Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2020)
Vol.02/ No. 01
Pages:19-28
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2020.1.003

Enhancing Security Mechanisms for Healthcare Informatics Using Ubiquitous Cloud

Dinesh Kumar,
Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Andra Prdesh, India.
Email: adinesh@kluniversity.in

Dr. S. Smys
Professor,
Department of Computer Science Engineering
RVS technical Campus
Coimbatore, India
Email:smys375@gmail.com

Abstract: The most vital chores of the health care is the proper attention and sharing of the information's about the patients record maintained whenever it is needed. The failure in proper maintenance of the patient's particulars and proper sharing of information's when required would lead to loss of privacy and reliability resulting in the inert and severe effects on the particulars of the patients as well as their lives respectively. So securing of the health care particulars in electronic form becomes a very important necessity nowadays. The constant monitoring of the centralized storage of health records that are prone to security threats are very difficult. So the paper puts forward a block chain technology to safeguard the reliability of the information's stored and utilizes the digital signature with authentication to protect the private information's in the patient's record developing a model utilizing the cloud that enables the authenticity and the reliability of the information. The model put forth in the paper was examined and compared with the traditional techniques used for storing the medical records, on the terms of reply time, along with the cost of storing and retrieving.

Keywords: Ubiquitous Cloud, Security Mechanism, Health Records in Electronic Form, Block Chain, Authentication

1. Introduction

Health care is of utmost importance today, as the number of patients and diseases continues to rise. Preserving a person's health records is important in order to accurately handle potential health needs. The current environment maintains a similar pattern for the preservation and exchange of health data across different organizations. Even though data are exchanged freely with other organizations, the confidentiality of health records remains a major problem. Data privacy often constitutes a threat and health records are vulnerable to security crises. In the current research a system is introduced to address the issues of confidentiality and data reliability. Preserving the private information in the medical record is highly important. Records can also be exchanged only if the corresponding values are partly dependent on attributes. This is achieved by using anonymous access by exchanging only the general information and then using attribute values to separate highly protected information. Thus, the model put forth scopes in enhancing the security mechanism to view the medical details of a patient.

The prime challenges in storing the health care data are (i) availability of data: The constant flow of data is an essential requirement of the healthcare sector, as it is crucial for patient treatment. A continual flow of data are often affected by the failures in the hardware components, due to the malfunctioning of the storage components. , but these kinds of interruption are hardly accepted in the medical field as it results in major losses such as patients' life as well as money. The next issues is the (ii) elasticity: the huge flow of data requires enormous of storage facility and the it often necessary to expand the storage space whenever new data's are to be stored and it must also be taken care that the alteration in the storage space made is not affecting the previously existing information's, so it becomes necessary to keep up the elasticity to elude the issues in properly maintain the data, and finally the (iii) proper functioning: It is necessary to see to that the stored data are kept secure and given only to the authenticated persons at a minimal response time and cost.

The present situations of the medical industry with enormous information's about the patients are maintained as "electronic health records" as it minimizes the time- intense labors and the costly techniques in observing the entire medical record of the patient, maintaining , properly delivering them by enabling a ubiquitous access as it is empowered by cloud. Cloud services provide the infrastructure needed at a lower cost and higher quality. When used in the healthcare sector, cloud computing reduces the expense of storage, processing and upgrading, with greater performance and quality. The block diagram below in figure.1 shows the basic structure of the "EHR".

