Secure EHR-Data Sharing of cloud based systems using Block chain approach

- Aniket Kishore Das

Abstract:

EHR-Electronic-Health Records creates the positive significance in the researches of disease diagnosis and aiding the medical practitioners for perusing the treatment phases. Hence in present decade, cloud based-systems enables delivery of computing platform and storage-space depicted as the service in cloud-server. This has been witnessed, and the storage of EHR-Electronic health records has been applied upon mobile cloud-environment through the implementation of block chain approach. This enhance model facilitates the data manipulation in healthcare-services with higher flexibility, EHR-availability and lower operational-costs of the system. The data sharing of the EHR-patient records has to be guaranteed with secure data, within mobile cloud-computing with reliability and without data-leakage. Hence a novel EHR sharing-framework-model integrating the clock-chain approach using AES-algorithm is implemented in mobile cloud-computing environment. The framework would connect the data among the different health-care providers. This model permits the participants for accessing the patient records more secured way from any location. The data is encrypted through AES-block-chain encryption algorithm, in prior to cloud-outsourcing. In turn, for the data-retrieval, Decryption process in turn decrypts the data in prior to the downloading process. This framework-model has been designed as the trust-worthy control-mechanism, utilizing the smart-contracts for attaining efficient EHR-data manipulation between the health-care providers and the users. On the basis of cryptographic-primitives, the proposed-framework depicts the higher computational efficiency than the other cloud-computing techniques.

Keywords: Cloud based systems, EHR-electronic-health records, AES—advanced-encryption algorithm, block-chain network, smart-contracts, robustness, secure, reliability.

1. Introduction:

In medical Stream, EHR-Health-Electronic-Records contribute the data for quality enhancement and also minimizes the health-care costs. This is complex task posed as the challenge due to the privacy-compatibilities complications and the complexities in the privacy of the data content. But also in the process of data interaction and privacy of the content gets impacted, in data integration mechanism. Hence this personalised health-records of the patient data has to be analysed in the cloud-computing environments. This enables faster manipulation of patient data within the secure system, applied with encryption system. Various studies has been put forward for the implementation of such systems in cloud-computing. The efficient access of the cloud resources and manipulation of those entities and data can be accomplished through these block-chain network. This block-chain network is utilized to those health-care providers system wherein the upload requisition is converted to blocks and further creates the block-chain. This block chain in incorporated to the cloud-server by generating the encrypted key. This encrypted key is then decrypted for uploading the download file request, uploading the data request and in monitoring the status of the patient-records within the cloud-system. In such systems, the privacy-shred block- chain based framework in employed in IoT environment, in smart-city culture[1]. The privacy of data is transmitted by partitioning block-chain to different channels, where every channel consists definite organisation count and manipulates the information such as financial-details, health data and smart-cars. The access of the data is controlled through smart-contract rules in mutual systems. BPRS-block-chain based privacy-preserving data-sharing is applied in certain studies, where the original EMR-electronic-medical records stored in cloud server securely, and the indexes been reserved through tamper proof-consortium block-chain network[2]. In such systems the owner of the data has capability for distributing secret-key to user and granting the scheme-archives and access-policies through the encryption and decryption of the shared-data[3]. This implementation would significantly minimizes the data leakage risks where the block-chain key indexes checks that EMR, ought not to be arbitrarily changed. And also it enhances system access-control within the cloud-system[4].Genetic-algorithm and DWT-Discrete-wavelet transform algorithm for improving the queuing-optimization and enhancing the security[5].

1.2. Paper-Organisation:

The organisation of the paper can be stated as follows. Section 1 of the paper enumerates the introductory section of the paper. Section 2 of the paper, states the survey analysis of the existing studies of EHR-secure cloud-based systems based on block-chain approach. Section 3 illustrates the proposed-framework. The section 4 depicted the results of the proposed-framework.

2. Related-Works:

HER-Health Electronic-Records would shares the health-care data for enhancing the data-quality and minimizes the health-care costs. Hence cloud based EMR-electronic-medical records sharing mechanism yields a lot of benefits, where the centralization of cloud-resources exhibits malicious threats to privacy-control and security mechanism. With the integration of cloud-computing, block chain based technology seen as the efficient solution for pointing out the problems of vulnerability, anonymity, security and decentration concepts.

