A Decentralized Cryptographic Blockchain Approach for Health Information System

Rexford Nii Ayitey Sosu [1], Kester Quist-Aphetsi [2], Laurent Nana [3]
[1]Ghana Technology University College
Faculty of Computing & Information Systems
[2]Department of Computer Science
[3]Lab-STICC (UMR CNRS 6285), European University of Brittany
University of Brest, France
[1]rnasosu@gtuc.edu.gh, [2]kquist-aphetsi@gtuc.edu.gh

***Abstract*— With the rise of cyber attacks and the advancement of technology providing easy access to personal data and information in real time using networks and other services such as the cloud. These advancements have placed sensitive data such as medical information under threat. Due to the ease in accessing and modifying such data leading to little or no trace of such wrongdoings. This paper proposes a cryptographic blockchain approach using the md5 hash algorithm to verify and validate the medical data of the health information system infrastructure. The approach makes it difficult for data to be altered without detection and adopts a distributed approach coupled with blockchain.**

Keywords - blockchain, cryptography, medical data, medical data security, md5.

I. INTRODUCTION

Medical research involves and requires huge processing and storage of health information across vast geographical areas involving different hospitals based on patient mobility. Data trail generated by patients and medical practitioners can be altered easily in situations where multiple users have access to the information systems. The quantity of medical reports on patients is normally constrained [1]. According to [2], medical data security has drawn much consideration from the research network in recent years.

Based on the sensitivity of medical information, which will be gathered, handled and managed. There is, therefore, the need for securing the medical data that will be saved as electronic health records (EHR). This paper proposes the use of blockchain, enabling a decentralized architecture for EHRs, using the md5 cryptographic hash algorithm to verify and validate the medical data on a health information system network.

II. LITERATURE REVIEW

Due to the major and continues advancement in technology and research, medical data has metamorphosed over the years from the brick and mortar approach of data gathering and processing to the cutting edge technologies being used lately. Below are a number of fields in which medical data can and is being applied.

A. Medical Data in IoT

The combination of prescription and data advancements, for example, medical informatics, will change social insurance, as we probably are aware of, controlling costs, increasing efficiency, and sparing lives. Figure 1 outlines how this insurgency in medicine will look in a common internet of things (IoT) hospital center, run-through as proposed by [3]. Patients will have all their records and medical history saved electronically in a secured cloud-based environment.

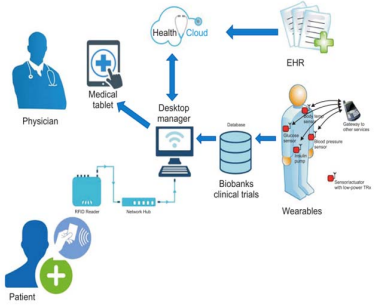

Figure 1. Illustrating the new phase of medicine in a distinctive Internet of Things (IoT) hospital, in run-throughs. [3]

B. Medical Data in Big Data

According to [4], the present pattern toward digitizing healthcare work processes and moving to electronic patient data has seen a change in perspective in the medical industry. The amount of clinical information that is accessible electronically will be then drastically expanded regarding intricacy, assorted variety, and convenience, coming about what is known as large information.

With the quick improvement and use of big data technology preparation and devices, a ton of research has been done in therapeutic data handling and use. For instance, Google effectively flu A (H1N1) in 2009, and its "influenza patterns framework" could anticipate influenza diseases weeks ahead in the United States by consolidating the customary

978-1-7281-0818-6/19/$31.00 ©2019 IEEE
DOI 10.1109/ICCMA.2019.00027

Authorized licensed use limited to: NATIONAL INSTITUTE OF TECHNOLOGY SURATHKAL. Downloaded on September 27,2021 at 08:44:08 UTC from IEEE Xplore. Restrictions apply.

checking technique and information preparing innovation as proposed by [5].

Figure 2. Big Data in Healthcare [6].

C. Cloud Computing and Medical Data Security

The medical data is developing quickly. In this way, an in-house saving of the data isn't an effective method to deal with medical information. The cloud servers are the best choice however, security is the principle downside in these servers. To upgrade the security by scrambling the medical information by relegating jobs before redistributing the information into the cloud as proposed by [7].

