Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Blockchain Technology Combined With AES Encryption Security System For Patient Healthcare System

S Joseph Gabriel[1*], Dr. P. Sengottuvelan[2]

[1]Research Scholar, Department Of Computer Science, PeriyarUniversity,Salem.*
[2]Research Supervisor, Periyar University Centre for PG and Research Studies,Dharmapuri-635205.

Blockchain is the prominent security that provides more security to critical information. Blockchain provides a shared, immutable and transparent history for all the transactions that have been built with the help of Blockchain technology that has trust, account, and transparency. Blockchain technology is used to protect data and gives reliability. An AES algorithm is used to encrypt the data. The aim of the paper is that to provide better communication between the patients and doctors to share their opinion and viewpoint on different kinds of problems and put the patients in control according to their clinical data, providing them the legal rights to share the data, the clear understandable version of their data with the medical network of every organization, if needed.

Keywords -AES, Blockchain, Clinical Data, Healthcare, PHR.

I. INTRODUCTION

Data mining is an insightful interaction for the most part intended for investigating information. It is dissecting the information and summing up it into helpful data. It is extricating obscure data from an enormous information base. The wide scope of uses of Data mining incorporates business, promoting, medical care, logical field, and so on. potential way whether the data is near and dear or corporate[1]. In an examination task, it will be valuable in explicit cases for both the individual or affiliation or a get-together of communicators. For sure, even having data can be destined to be private. In data mining measures there is a necessity for saving sensitive data. Likewise, this issue is suggested as Privacy shielding data mining. In data mining, it is a mind-boggling issue to mining data in a secure way. For data mining and AI techniques many secure shows have been proposed so far for decision tree plan, clustering, connection rule mining, Neural Networks, Bayesian Networks[2]. Defending the security of social events' fragile data, is the essential concern of these computations, similarly from the whole dataset they increment supportive data. visit thing sets and, hence connection rules are found and this technique is perhaps the most analyzed issue in data mining.

Interaction mining has been effectively applied in the medical services area and has served to reveal different experiences for improving medical services measures. While the advantages of interaction mining are generally recognized, numerous individuals legitimately have worries about unreliable employments of individual information. Medical services data

frameworks contain exceptionally delicate data and medical services guidelines regularly require assurance of information security[3]. The need to conform to severe protection prerequisites may bring about a diminished information utility for examination. Up to this point, information security issues didn't get a lot of consideration in the process mining local area; notwithstanding, a few protection safeguarding information change strategies have been proposed in the information mining local area. By and large Doctor-open minded relationship contains the total dependence of the patient on the Doctor. Experts need to keep precise record systems to store information about patients and use the records to make decisions and recommendations. Recollecting this, one huge accomplishment is the use of the electronic health record (EHR)[4]. Varieties of patient prosperity data are the Health records; the high-level vault of the prosperity status of patients is portrayed as EHR. The EHR started from a substitute electronic system for taking care of patient data that transformed into a coordinated and interoperable philosophy. Since their records rely on and large upon data detailed by medical care suppliers, it transforms into the limitation of EHR[5].

II. RELATED WORKS

Since the presentation of the Internet of Things (IoT), e-health has gotten one of the fundamental examination themes. Because of the affectability of patient information, saving the security of patients has all the earmarks of being tested. In medical care applications, patient information is normally put away in the cloud, which makes it hard for the clients to have sufficient power over their information. Nonetheless, because of the General Data Protection Regulation (GDPR)[6], it is the information subject's entitlement to know where and how his information has been put away, who can get to his information, and how much. In this paper, we propose a blockchain based design for e-wellbeing applications that gives an effective protection-saving access control system.

