Impact Factor (SJIF): 5.301

International Journal of Advanced Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 6, Issue 2, February-2019

Blockchain for Healthcare: Parallel System for Medical Record

Dhanashree[1] Akshata[2] Sheetal [3]Sharavri[4]

Abstract: Healthcare applications are considered as promising fields for block chain, where students can be monitored using blockchain networks. Current blockchain health care research trends focus on student's reliable communication, student's mobility, and energy client routing, as a few examples. However, deploying new technologies in healthcare applications without considering security makes student's privacy vulnerable. Moreover, the physiological data of an individual are highly sensitive. Therefore, security is a paramount requirement of healthcare applications, especially in the case of student's privacy, if the patient has an embarrassing disease.

This project discusses the security and privacy issues in healthcare application using blockchains. We highlight some popular healthcare projects using block chain networks, and discuss their security the existing systems solutions can simply protect the patient's data during transmission, but cannot protect the inside attack where the administrator of the patient database reveals the sensitive patient data. So we are proposing a approach to prevent the inside attack by using multiple data servers to store patient data. The main contribution of this paper is to distribute patient's data securely in multiple data servers and performing the Paillier cryptosystems to perform statistical analysis on the patient data without compromising the patient 's privacy.

Keywords: Wireless medical network, Patient data privacy, Paillier encryption, AES

I. INTRODUCTION

Blockchain is a network to monitor physical or environmental conditions such as temperature, sound, pressure, etc. The development of block chain was motivated by air pollution monitoring, water quality monitoring, land side detection, forest detection, habitat monitoring and so on. Though there are many applications in wireless block chain network domain, human healthcare applications takes the major role. In human healthcare, sensors are used to monitor the patient's' health status such as temperature level, sugar level, heart beat rate, blood pressure. For instance, if the patient's sugar level is monitored 10 times per day then the data is updated in the database which is present in the local server. Likewise the values for blood pressure, heart beat, and temperature are also noted at regular intervals. There are many security issues such as data stealing, stealing and updating, storing the wrong values. Suppose if the intruder is trying to hack the patient details, there are many chances for the misuse of data which may lead to severe consequences. The data can be modified by the hackers due to lack of security. The treatment prescribed by the doctors can be hacked which may even lead to death of the patient's. Patient's are the victims because of the above issues. To prevent these issues, the intrusion detection system is proposed. An intrusion detection system is a system used to check the malicious activities and produces electronic reports to a management station. It consists of Paillier algorithm key cryptosystems. The algorithm is used to encrypt the patient details before storing it in the database and perform decryption when needed by the physician Department.