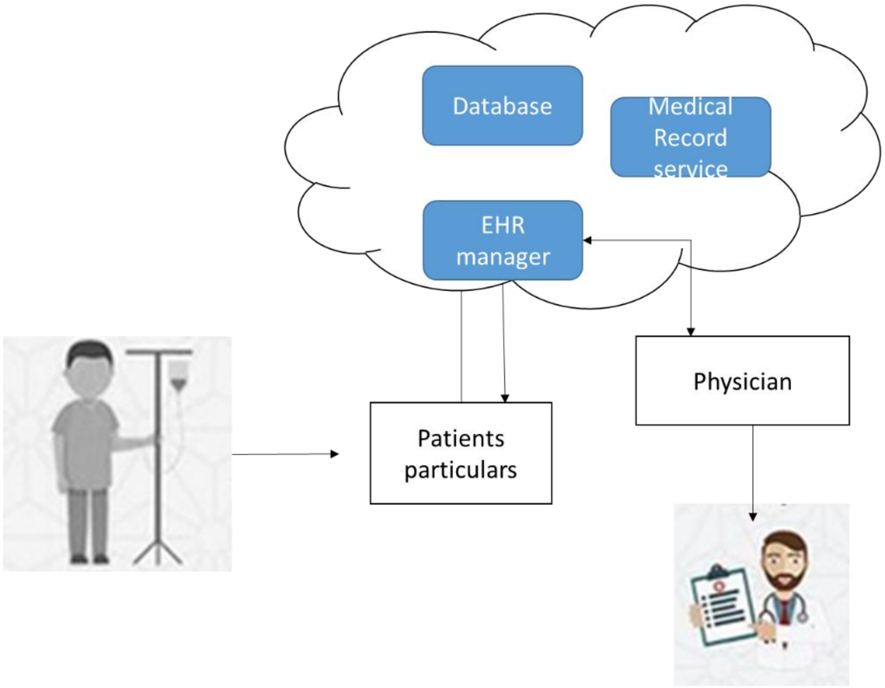

Figure.1 Basic “EHR” Structure

But the security provisions of the cloud are still under research, as the “electronic heath care records hold” very important particulars and the information’s of the individuals, it is essential that these information’s are guarded properly to elude the unnecessary hackings and misdirection’s in the treatment.

So the paper puts forward the cloud frame work that is capable of affording the security demands of the “HER” utilizing the block chain, and the multi signature implementation (MSI) that is commonly referred as the “KSI”. The enhanced security mechanism for the health care informatics using the ubiquitous cloud is formulated with the part 2 presenting its related works and the existing methods, part 3 detailing the security model put forth with the help of the block chain and MSI, part four providing the performance assessments and part 5 the Conclusion.

2. Related Works

The current cryptography system is the primary driving force of the development of the BC, now the related work section provides the particulars of the techniques that were practiced earlier and the prevailing security systems in securing the network. Sultan, et al [1] in his paper elaborates the issues and the chances in utilizing the cloud service to observe the health status. Narayanan, et al [2] uses the cloud services to control the access of the medical systems. Chauhan et al [3] elaborates the methods, potential and issues that are associated with the medical care mechanisms developed utilizing the cloud. John, et al [4] utilizes the cloud platform to avail the health status as service. Kuo et al [5] discusses the "Opportunities and challenges of cloud computing to improve health care services."

He et al [6] puts forward the naively procedure to formulate the ubiquitous service for medical care utilizing the cloud. Linn et al [7] designs the "Blockchain for health data and its potential use in health it and health care related research." Buldas, et al [8] discusses the details of the KSI how it is used in developing a distributed hash tree. Smys, S et al [9] has conducted the Big Data Business Analytics as a Strategic Asset for Health Care Industry." Valanarasu, et al [10] puts forth the mechanism incorporating the IOT and the AI along with the Cloud for the Health care system development.

Sridhar, S et al [11] details the designing of the novel multi-level authentication strategy that could be utilized in the cloud platform and in his other paper Sridhar, S., et al [12] elaborates the A survey on cloud security issues and challenges with possible measures. Whereas Bhalaji, N et al [13] details the use of block chain in the wireless communication networks and Jennifer S. Raj et al [14] elaborates the usefulness of the IOT and the BDA in the cloud paradigm that is used for the health services.