MedBlock-block-chain network based information-management system is employed for handling the information of patients[6]. In this framework, the Med-block distributed ledger permits the access and retrieval of EMR records. Medblock framework as an instance for block-chain based system in cloud computing. As the inferences of the study, this system attains higher secure information integrating the cryptography mechanism and the access-control protocols within the system[7]. Another study, BSPP-block-chain based secure-privacy-preserving PHI-sharing mechanism is implemented for diagnosis enhancement in E-health care-systems. Further to this, the block-generators are necessary to bring out the conformance proof, for blocks addition in block-chain based network. The access of the data and the utilization of that heal-care data were been located central in cloud-computing platform. In this block-chain based network, node is processed and it is acted as the proxy-server. This processing-node does the data re-encryption process. This encryption and decryption of data within block-chain network ensures in preserving from collision-attacks and checking out data-confidentiality[8]. The data is partitioned, storage of one-part block-chain and another part storage in cloud-server. This implementation yield out the fine grained data access-control. This block-chain network recognizes the cloud-non repudiations, self-certification, smart-contracts usage and in accessing the policies of the users. An efficient scheme is proposed for handling this type of dynamic-network and complex larger scale systems. The policy-hiding scheme is employed[9], for in consideration of sensitive information in access-policies. The approach also assists in the data-revocation in vehicles, where the vehicles is no longer require for sharing the VSN-data. Hence through this study, simulation inferences and the security-analysis is depicted efficiently.

Similarly, to provide a better approach for the aforementioned issues of security and robust health-care data maintenance, SRHB-Secure and Robust-Healthcare-based block-chain network is implemented with attribute basis encryption for transmitting the health-care information securely. This proposed-framework gathers the information from patient, through wearable devices in block-chain based centralised system for every records of patients. In this type of approach, every entry is created as a new-block and as block-chain. The modification in block, is created as new-entry in the chain[10]. The experimental analysis of the study, shows that SRHB-framework minimizes SET-system-execution time and AD-Average-delay time and also enhances the success-rate of the secure data manipulation in block-chain network by 28 percentage in comparison with the other conventional-methods. The significance of clinical intelligence obtained from data-analytics source is vital in taking out the decisions in organisation and in developing the preventive-steps for insecurity. The block-chain network is a promising technique for providing data-security in decentralized and distributed environment[11]. Hence a dynamic-consent architecture which leverages block-chain network with usage of smart-contracts is implemented in cloud-computing environment.

Likewise, another approach of employing Block-chain bases privacy-preserving and secured HER-electronic-health records sharing protocol is applied in this cloud-server. The requester of data traverses the search through the specified keywords from the relevant service-provider. The corresponding HER upon ENHR-consortium is fetched. The owners of the data is authorized by getting the re-encryption technique of cipher-text obtained from the cloud-server[12] . This method is majorly utilizes the conditional proxy-re-encryption technique also with searchable encryption-technique as well for recognizing the security and in granting the access-policies.

Some of the centralised SDN-software-defined network, faces few challenges such as single-point of malicious attacks (DDoS) in IoT environment and majorly concerns with the data-leakage issues. For resolving this issue, PRE-block chain based proxy-re-encryption techniques has been utilized for handling this complications[13]. In this block-chain network, the devices were all authorized for enhancing in their authenticity and in credibility. The smart-contracts series were modelled for flexible search operations and in records updating process upon the block-chain network. Hence these implementation of block-chain based secured transmission of EHR data within cloud computing guarantees the availability of the system and met with the goals of security mechanism in E-healthcare systems.

Similarly, DIT-Block-chain based decentralised Interoperable-Trust framework is implemented on IoT-zones. The presence of smart-contracts supports ITIS-indirect trust-inference system and in budgets authentication. This methodology minimizes the semantic-gaps and improvises the TF-Trustworthy-factor prediction through node edges and network-nodes. This DIT-implementation in IoHT networks, utilizes block-chain ripple-chain for exploring the trustful communication through nodes validation on the basis of structure interoperability. This controlled-communication is necessary for solving integration problems and fusion issues in several IoHT zones. The implementation utilizing Ripple-block chain and Ethereum, depicted as models for relating the aggregated-requests upon the trusted-zones.

