com/blogs/insights-on-business/healthcare/todays-healthcare-challenges-blockchain-can-help-solve-join-ibm-himss17-breakfast-briefing/

[31] M. A. Engelhardt, "Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector," *Technology Innovation Management Review,* vol. 7, no. 10, 2017, pp. 22-34.

[32] D. Randall, P. Goel, and R. Abujamra, "Blockchain applications and use cases in health information technology," *Journal of Health & Medical Informatics*, vol. 8, no. 3, 2017.

[33] "Who will build the health-care blockchain?" https://www.technologyreview.com/s/608821/who-will-build-the-health-care-blockchain/

[34] S. Solat and M. Potop-Butucaru, "ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin," Sorbonne Universites, UPMC University of Paris 6, Technical Report, May 2016. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01310088

[35] "Crypto-currency market capitalizations," 2017. [Online]. Available: https://coinmarketcap.com

[36] "The biggest mining pools." [Online]. Available: https: //bitcoinworldwide.com/mining/pools.

[37] N. Szabo, "The idea of smart contracts," 1997.