3. Proposed Security Frame Work

3.1. Back Ground

The back ground section holds the details of the major techniques involved in the security model put forth in the paper, it provides the basic details of the block chain and its associated techniques as well as the MSI (KSI) that is merged with the block chain technology in the paper to enhance the security mechanism of the “EHR”. Starting with the block-chain (BC) technology and its associated techniques the paper takes effort to elaborate the basic uniqueness of the block chain the, procedures involved in it and the risks endured by it. The BC is a peer-peer system with the capability of making transactions in a transparent and secure manner. The key advantage of BC is that it has no links that are already defined, and it also manages circumstances under which a trustworthy party turns out to be dangerous, thus minimizing the danger and enhancing the system's robustness. The fundamental BC –divisions are “public, private and consortium centered private” and the essential components of the BC are “block header (BH) with the blocks along with the merle tree (MT). The BH is comprised of the preceding BH values and a hash-signature. Every block is allowed to perform transaction and alter the data content present in each blocks and update new blocks into the chain whenever it is necessary. The MT is the combination of mathematically derived file coined as hash and another file that was developed on the similar duration. These file are developed or altered during a particular duration and incremented utilizing the cryptographic connections. The root hash is usually produced to be used as the proof of contribution of every file that is created. The key advantage of BC is that the rules could be updated and the data could be adjusted as and when necessary in the BC. The risk of attack is reduced in large measure due to decentralized architecture. The private BC are more secure and beneficial because of their, fast computing capacities and improved verification. Despite its advantages the block chin also has certain risks that are categorized as “standard risks, smart contract risks and the value transfer risks”

The next fundamental technique involved in the proposed architecture is the Multi-signature implementation that is termed as the KSI, and otherwise known as the key-less-infrastructure. It totally relies on the hash function that are utilized in delivering the necessary security to the system. The aggregator, cores and the gateways play a major role in the generating the signatures that are key less. This is basically not without keys, but is implemented with multiple signature involving the following steps such as (i) hashing: “The documents to be signed are hashed, and the hash values are used in the rest of the process to represent the documents”, (ii) Aggregation: “A global, temporary hash tree per round is created to represent all documents signed in a round. The duration of the rounds may vary; in the described implementation, it is set at one second” and (iii) publication: The hash values obtained on every aggregator round is gathered into a unending hashing calendar or tree and the topmost hash value in that tree is published as trust anchor. This guarantees the privacy, transparency and the secrecy of the information’s.

3.2 Methodology

The proposed model combines MSI and the BC to enhance the security mechanism of the “EHR” the information’s kept stored inside with the sign in the BC-MSI, using the multiple signatures and the hash functions. Eluding the need for third party maintenance. The flowchart below explains the complete research process for developing the security mechanism for the medical particulars.

DOI: https://doi.org/10.36548/jucct.2020.1.003

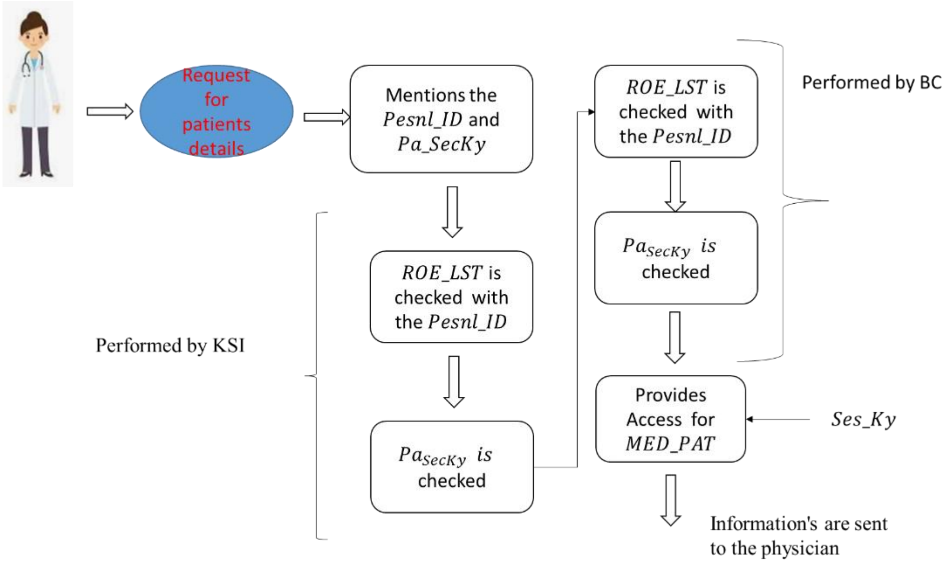
Request for patients details
Mentions the $Pesnl\_ID$ and Pa_SecKy
ROE_LST is checked with the $Pesnl\_ID$
Pa_{SecKy} is checked
Performed by KSI
ROE_LST is checked with the $Pesnl\_ID$
Pa_{SecKy} is checked
Performed by BC
Provides Access for MED_PAT
Ses_Ky
Information's are sent to the physician