Medical services information is getting the interest of digital assailants lately. Obliterating outcomes of medical services information could be lightened through decentralization. During a patient's stay in a hospital for treatment, rehabilitation, examination, or surgery, a case-specific ledger could be created. The network would link physicians, nurses, and family members to the effectiveness and transparency of treatment. This will eliminate human errors and ensure consensus in the event of a discussion on a certain stage of treatment. A shared (P2P) network empowers the property of decentralization, where various gatherings can store and run calculations while keeping touchy wellbeing information hidden. Blockchain innovation uses a decentralized or circulated measure, which guarantees the responsibility and honesty of its utilization. This paper[7] presents patient-driven medical care information the board framework by utilizing Blockchain as the capacity to accomplish protection. Pseudonymity is guaranteed by utilizing cryptographic capacities to ensure patient information. The protection of Electronic Health Records (EHRs) is confronting a significant obstacle with re-appropriating private wellbeing information in the cloud as there exists a risk of spilling wellbeing data to unapproved parties. Indeed, EHRs are put away on brought together information a base that builds the security hazard impression and requires trust in a solitary power which can't successfully shield information from inside assaults[8]. This examination centers on guaranteeing patient protection and information security while sharing delicate information across the same or various associations just as medical services suppliers

in a circulated environment[9-13]. This examination builds up a protection saving system through Health chain dependent on Block chain innovation that looks after security, protection, adaptability, and honesty of the e-wellbeing information. The Blockchain is based on Hyperledger texture, permission disseminated record arrangements by utilizing Hyperledger-author and stores EHRs by using InterPlanetary File System (IPFS) to assemble this health chain structure[10].

III. PROPOSED METHODOLOGY

The architecture of the proposed system is shown in Figure 1. The architecture is made up of some actors like a patient, doctor, database for strong PHP(personal health record) data (related data), Blockchain technology is the secure way of sharing PHR and API for the participants who can interact system different kinds of activities.

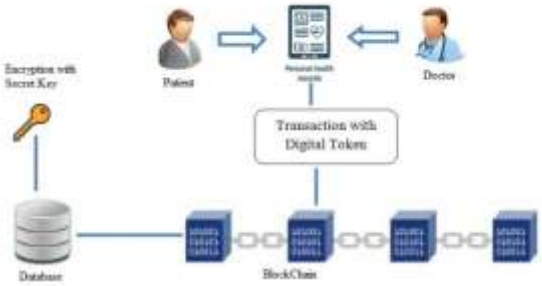

Figure 1: Secure Transactions using Blockchain Technology

A Blockchain Technology

A Blockchain contains blocks, in which each block can store a group of information or data of its past, present, and future. Every block plays an important role in associating with the past block and accompanying block that becomes a part of the chain as soon as it comes into the system. Recording, approving, and disseminating the exchanges among the block is the primary job of each block. The changes in each resulting block show that a block in the chain that cannot be expelled or modified. Thus the blockchain is a decentralized data frame that stores all data of past exchanges and it works on a pre-chosen convention that can specify the bearing of performing and approving the exchanges and it can work as same as the whole system and. Furthermore, the system is indicated as a disseminated vault, and the data is given to every block which works in each of the systems. In a Blockchain system, the exchange bunch is integrated into blocks of frameworks associated with the chain which utilizes the hash of the past block's record. In such wise and unchanging nature's property, the basic security highlight of the Blockchain system has been upheld. In addition, the block along with the could be remembered for it is a shield from the changes. In case the change in any of the keys assailant attempts, the neighbor register immediately stops, and the fact that inside the squares headers the hash esteems will be unique and relies upon the hash work system.

B Blockchain Model for the Health Care

Medical care has become an inseparable part of human life and the medical data, for example, the patient's prescriptions, their old clinical history, and record have become an important part of diagnosing patients and proceeding with the forthcoming treatment. In general, the clinical history was reported on the paper, later on, it may get a chance of being modified and get damaged. Hence, it is important to store and protect the data in the system electronically. Even so, the medical database could be corrupted or permanently deleted. In the medical system, it is important to provide security mechanisms to protect the medical data of patients which also contains private information. The traditionally used method to protect the data sometimes leaks the privacy of the data and patients privacy and integrity too. The data is also shared with stakeholders for various purposes. The main aim of the paper is that to provide a security mechanism to the medical record and private information of the patients. And this proposed system provides secure and reliable healthcare schemes to the patients using Blockchain technology. Healthcare Blockchain system which under a decentralized environment based on the IPFS protocols. Blockchain technology has many uses in the healthcare system and it can increase mobile health applications, health monitoring devices, sharing and storingthe medical data electronically, clinical trial data, and the insurance data storage of each patient. Generally, any Blockchain for healthcare to be public, and it is also necessary to have the technological solutions for three key elements: scalability, access security, and data privacy.
A system “Healthcare Data Storage Using Blockchain" can provide top-level security to all the health-related data. By using this technology, the cost and time can be reduced, and also other resources are required to manage all their information.