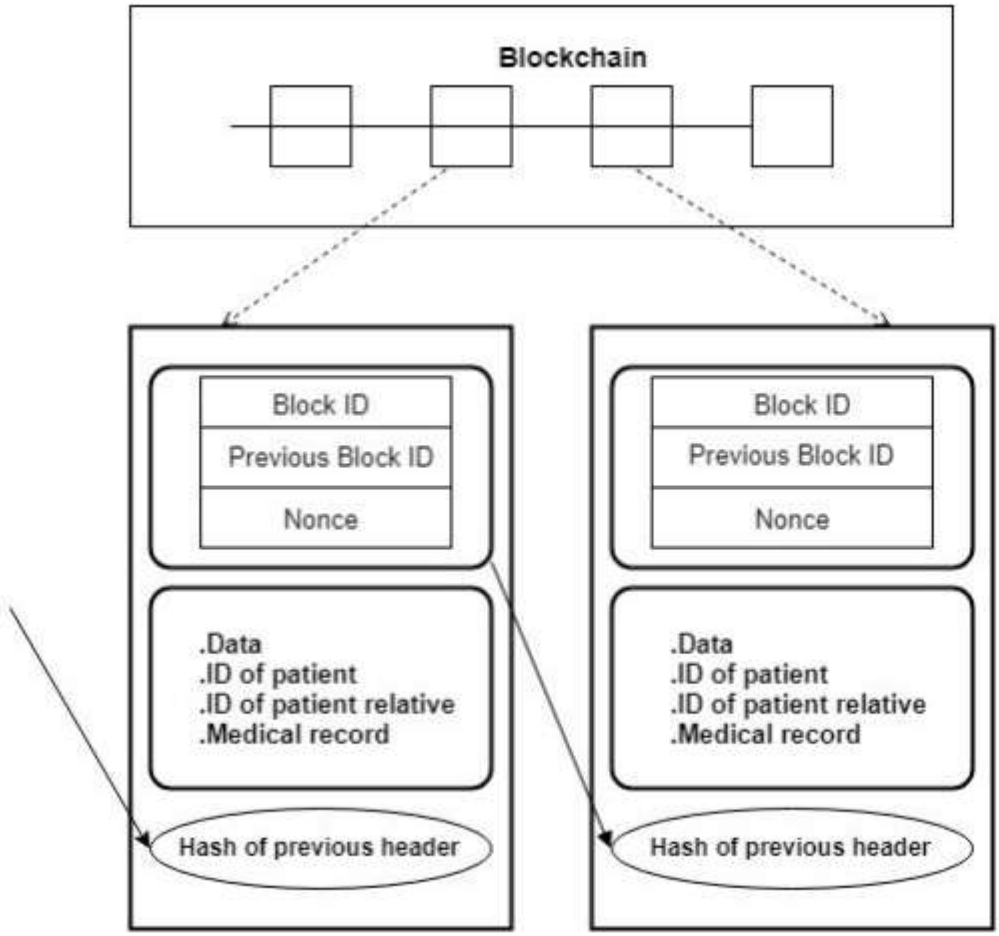

Figure 1: Blocks in Healthcare

II. RELATED WORK

Dan Bogdanov et al.[1] Gathering and processing sensitive data is a difficult task. In fact, there is no common method for building the necessary information systems. In this paper, probably secure and effective general-purpose computation system to address this problem. Our solution SHAREMIND is a virtual machine for privacy-preserving data processing that on share computing techniques. This is a standard way for securely evaluating functions in a multi-party computation environment. The novelty of our solution is in the choice of the secret sharing scheme and the design of the protocol suite. We have made many practical decisions to make large-scale share computing feasible in practice. The protocols of SHAREMIND are information theoretically secure in the honest but curious model with three computing participants. Although the honest but curious model does not tolerate malicious participants, it still provides significantly increased privacy preservation when compared to standard centralized databases.

Subhadeep Banik et al.[2] The implementation of the AES encryption core by Moradi et al. at Euro crypt 2011 is one of the smallest in terms of gate area. The circuit takes around 2400 gates and operates on an 8 bit data path. However this is an encryption only core and unable to cater to block cipher modes like CBC and ELmD that require access to both the AES encryption and decryption modules. we look to investigate whether the basic circuit of Moradi et al. can be tweaked to provide dual functionality of encryption and decryption (ENC/DEC) while keeping the hardware overhead as low as possible. As a result, we report an 8-bit serialized AES circuit that provides the functionality of both encryption and decryption and occupies around

2645 GE with a latency of 226 cycles. This is a substantial improvement over the next smallest AES ENC/DEC circuit (Grain of Sand) by Feldspar et al. which takes around 3400 gates but has a latency of over 1000 cycles for both the encryption and decryption cycles.

Shuai Wang et al.[3]To improve the accuracy of diagnosis and the effectiveness of treatment, a framework of parallel healthcare systems (PHSs) based on the artificial systems + computational experiments + parallel execution (ACP) approach is proposed. PHS uses artificial healthcare systems to model and represent patient's conditions, diagnosis, and treatment process, then applies computational experiments to analyze and evaluate various therapeutic regimens, and implements parallel execution for decision-making support and real-time optimization in both actual and artificial healthcare processes. In addition, we combine the emerging blockchain technology with PHS, via constructing a consortium blockchain linking patient's, hospitals, health bureaus, and healthcare communities for comprehensive healthcare data sharing, medical records review, and care auditability. Finally, a prototype named parallel gout diagnosis and treatment system is built and deployed to verify and demonstrate the effectiveness and efficiency of the blockchain-powered PHS framework.