The major-contribution of the paper has been stated as follows:

- To implement the secure based data manipulation of patient health-records in cloud-based systems, through AES-algorithm.
- To implement the efficient validation of the data request, in cloud server.
- To ensure the data-integrity and intrusion free cloud- based systems, thus preventing the data-leakage within cloud environment.

3. Proposed-Frameworks:

The proposed-framework comprises of efficient and secure of data transformation within the cloud systems using Block-chain approach. This method, enables the data manipulation with in the cloud systems, through encryption and decryption techniques. The Keys are generated in the upload task from health-care provider A, in uploading the records of the patients and also it is generated in the downloading process from the cloud-server. The Patient Records are maintained in the cloud-server. Validation of the user is also carried in the server , by using block-chain approach.

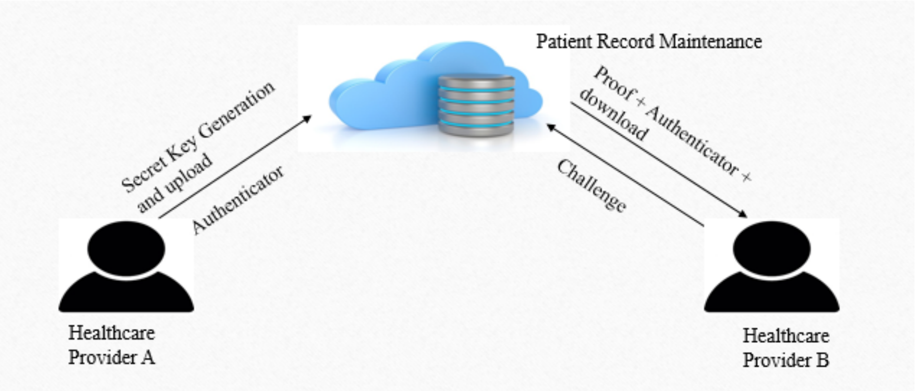

Patient Record Maintenance
Secret Key Generation and upload
Authenticator
Proof + Authenticator + download
Challenge
Healthcare Provider A
Healthcare Provider B

Figure 1. Overall Architecture flow

The proposed-framework involves the efficient and secure health-care data manipulation between the health-care providers within the cloud-system in E-health-care systems. The above figure 1 depicted the overall architectural flow of the proposed-framework.The patient records were loaded after the login process. After the login process, the key is generated for every records in data. The key is evolved in encryption of the data. The records after the encryption, the participant creates an upload request which has to be transmitted. If the login authentication failed, the registration of the user is performed. The patient records can also be downloaded after the login process. The same step wherein the download requisition is also created and then the same key (denoting the encrypted key) is decrypted for the download process. After the upload requests are received, blocks were created of those transaction data. These blocks were all integrated as block-chains.