C. Database Security with AES Encryption

A database is the gathering of data and information which provides authentication to the data storage. All the data are given as input to the database system and it is often known as an important corporate asset. Additionally, the data also gives system interrogating, creating, modifying, and deleting information. The secure database is apprehensive which regards guaranteeing the mystery, honesty, and retrieving of information that is given together in a database system. The process of the AES encryption algorithm is shown in figure 2.

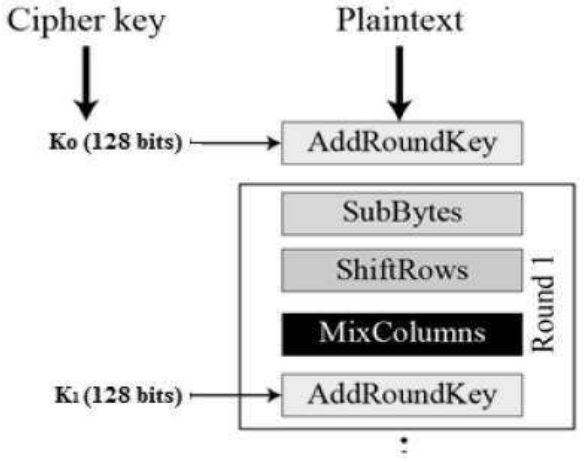

Figure 2: Encryption Process of AES Algorithm

The security dangers of the basic database system are generally not approved or unplanned action or sometimes abused by the licensed database clients and overseers, or the directors of the framework, or by the system, or also the unlicensed clients or programmer who can make illegal access to the confidential information, metadata or volume inside the database or which can inappropriately modifies the database endeavor and its structure or the design of the security. As same as the malware contamination causing circumstances, for example, the approved retrieval, leaking or exposing the client or prohibitive information, damaging or deleting the data or the projects, intervention, and disavowal of the approved retrieval to the database, making harmless on various framework and the unexpected disappointment of database management may occur in the database.

Steps for AES key with block:

```
begin
word tmp
i=0;
while (i<n)
a(i) = key(4*1);
end while
while (i<n, n+1)
tmp = a(i-1);
end while
end
```

To provide a proper, solid, andprogressively productive strategy which can clear out all unlicensed clients for obtaining database and mystery data by clear and easy advances: oversee PC chance, limitation in security the executive and the extra measures of the security can be developed to encrypt the confidential data before storing theinformation in the database system.

In this paper, we created and added more security to store the database information of the client's Medical Report, Blockchain Tokens, etc. with the help AES encryption algorithm. Advanced Encryption Standard is an algorithm of symmetric encryption and a set of keys called round key is used for the encryption process.

IV. EXPERIMENTAL RESULTS

The proposed system has been implemented by AES and Blockchain technology. And this system is to be used in real-time schemes of various clients who can perform several functions on the system, and we have the assessment execution by using Apache. Apache is a testing tool of desktop performance that is used for analyzing and testing applications. The collection of data that is transferred from one location to another in a unit of time is referred to by Throughput. By using this technique, the number of uses from 500 users to 1000 users who are using the framework and executing out its different dimensions. Throughput is represented in Data/Time, for example, KB/sec units. While executing the trials of using this system, we analyzed the exhibition of the data. And so the outcomes are run on the proposed system and the throughput of this system is investigated.

The system's execution time gets incremented when the amount of data or framework is being increased. It is noted while learning the test as the number of patients and petitions get increases, the framework's throughput also increased dramatically. The efficiency of the proposed framework of throughput is demonstrated by straight increment.