[8] Proposed cloud computing is a potential arrangement, because of the capacity to help ongoing information sharing despite geographical areas, to provide the relevant data as required, and to deal with big data (for example facilitating of analytical tools for big data) to acquire helpful bits of knowledge from the investigation of enormous healthcare information for research and planning for decision making.

The security issues, just as the related difficulties of authoritative development and consistency, apply to associations in numerous ventures. The effect on patients goes well past conventional financial data fraud. Given the effect to people, the media and general community frequently question why medicinal services associations don't better ensure private human services information as proposed by [9].[10] Proposed that the patient data in their document must be kept classified to maintain a strategic distance from any sort of altering of patient's information, illicit replicating and to ensure copyright security.

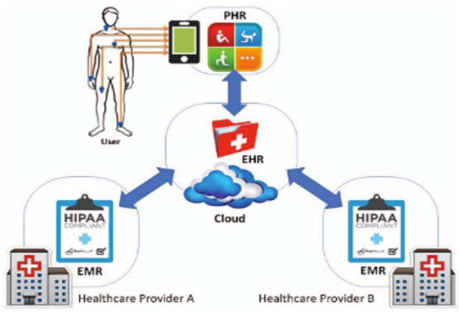

Figure 3. A cloud-based conceptual Ecosystem [8]

D. Blockchain and Medical Data

Blockchain enables a decentralized architecture for electronic health records (EHRs) on a network. Each EHR in the network saves replica of the blockchain and contributes to the shared process of authenticating and verifying digital transactions of the EHRs within the network as proposed by [11].

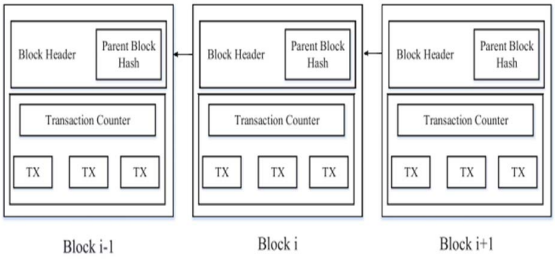

Figure 4. An example of a blockchian architecture illustrating the flow of blocks [12]

III. METHODOLOGY

A. MESSAGE DIGEST (MD)5 CRYPTOGRAPHIC HASH ALGORITHM

The MD5 algorithm was used in this paper as an approach was adopted to verify and authenticate the medical data that was captured for analysis. It is the most broadly utilized Hash security algorithm utilized in message confirmation, respectability discovery, and so on. The algorithm isolates the message into 512 piece input squares. Each square is experienced a movement of abilities to make an uncommon 128-piece message isolates the message into 512 piece input squares. Each square is experienced a movement of abilities to make an uncommon 128-piece message. [13]

The algorithm demands 8 bit of message length.

// Z= (Y0, Y1,....., Yn-1), Message to hash, after padding

// Each Yi is a 32-bit word and N is a multiple of 16

Authorized licensed use limited to: NATIONAL INSTITUTE OF TECHNOLOGY SURATHKAL. Downloaded on September 27,2021 at 08:44:08 UTC from IEEE Xplore. Restrictions apply.

MD5 (Z)
//initialize (A,B,C,D) = IV
(A,B,C,D) = (0x67452301,0xefab89 , 0x98badcfe , Ox10325476)
For i=0 to N/16 -1
// Copy block I to X
Xj = Y16i+j for j = 0 to 15
// Copy X to W
Wj = X
σ
(j) , for j = 0 to 63
// initialize R
(Q-4 , Q-3 , Q-2 , R-1) = (A , D , C , B)
// Rounds 0 , 1 , 2 and 3
Round0(Q , W) Round1(Q , W) Round2(Q , W) Round3(Q , W)
// Each accumulation is modulo 232
(A , B , C , D)=(Q60 + Q-4 , Q63 + Q-1 , Q62 + Q- 1 , Q61+ Q-3)
next i
return A , B , C , D
end MD5
Round0(Q , W)
//steps 0 through 15 for i = 0 to 15
Qi = Qi-1 + ((Qi-4 + F(Qi-1 , Qi-2 , Qi-3) + Wi +Ki) <<< si)
next i
end Round()

Stage 1: Padding bits and Add Length
Padding of the bits is necessary with '0' and '1' first and last separately until the subsequent ≠ bit length which = 448 mod 512, and the remainder of bit length of the first message as 64-bit whole number. The last piece length of the message, which is now padded, is 512N for a genuine whole number N

Stage 2: Divide the contribution to 512-piece squares
The message, which is now padded, is presently apportioned into N progressive 512-piece squares m1, m2.....mn.