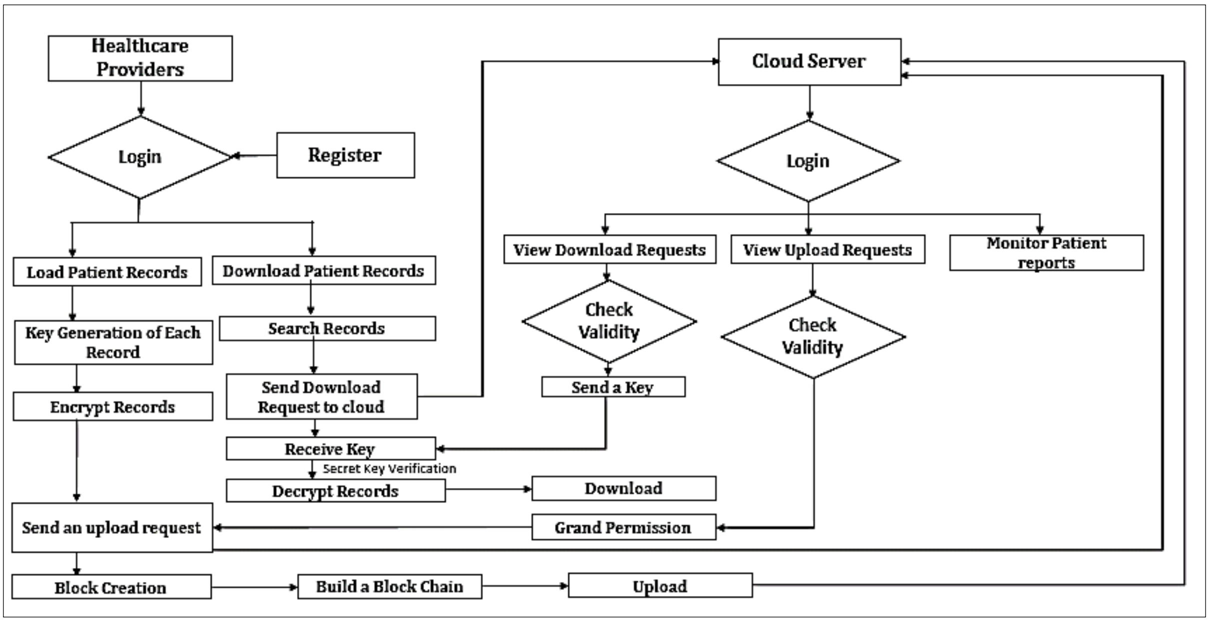


Figure 2. Flow Diagram of proposed-framework

The above figure 2 illustrates the data flow of the proposed-framework model. The decrypted request after the decryption process is moved on to the cloud-server. The cloud-server requires the login of the participant. This login process enables the user to enter into the block-chain based cloud system, handling the EHRS records for data manipulation. After the login process, the user (health-care provider) can involve in monitoring the patient-reports, viewing all the upload-requests, and viewing all the download-requests. In each process of viewing and monitoring the data-requests, validity of the Participants is ensured in each step. The validation of the user is followed by sending the key, to the corresponding request and performing the relevant decryption process for obtaining the desired outcomes. This key-generation is implemented by AES-Advanced-Encryption algorithm.

3.1. Encryption Process using AES-Advanced-Encryption Algorithm:

Table 1 : AES-Algorithm

```
Input_Feed  : hybrid Binary-Pattern ,
Output Result : Chaotic-Hybrid Binary-pattern

Start Process
For p=0 to length (Hybrid Binary-pattern)
m (p+1)= m(p) + R * sin ((p))
(p+1) = (p) + m(p+1)
End for
Chaotic-Indices = int()
Chaotic-Indices = Chaotic-Indices% length (Hybrid Binary-pattern)
Chaotic-Hybrid Binary-pattern = Hybrid Binary-pattern
For p=0 to length(Hybrid Binary-pattern)
idn × 1 = p
idn × 2 = Chaotic-Indices (p)
swap(Chaotic-Hybrid Binary-pattern(idn × 1), Chaotic-Hybrid Binary-pattern(idn × 2))
end for process
end
```

3.2. AES-Encryption Technique:

The more Significant block-cipher chosen-algorithm for encryption is AES-Advanced Encryption-algorithm, which is a asymmetric Key-encryption standardized algorithm, utilized for data security. The AES encrypts the long plain-texts with higher-efficiency. This AES-algorithm assists the block of data comprising of 128-bits in varying sizes of 192-bits, 256-bits and 128 bits. The algorithm attains the consistent speed in hardware and software implementation. This algorithm is applied in several platform, specifically in small-devices. The above table describes the algorithm implemented in the study. For enhancing the data encryption efficiency, through AES, the process ought to be employed with varying key-sizes of 192-bits in 12 iteration rounds. Block-chain approaches, is employed in these cloud-computing environment, consisting of crypto currency-contracts, smart-properties, and intellectual rights between the other parties.

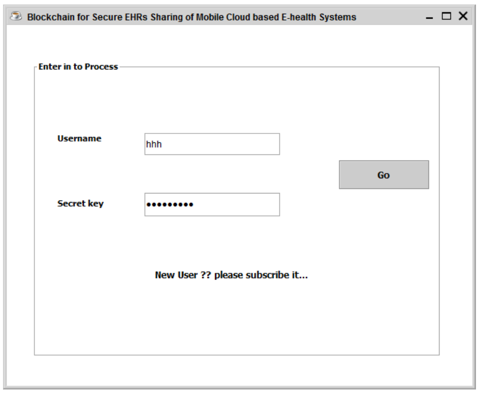
Hence as the result, the block-chain technique is implemented for ensuring the integrity and credibility in data verification systems. This clock-chain system, a technical mechanism for achieving the secure level of transmission and also neglects the centralised-authentication. This will further overcomes the failure complication occurring in all network-nodes. In this methodology, the encryption process is followed by modelling the upload requisition of the user to blocks. Many such blocks has been integrated as full block-chain. This block chain with separate-blocks comprises of all the data of every transaction, in a definite interval of time. These chain of blocks has been linked altogether in a chronological manner. Each and every block consists of hash functions of the previous data-block.