A. Accuracy

The accuracy of the data model is defined as the optimal recognition of the amount of pattern after learning the data mining algorithm. Result with accuracy % and plots showing their comparison as shown in figure 3. The accuracy of the data model is given by the following equation:

Accuracy= correctly recognized patterns/total patterns to classify *100 -----(1)

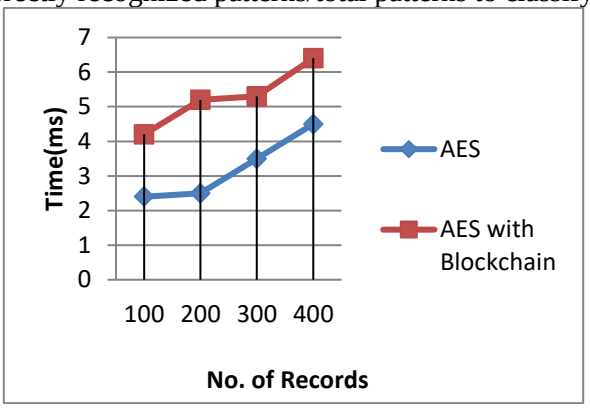

Figure 3: Accuracy Percentage for Proposed System

B. Error rate

The error rate of the learning algorithm is defined as the improper recognition of the number of data instances during pattern recognition. Result with error rate % and plots showing their comparison as shown in Figure 4. The error rate is given by the following equations:

Error rate % =100- accuracy ----------(2)

Error rate % = incorrectly classified samples/ total samples to classify * 100 -----(3)

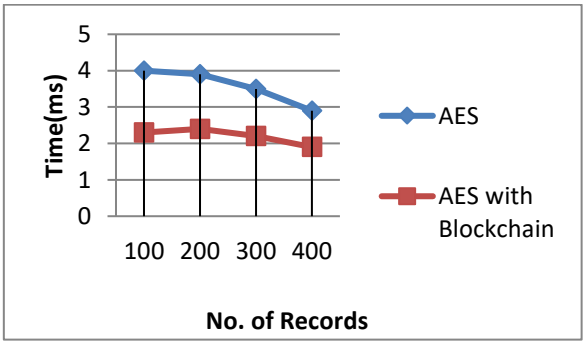

Figure4: Error Rate for Proposed Method

C Space complexity

The memory consumption or space complexity is defined as the input amount of data, amount of main memory required to execute the algorithm. The result with Space complexity and plots showing their comparison is given in Figure 5. The Space complexity is given by the following equation:

Consumed memory= total memory-free memory -----(4)

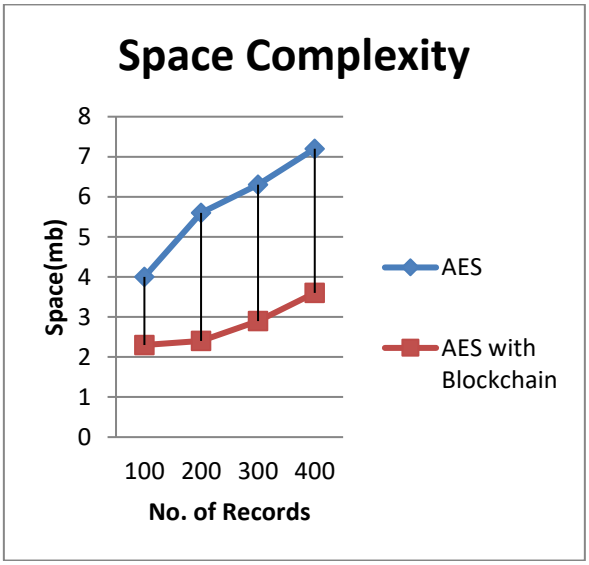

Figure 5: Consumed Memory of AES vs AES with Blockchain

D Time complexity

The time complexity or time consumption of the algorithm is defined as the amount of time required to develop the learning data model. The result with Space complexity and plots showing their comparison is given in Figure 6. The time consumption is given by the following equation:

Time consumption= Algorithm stop time –Algorithm start time ------ (5)