Stage 3: Reset Channing factors
Instatement of 32-bit number through tying factors (A,B,C,D) these qualities are spoken to in a single hash
A = 01 17 2d 43
B = 89 AB CD EF
C = FE DC BA 98
D = 76 54 32 10

Stage 4: Process blocks
The four cushions (A, B, C, and D) messages (content) are united now with the info words, utilizing the four assistant capacities (W, X, Y, and Z).4 rounds are performed and each includes 16 fundamental tasks. The Processing square P is connected to the four cradles (A, B, C, and D), by utilizing message word M[i] and consistent K[i]. The thing "<<<s" indicates a double left move by s bits. The four sort of IRF(info related capacities) that each take as info three 32-bit words and produce same bits of yield for example 32-bit word. They apply the sensible administrators ^, v,! what's more, xor to the data

Q (A, S, D) = AS v not (A) F
W (A, S, D) = AS v S not (F)
E (A, S, D) = A xor S xor F
R (A, S, D) = S xor (A v not (F))

The bits of A, S, and D are extremist and equalization each piece of Q (A, S, D) will be authoritarian and parity.
The capacities (A, S and D) = P, in that they do work in "bitwise parallel" to create the dependable yield from the bits of A, S and D.In such a way, that if the be comparable bits of D, E and F are autarchic and adjusted, at that point each piece of W (A, S, D), E (A, S, D) and R (A, S, D) will be authoritarian and parity.

• Step 5: Hashed Output

There are 4 rounds performed in message digest 5 (MD5) which is of 128 bits. Fig 5 shows One MD5Operation

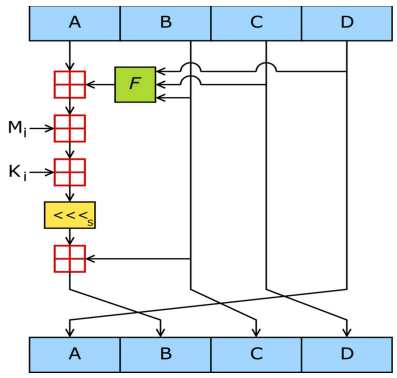

Figure 5. A Diagrammatic Representation of MD5 Algorithm [14]

B. Electronic Health Records (EHR) Architecture

The medical field has experienced various improvements continually experiencing significant changes due to the advent of technology ranging from areas such as diagnostics, electronic records keeping and so on.
The proposed architecture below represents entity models of medical records within a health information system. The patient entity has attributes such as the patient id, name and so on. The doctor entity also has attributes such as doctor id, patient id, name, medical data, and so on. The records entity has attributes such as records id, doctor id, reports, timestamp, and so on.

Authorized licensed use limited to: NATIONAL INSTITUTE OF TECHNOLOGY SURATHKAL. Downloaded on September 27,2021 at 08:44:08 UTC from IEEE Xplore. Restrictions apply.

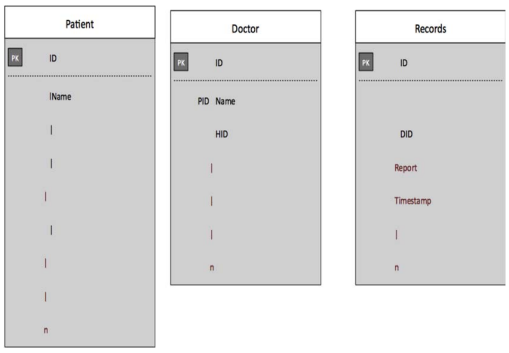

Figure 6. A Medical Data Classes Representation of Electronic Health Records

C. *Health Information System Architecture*

The below architecture illustrates the exchange of a patient's medical data among different hospitals and health centers via health information systems as he or she seeks medical care. The performance was achieved perfectly using the md5 hash algorithm.