Zainab Alhadhrami et al.[4] Blockchain as a technology emerged to facilitate money exchange transactions and eliminate the need for a trusted third party to notarial and verify such transactions as well as protect data security and privacy. New structures of Blockchain have been designed to accommodate the need for this technology in other fields such as e-health, tourism and energy. This paper is concerned with the use of Blockchain in managing and sharing electronic health and medical records to allow patient's, hospitals, clinics, and other medical stakeholder to share data amongst themselves, and increase interoperability. The selection of the Blockchain used architecture depends on the entities participating in the constructed chain network. Although the use of Blockchain may reduce redundancy and provide caregivers with consistent records about their patient's, it still comes with few challenges which could infringe patient's privacy, or potentially compromise the whole network of stakeholders. In this paper, we investigate different Blockchain structures, look at existing challenges and provide possible solutions. We focus on challenges that may expose patient's privacy and the resiliency of Blockchain to possible attacks.

Michael O'Keee et al.[5] A So long as there are secrets, there is a need for encryption to help guard these secrets. The Paillier Cryptosystem is an encryption scheme that can be used to conceal information, with a few interesting properties. When creatively applied, allow the Paillier Cryptosystem to be used in ways that other cryptographic systems simply can't be used. This paper will explore how the Paillier Cryptosystem works, how these properties arise, and one way in which the system can be used in a real-world situation as a result of these properties.

III. EXISTING SYSTEM

The security may be a overriding demand of care applications, particularly within the case of patient privacy, if the patient has embarrassing malady. This project discusses the safety and privacy problems in care application victimization WMSNs. we tend to highlight some widespread care comes victimization wireless medical device networks, and discuss their security the prevailing systems solutions will merely shield the patient knowledge throughout transmission, however cannot shield the within attack wherever the administrator of the patient info reveals the sensitive patient knowledge.

3.1 Disadvantages of Existing System

1. Less secure.
2. Cannot protect inside attacker.
3. If any hacker get data from one DB server then whole data will be get to hacker.

IV. PROPOSED SYSTEM

Block chain deployed at a large scale in a distributed manner, and their data rates differs based on their applications, where the Wireless Medical Sensor Networks have direct human involvement are deployed on a

small scale must support mobility (a student can carry the devices), and Block chain requires high data rates with reliable communication. Physiological conditions of student's are closely monitored by deploying Wireless medical sensor motes. These medical sensors are used to sense the student's vital body parameters and transmit the sensed data in a timely fashion to some remote location without human involvement. Using these medical sensors reading the doctor can get the details of a student's health status. The student's vital body parameters include heart beats, body temperature, blood pressure, sugar level, pulse rate. Block chain carry the quality of care across wide variety of healthcare applications. In addition, other applications that also benefit from Block chain include sports-person health status monitoring and student's self-care. Several research groups and projects have started to develop health monitoring using wireless sensor networks. Block chain healthcare application offers a number of challenges, like, reliable transmission of data, secured data transmission, nodes mobility, detection of event delivery of data in time, power management, etc. Deploying new technologies in healthcare applications without considering security often makes student privacy vulnerable. For instance, the student's physiological vital signals are very sensitive so the leakage of the student's diseased data could make the student embarrassed. Sometimes revealing disease information can make it impossible for them to obtain insurance protection and also result in a person losing their job.

4.1 Advantages of Proposed System

1. Practical approach to prevent the inside attack by securely distributing the patient data in multiple data servers.
2. Employing the Paillier cryptosystems to perform statistical analysis on the patient data without compromising the patient's' privacy.
3. In Proposed system, Due to secured distributed database architecture we can achieve data storage & data analysis security.
4. Proposed data retrieval technique allows to retrieve the data compromised server(s)