The symmetric encryption algorithm utilizes the same key for decryption and encryption process, which is shared commonly by the communicating participants. The data sending participants uses the secret secured key for encryption process and on the other side, the receiving participants utilizes the same generated key for decryption process.

4. Results and Discussion:

The proposed-framework utilizes the data records sourced from EHRS-data set. This EHRS data-set consists of Patient records. On the basis of block chain network settings, smart-contracts is deployed along with encryption and decryption process, for the efficient data manipulation of Electronic health-records of the patients. This is implemented with mobile-applications in constructing the e-healthcare systems. With this EHR-sharing systems, the proposed-framework is evaluated for efficiency assessment, with these settings through the network-overheads and access-controls.

Process entry


Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems
Enter in to Process
Go

Username: hhh

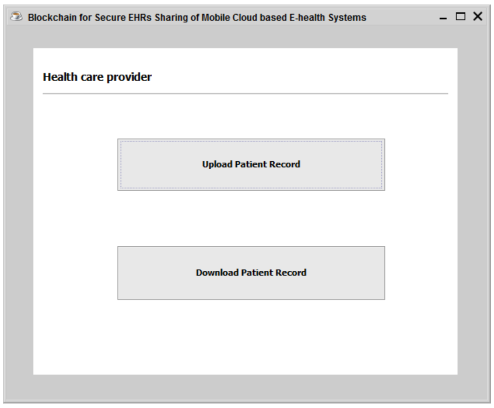
Secret key: •••••••••

New User ?? please subscribe it...

Figure 3. Process-entry

This figure 3 illustrates the homepage of the user interface. The data is inputted in the text box.

Healthcare Provider:



Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems

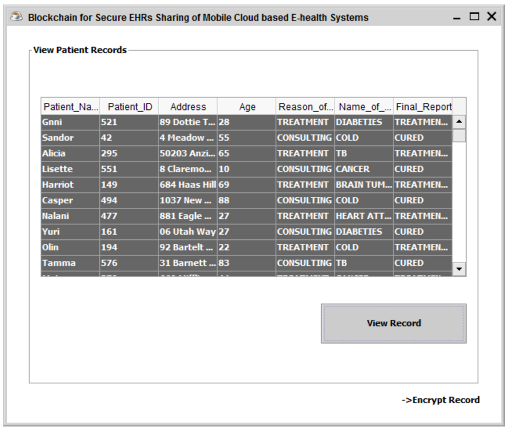
Health care provider

Figure 4: Interface of the user

The above Figure 4 enumerates the interface details of the user. The health-care provider, can perform the upload task of the patient records and also in downloading the patient records.