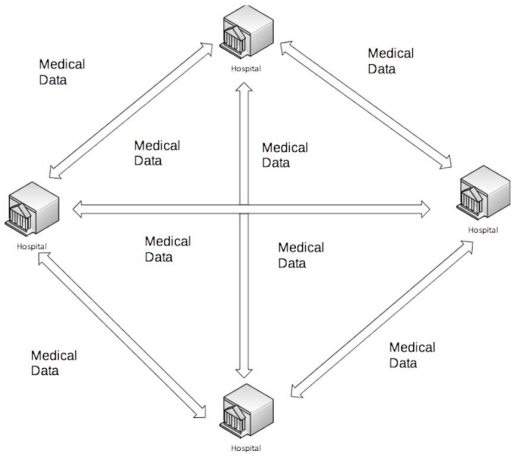

Figure 7. A Health Information System Architecture Representing Medical Data Exchange

IV. RESULTS

In this section, we represent detailed information of a patient's medical ledger generated from the EHR. After that, the patient's medical records are then hashed using the MD5 cryptographic algorithm. This then yields a chain of blocks created to securely validate and verify the patient's entire ledger within the health information system. Thus preventing any form of alteration or data falsification.

In Figure 8 below, the values from the patient's medical records were captured in blocks based on blockchain principles as follows: m91, HC91, NDN09771, olweutyain representing the patient's medical data information, 03:59:40am representing the timestamp of the medical data and 75b06a42be62fbc39dd0975f449e8135 representing the hash value computed on the patient's medical data captured. The subsequent blocks are then created from the updated patient's medical data, with the new hash of the updated medical records and the hash of the previous hash block and so on for the remaining blocks forming the chain.

rn91 , HC91 , NDN09771 , olweutyain , 03:59:40am , 75b0ba42be62fbc39dd0975f449e8135
rn52 , HC102 , NDN09752 , uphnanvttw , 10:05:44am , 4fc19434969c3912534b353e7921cca0
rn83 , HC63 , NDN097103 , uumvmodawy , 10:36:09pm , 1510b0f28208d4dc886326793eebe578
rn84 , HC14 , NDN09794 , sqbmxyqjjo , 05:34:10pm , 276ae50919eac96157d11fa0b18c6b5a
rn15 , HC95 , NDN09755 , fzigwjnhsn , 08:02:24am , b72eebd1d15cefeea962312c6040ee86
rn106 , HC96 , NDN09786 , ngyxzztmll , 12:08:50pm , 66f4e7da07c556b63f4370c8ff5e66cc
rn47 , HC87 , NDN09747 , lsuqbnfthy , 09:00:13pm , 5c032f6f15e0eea15d99202d5867bb24
rn68 , HC28 , NDN097108 , lihpmhshaa , 07:11:48am , eb50aeee3c9e65b3a228d55cc07d568c
rn29 , HC79 , NDN09789 , bvrjogkupq , 10:22:38pm , b725b617c5f2a1b467cc25a9cd96c8ec
rn310 , HC1010 , NDN097910 , mssdjiaivd , 06:14:39pm , d22db55b58e041c85a789c7cfe9966db
rn311 , HC611 , NDN097911 , nqgcisrizz , 09:36:38am , 68c747e3fd3be5f938435adbea07bb61
rn112 , HC712 , NDN097212 , lciavkhsqs , 09:56:35pm , a012fd67f033c441fb34258cdfa25b66
rn713 , HC413 , NDN097413 , mmiztfjbvt , 04:21:28am , 7d11b73858df5b66b5e0340257b65036
rn714 , HC814 , NDN097814 , wqwkbmhyfw , 08:23:50am , 06e068fcde3cc4dad2f1fd9236e28d16
rn415 , HC115 , NDN097515 , mgudyydrvv , 03:40:02am , b41d08065f4293cc08b35953db499150
rn416 , HC416 , NDN097516 , ntazondwpv , 11:42:13pm , 1f7f7eae995fd31a3cf490062ba564d4
rn117 , HC917 , NDN0971017 , grvbelpesa , 10:48:44am , 86e21cd43fa233e301c69b91590ffe72
rn618 , HC218 , NDN097618 , juedmthsrz , 02:40:10am , 3a776af485345e3d26e51c3955d822f7
rn819 , HC1019 , NDN097719 , ylpjrwjkti , 09:23:53am , 9adb9240ff251c51b084808ccca925d3
rn320 , HC420 , NDN097320 , rsjtkpldml , 10:06:30am , f8d7b28a9e0c4fc47e9413c1f030a6db