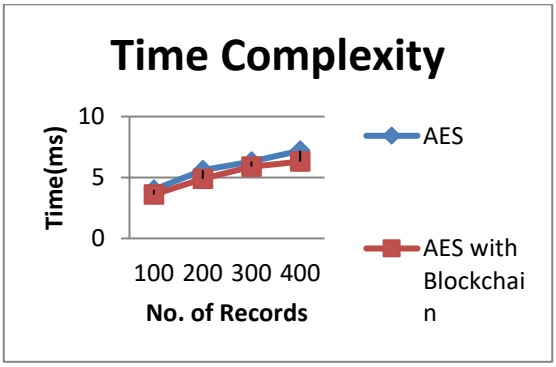

Figure 6: Time consumption of AES vs AES with Blockchain

V. CONCLUSIONS

A Blockchain is open-source software, Open APIs, and enterprise hardware. The components used in the Blockchain system facilities easier and faster interoperability between systems. The system can effectively handle a higher volume of data and more block users. This paper provides a survey of the different technology used by the researcher for implementing the Blockchain system in various sectors. Medical care is one among them and it has become an important part of human life and this medical data such as doctor's prescriptions, old medical history reports. Despite the progress in the healthcare section and technological development in the PHR framework even though they confronted little more problems. In this paper, a framework which produces the creation in Blockchain system used in medicinal fields for the rightness of medical records and to increase the interactivity of currently using data and in addition we also evaluated how the Blockchain creation is valuable for the healthcare filed and how the system is used for Personal health records (PHR). And it is easier for the users to use and understand the system. In the future system, we are intended to make a payment module to increase the system's advancement in this existing system. But it has a certain consideration and to choose how much patients should pay for consultation given by the specialists. This proposed system and presentation of all models is dissected by a precision %, Error rate, space utilization, and Time utilization. The outcome of this proposed system clearly shows that the vertically parceled information gives better execution in the existence utilization regardless of little lower precision. The exactness rate with a lower mistake rate is shown by a superior presentation on a level plane divided information.

REFERENCES

1. Domadiya, N., & Rao, U. P. (2019). Privacy-preserving distributed association rule mining approach on vertically partitioned healthcare data. Procedia computer science, 148, 303-312.
2. Salehi, H., Das, S., Biswas, S., & Burgueño, R. (2019). Data mining methodology employing artificial intelligence and a probabilistic approach for energy-efficient structural health monitoring with noisy and delayed signals. Expert Systems with Applications, 135, 259-272.
3. Pirbhulal, S., Wu, W., Li, G., &Sangaiah, A. K. (2019). Medical information security for wearable body sensor networks in smart healthcare. IEEE Consumer Electronics Magazine, 8(5), 37-41.
4. Sundermann, A. J., Miller, J. K., Marsh, J. W., Saul, M. I., Shutt, K. A., Pacey, M., ... & Harrison, L. H. (2019). Automated data mining of the electronic health record for investigation of healthcare-associated outbreaks. Infection Control & Hospital Epidemiology, 40(3), 314-319.
5. Cottrell, E. K., Dambrun, K., Cowburn, S., Mossman, N., Bunce, A. E., Marino, M., ... & Gold, R. (2019). Variation in electronic health record documentation of social determinants of health across a national network of community health centers. American journal of preventive medicine, 57(6), S65-S73.
6. Spencer, A., & Patel, S. (2019). Applying the data protection act 2018 and general data protection regulation principles in healthcare settings. Nursing Management, 26(1).
7. McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62-75.
8. Yookesh, T. L., Boobalan, E. D., &Latchoumi, T. P. (2020, March). Variational Iteration Method to Deal with Time Delay Differential Equations under Uncertainty Conditions. In 2020 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 252-256). IEEE.

9. Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326.
10. Garikapati, P., Balamurugan, K., Latchoumi, T. P., & Malkapuram, R. (2021). A Cluster-Profile Comparative Study on Machining AlSi 7/63% of SiC Hybrid Composite Using Agglomerative Hierarchical Clustering and K-Means. Silicon, 13, 961-972.
11. Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. Journal of medical systems, 43(1), 1-9.
12. Pavan, V. M., Balamurugan, K., &Latchoumi, T. P. (2021). PLA-Cu reinforced composite filament: preparation and flexural property printed at different machining conditions. ADVANCED COMPOSITE MATERIALS.
13. Al Omar, A., Bhuiyan, M. Z. A., Basu, A., Kiyomoto, S., & Rahman, M. S. (2019). A privacy-friendly platform for healthcare data in the cloud-based on blockchain environment. Future generation computer systems, 95, 511-521.