V. SYSTEM ARCHITECTURE

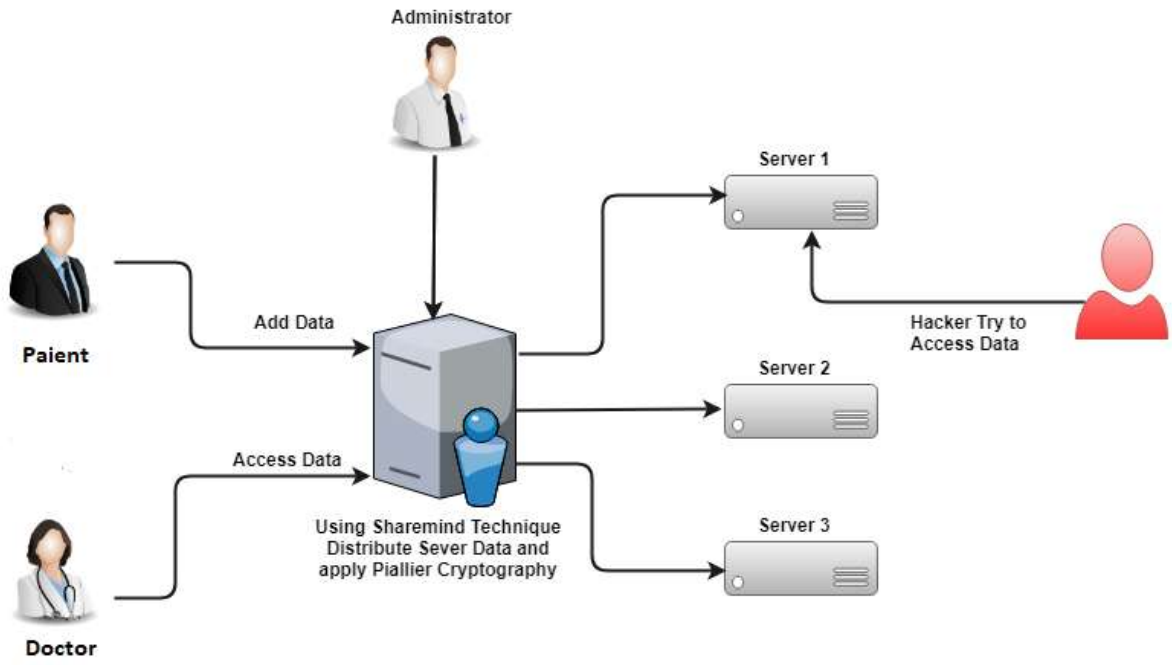

Figure 1. Proposed System Architecture

VI. MATHEMATICAL MODEL

Let W be the whole system which consists:
W= {IP, PRO, OP}
Where,

IP is the input of the system.

A) IP= {P, PD, U}

1. P is the number of patient's in the system.
2. PD is the patient's database system which consists of number of patient's information.
3. U is the set of number of users in the systems that are accessing the data from patient's database server.

B) PRO is the procedure of our proposed system:

Step 1: At first the wireless medical network which senses the patient's body and transmits the patient data to a patient database system.

Step 2: A patient database system which stores the patient data from medical and provides querying services to users (e.g., physicians and medical professionals).

Step 3: A patient data access control system which is used by the user (e.g., physician) to access the patient data and monitor the patient.
Step 4: A patient data analysis system which is used by the user (e.g., medical researcher) to query the patient database system and analyze the patient data statistically.

C) OP is the output of the system:

The system provides the privacy to the patient's sensible data available on the patient's database system in the sense of inside attacks.

VII. CONCLUSION

We have investigated the security and privacy issues in the block chain data collection storage and queries and presented a complete solution for privacy-preserving block chain net-work through the ad-hoc network. To keep the privacy of the student's data, we proposed a new data collection protocol which splits the student's data into three numbers and stores them in three data servers, respectively. As long as one data server is not compromised, the privacy of the student's patient data can be preserved. For the legitimate user e.g., physician to access the student's data, we proposed an access control protocol, where three data servers cooperate to provide the user with the student's data, but do not know what it is. In case any two of three servers are compromised the proposed system provides a proxy-based data retrieval system.

REFERENCES

[1] Yi, Xun, et al. "Privacy Protection for Wireless Medical Sensor Data." IEEE Transactions on Dependable and Secure Computing 13.3 (2016): 369-380.
[2] X. Yi, J. Willemson, F. Nat-Abdesselam. Privacy-Preserving Wireless Medical Sensor Net-work. In Proc. TrustCom13, pages 118-125, 2013.

[3] D. He, S. Chan and S. Tang. A Novel and Lightweight System to Secure Wireless Medical Sensor Networks. IEEE Journal of Biomedical and Health Informatics, 18 (1): 316-326, 2014.
[4] Y. M. Huang, M. Y. Hsieh, H. C. Hung, J. H. Park. Pervasive, Secure Access to a Hierarchi-cal Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks. IEEE J. Select. Areas Commun. 27: 400-411, 2009.
[5] K. Malasri, L. Wang. Design and Implementation of Secure Wireless Mote-Based Medical Sensor Network. Sensors 9: 6273-6297, 2009.