Figure 8. Patient Ledger

V. CONCLUSION

In this paper, the approach of blockchain was proposed using the md5 hash algorithm to securely verify and validate patient ledger (medical data) within a health information system as explained in the above results.

REFERENCES

[1] X. Wang, L. Tian, B. Xu, X. Wang, and W. Wu, "MOOC for medical big data research: An important role in hypertension big data research," Proc. - 2015 IEEE 1st Int. Conf. Big Data Comput. Serv. Appl. BigDataService 2015, pp. 453–455, 2015.

[2] K. Kalaivani and R. Sivakumar, "A novel fuzzy based bio-key management scheme for medical data security," J. Electr. Eng. Technol., vol. 11, no. 5, pp. 1509–1519, 2016.

[3] D. V. Dimitrov, "Medical internet of things and big data in healthcare," Healthc. Inform. Res., vol. 22, no. 3, pp. 156–163, 2016.

[4] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, "Big data security and privacy in healthcare: A Review," Procedia Comput. Sci., vol. 113, pp. 73–80, 2017.

Authorized licensed use limited to: NATIONAL INSTITUTE OF TECHNOLOGY SURATHKAL. Downloaded on September 27,2021 at 08:44:08 UTC from IEEE Xplore. Restrictions apply.

[5] F. Weiwei, Z. Dongsheng, and W. Songjun, "A fast statistics and analysis solution of medical service big data," Proc. - 2015 7th Int. Conf. Inf. Technol. Med. Educ. ITME 2015, pp. 9–12, 2016.

[6] "Big Data in Healthcare Market 2018 | Size, Share, Segmentation & Business Demand | Hypothesis Investigation | Forecasts till 2022 | Medgadget." [Online]. Available: https://www.medgadget.com/2018/02/big-data-in-healthcare-market-2018-size-share-segmentation-business-demand-hypothesis-investigation-forecasts-till-2022.html. [Accessed: 18-Jan-2019].

[7] G. Ramu and A. Jayanthi, "Enhancing Medical Data Security in the Cloud Using RBAC-CPABE and ASS," vol. 13, no. 7, pp. 5190–5196, 2018.

[8] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K. K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?," IEEE Cloud Comput., vol. 5, no. 1, pp. 31–37, 2018.

[9] J. Kwon and M. E. Johnson, "Protecting Patient Data - The Economic Perspective of Healthcare Security," IEEE Security. Priv., vol. 13, no. 5, pp. 90–95, 2015.

[10] M. A. Usman and M. R. Usman, "Using image steganography for providing enhanced medical data security," CCNC 2018 - 2018 15th IEEE Annu. Consum. Commun. Netw. Conf., vol. 2018–Janua, pp. 1–4, 2018.

[11] M. Benchoufi and P. Ravaud, "Blockchain technology for improving clinical research quality," Trials, vol. 18, no. 1, pp. 1–5, 2017.

[12] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, pp. 557–564, 2017.

[13] S. Purwanti, B. Nugraha, and M. Alaydrus, "Enhancing security on E-health private data using SHA-512," 2017 Int. Conf. Broadband Commun. Wirel. Sensors Powering, BCWSP 2017, vol. 2018–Janua, pp. 1–4, 2018.

[14] "File:MD5.png - Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/File:MD5.png. [Accessed: 23-Jan-2019].

Authorized licensed use limited to: NATIONAL INSTITUTE OF TECHNOLOGY SURATHKAL. Downloaded on September 27,2021 at 08:44:08 UTC from IEEE Xplore. Restrictions apply.