Figure. 2 Security Mechanism Put Forth

According to the flow chart shown in the figure.2 the security mechanism function as follows, the Doctor treating a patient to know his complete history, should makes requisition ($Reqstn$) for the particulars of the patients providing his personal identification ($Pesnl\_ID$) and the patient's secret_key (Pa_SecKy), The particulars of the patients that was reclaimed is kept in reserve in a database that is retained locally. And verification process takes place, the $Pesnl\_ID$ provided by the physician is verified with the right of entry list (ROE_LST), once verified the MSI, checks the Pa_SecKy provided and to confirm its confidentiality and the information provided are once again verified by the BC, and the $Reqstn$ is forwarded to the Medical particulars (MED_PAT) databank and allows the physician to access the patient's particulars, providing a term key (Ses_Ky) authenticating the user.

The proposed method ensures the security of the "EHR" stored in the cloud with multiple verifications, authenticating that the persons requesting the information's by this the security breaches in the health care particulars, hacking the person's personal details or replacing the particulars leading to misdirection in treatment could be eluded. The security mechanisms, front end is encompassed with the clients and the stake holders who request and maintain the particulars of the medical records respectively and the verification and the authentication process involving the series of validation levels are done in its back end.

The multiple signs are used in safe guarding the integrity of the data rather than the using keys, this MSI (KSI) allows the user to substantiate the registration time of the medical particulars, the block diagram below explains the security offered by the BCMSI,

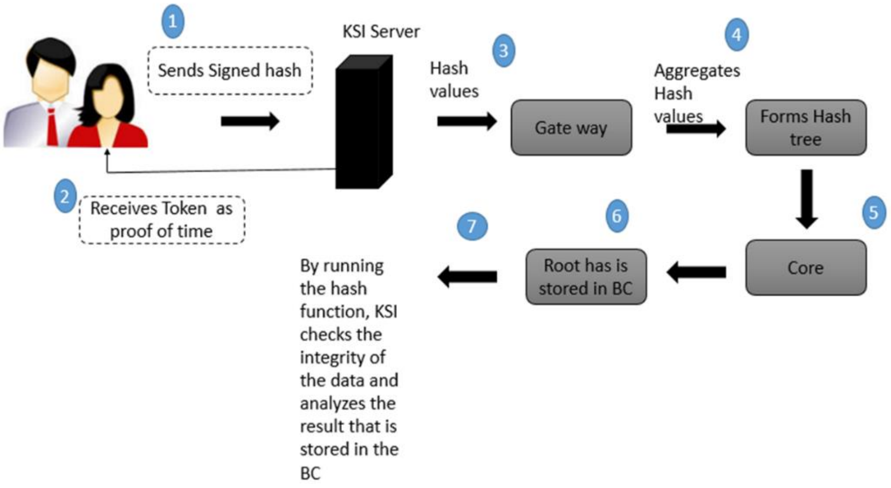
1
Sends Signed hash
2
Receives Token as proof of time
KSI Server
3
Hash values
Gate way
4
Aggregates Hash values
Forms Hash tree
5
Core
6
Root has is stored in BC
7
By running the hash function, KSI checks the integrity of the data and analyzes the result that is stored in the BC

Figure.3 Working of BCMSI

With the number of transactions the ledger size increases. The hash path is stored with the document, so that the validity and timestamp of the document can be easily checked. If the transaction frequency is unusual then function proof is not an acceptable option.