Upload Patient Records

View Records



Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems

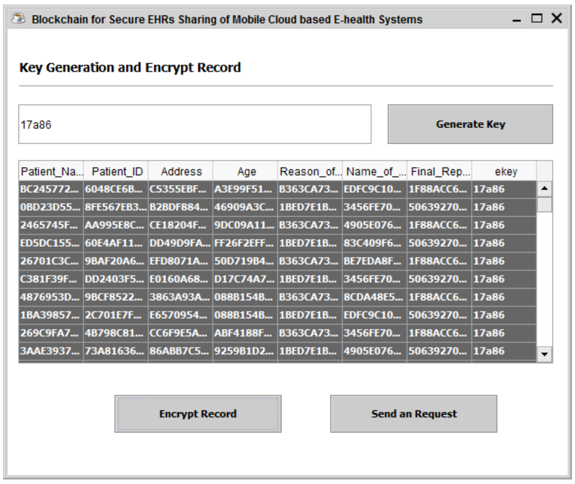
View Patient Records

Patient_Na...	Patient_ID	Address	Age	Reason_of...	Name_of_...	Final_Report
Gnni	521	89 Dottie T...	28	TREATMENT	DIABETIES	TREATMEN...
Sandor	42	4 Meadow ...	55	CONSULTING	COLD	CURED
Alicia	295	50203 Anzi...	65	TREATMENT	TB	TREATMEN...
Lisette	551	8 Claremo...	10	CONSULTING	CANCER	CURED
Harriot	149	684 Haas Hill	69	TREATMENT	BRAIN TUM...	TREATMEN...
Casper	494	1037 New ...	88	CONSULTING	COLD	CURED
Nalani	477	881 Eagle ...	27	TREATMENT	HEART ATT...	TREATMEN...
Yuri	161	06 Utah Way	27	CONSULTING	DIABETIES	CURED
Olin	194	92 Bartelt ...	22	TREATMENT	COLD	TREATMEN...
Tamma	576	31 Barnett ...	83	CONSULTING	TB	CURED

Fig 5. Records view

The above figure 5 describes the entire records view within the cloud systems. After the key generation, the records can be viewed through this interface. The records has been retrieved from the cloud-server.

Key Generation and Record Encryption



Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems

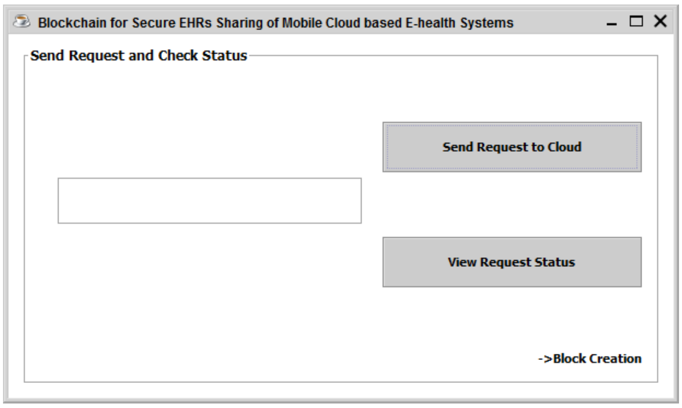
Key Generation and Encrypt Record

17a86

Patient_Na...	Patient_ID	Address	Age	Reason_of...	Name_of_...	Final_Rep...	ekey
BC245772...	6048CE6B...	C5355EBF...	A3E99F51...	B363CA73...	EDFC9C10...	1F88ACC6...	17a86
0BD23D55...	8FE567EB3...	B2BDF884...	46909A3C...	1BED7E1B...	3456FE70...	50639270...	17a86
2465745F...	AA995E8C...	CE18204F...	9DC09A11...	B363CA73...	4905E076...	1F88ACC6...	17a86
ED5DC155...	60E4AF11...	DD49D9FA...	FF26F2EFF...	1BED7E1B...	83C409F6...	50639270...	17a86
26701C3C...	9BAF20A6...	EFD8071A...	50D719B4...	B363CA73...	BE7EDA8F...	1F88ACC6...	17a86
C381F39F...	DD2403F5...	E0160A68...	D17C74A7...	1BED7E1B...	3456FE70...	50639270...	17a86
4876953D...	9BCF8522...	3863A93A...	088B154B...	B363CA73...	8CDA48E5...	1F88ACC6...	17a86
1BA39857...	2C701E7F...	E6570954...	088B154B...	1BED7E1B...	EDFC9C10...	50639270...	17a86
269C9FA7...	4B798C81...	CC6F9E5A...	ABF4188F...	B363CA73...	3456FE70...	1F88ACC6...	17a86
3AAE3937...	73A81636...	86ABB7C5...	9259B1D2...	1BED7E1B...	4905E076...	50639270...	17a86

Figure 6. Key-generation and encryption of record

The figure 6 depicted the process of key generation and the finalised tables showing the encrypted records , along with the encrypted keys in the table.



Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems

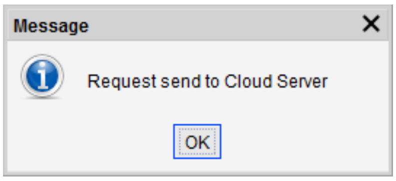
Send Request and Check Status

Fig 7. States of data request

Send a request to cloud server

The above figure 7 , shows the two processes that the health-care providers , given the options to perform in data-manipulation within the cloud-system.