4. Results Evaluation

The “Apace J meter” was used to validate the performance of the security mechanism developed to prevent the hacking in the “EHR” in terms of the time taken to reply as well as the cost spent on storing and retrieving as the cloud services are provided in pay as you go manner. The table.1 below provides the duration consumed in developing the Block chain, updating the information in it and considering also the time taken to sharing and deletion.

Data Type	Average Time (s)	Transfer File Size (KB)
Creation of Block	.520	1.25
Updating Blocks	.435	1..20
Sharing Blocks	.442	1.22
Deleting Blocks	.545	1.09

Table.1 Block Chain Details

From the above table it was found that the average duration taken to retrieve the data utilizing the proposed mechanism was much convincing than the traditional storages schemes that enable the data storage in cloud, the Figure. 4 below shows the average time taken to provide the response based on the size of the file that was requested.

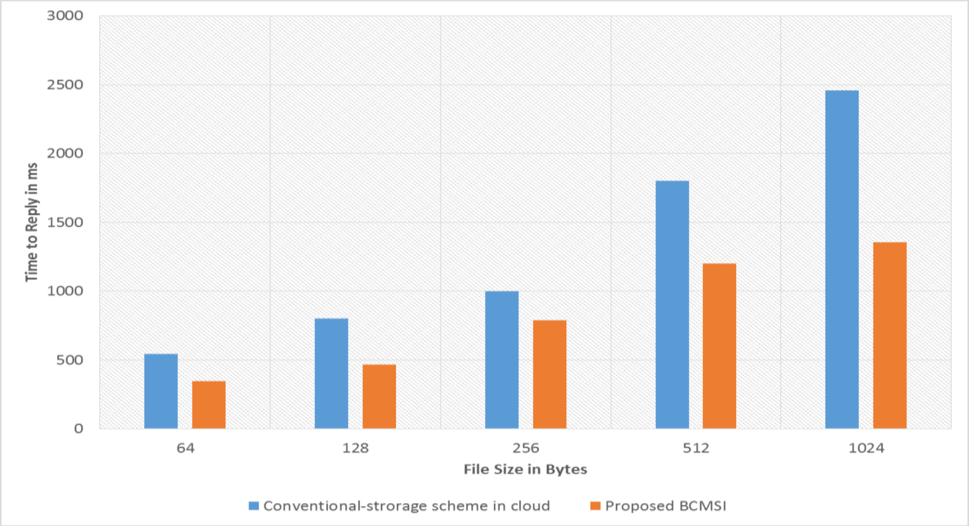

Figure.4 Time to Reply

The results observed on the response time for the proposed and the traditional storage schemes shows that the mechanism put forth consumes lesser time compared to aforementioned.

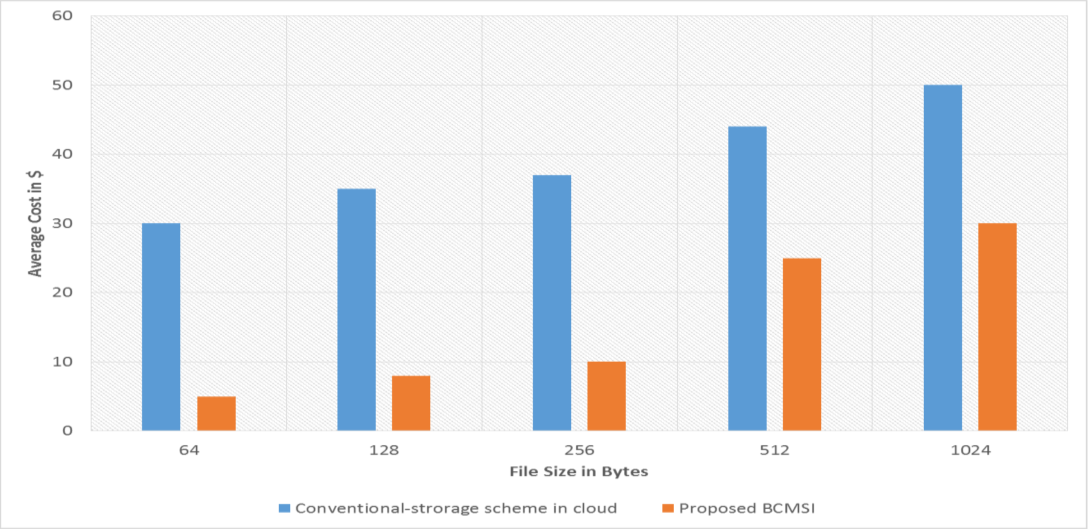

Figure.5 Average Cost

The figure.5 is the average cost that was consumed by the mechanism put forth in the paper and the conventional methods, according to the size of the file that was stored as well as retrieved. The results observed shows that the mechanism put forth is cost effective than most of the conventional schemes.

5. Conclusion

The security mechanism was put forth in the paper incorporating the block chain technology with the key less signature technology that is implemented with multiple signatures to verify the authenticate the data that stored in the cloud, the series of authentication levels enabled the data storage and retrieval to be safe. The validation of the mechanism put forth utilizing the Apache J Meter proved that the cost and the response time of the proffered method was more convincing compared to the existing schemes for storing in cloud. In future the paper is implement the security mechanism in the cloud that are federated and the compare its efficiency with the existing methods.

References

[1] Sultan, Nabil. "Making use of cloud computing for healthcare provision: Opportunities and challenges." *International Journal of Information Management* 34, no. 2 (2014): 177-184.

[2] Narayanan, Hema Andal Jayaprakash, and Mehmet Hadi Güneş. "Ensuring access control in cloud provisioned healthcare systems." In *2011 IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 247-251. IEEE, 2011.

[3] Chauhan, Roma, and Amit Kumar. "Cloud computing for improved healthcare: Techniques, potential and challenges." In *2013 E-Health and Bioengineering Conference (EHB)*, pp. 1-4. IEEE, 2013.

[4] John, Nimmy, and Sanath Shenoy. "Health cloud-Healthcare as a service (HaaS)." In *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1963-1966. IEEE, 2014.

[5] Kuo, Mu-Hsing. "Opportunities and challenges of cloud computing to improve health care services." *Journal of medical Internet research* 13, no. 3 (2011): e67.

[6] He, Chenguang, Xiaomao Fan, and Ye Li. "Toward ubiquitous healthcare services with a novel efficient cloud platform." *IEEE Transactions on Biomedical Engineering* 60, no. 1 (2012): 230-234.

[7] Linn, Laure A., and Martha B. Koo. "Blockchain for health data and its potential use in health it and health care related research." In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, pp. 1-10. 2016.

[8] Buldas, Ahto, Andres Kroonmaa, and Risto Laanoja. "Keyless signatures' infrastructure: How to build global distributed hash-trees." In *Nordic Conference on Secure IT Systems*, pp. 313-320. Springer, Berlin, Heidelberg, 2013.

[9] Smys, S., and C. V. Joe. "Big Data Business Analytics as a Strategic Asset for Health Care Industry." *Journal of ISMAC* 1, no. 02 (2019): 92-100.

[10] Valanarasu, Mr R. "Smart and Secure Iot and Ai Integration Framework for Hospital Environment." *Journal of ISMAC* 1, no. 03 (2019): 172-179.

[11] Sridhar, S., and S. Smys. "A hybrid multilevel authentication scheme for private cloud environment." In *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, pp. 1-5. IEEE, 2016.

[12] Sridhar, S., and S. Smys. "A survey on cloud security issues and challenges with possible measures." In *International Conference on Inventive Research in Engineering and Technology*, vol. 4. 2016.

[13] Bhalaji, N. "Qos and Defense Enhancement Using Block Chain for Fly Wireless Networks." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 01 (2019): 1-13.

[14] Smys, S., and Jennifer S. Raj. "Internet of Things and Big Data Analytics for Health Care with Cloud Computing." *Journal of Information Technology* 1, no. 01 (2019): 9-18.