For the uploading task, the participant ought to send the requsition to the cloud server. Hence after the validation, the request can be uploaded to the server. This also includes the decryption of the key.



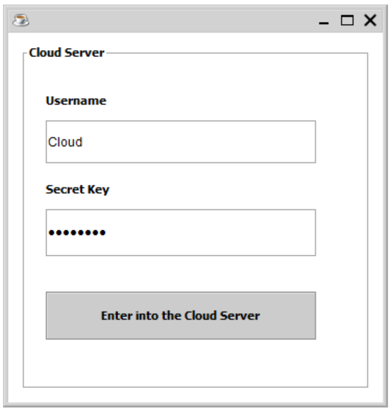
Message

Request send to Cloud Server

Fig 8. Message prompt

The above figure 8 depicted the acknowledgment to the user about the sent successful message

Cloud-server page:



Cloud Server

Username

Cloud

Secret Key

••••••••

Fig 9 : Cloud-server page :

The above figure 9, illustrates the home page, which yields out the option to enter to the cloud-server.

Cloud Server Process:

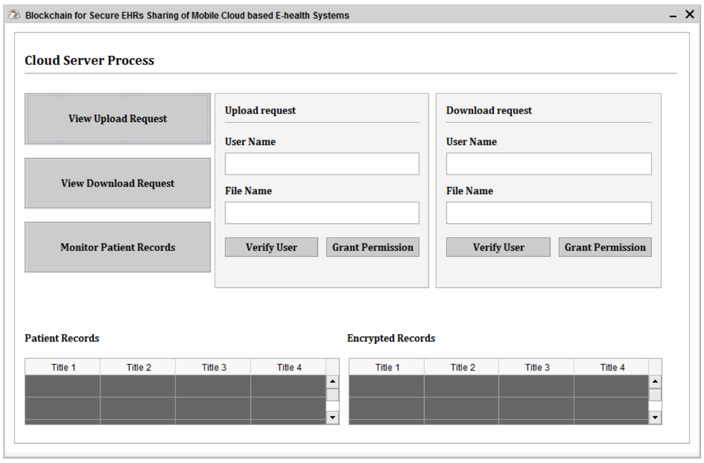
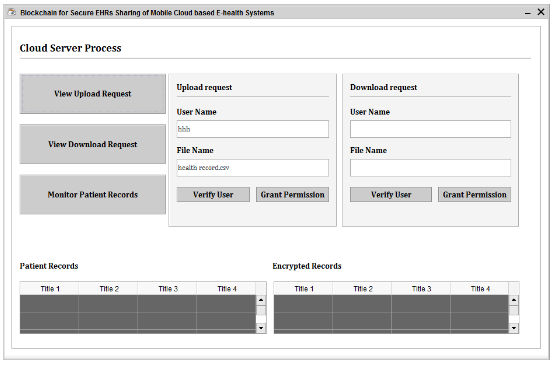


Fig 10: Cloud Server Process

The above figure 10, depicted the cloud-server options, while the user requests for viewing the upload requests, download-request and in monitoring process.

View Upload Request



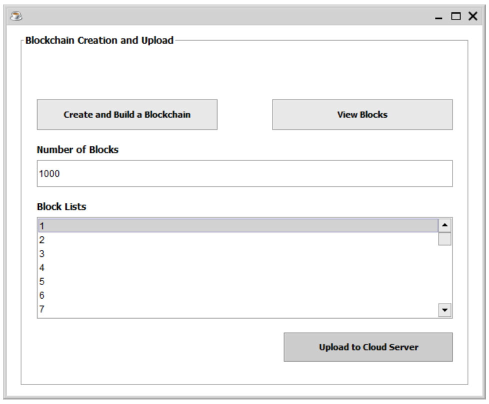
User Name: hhh

File Name: health record.csv

Fig 11. View Upload Request

The above figure 11 showed the upload request screen, where the user name and relevant file name has been given as inputs.

Block Creation

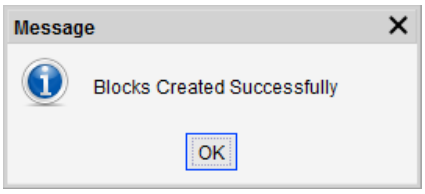


Number of Blocks: 1000

Block Lists
1
2
3
4
5
6
7

Fig 12. Block Creation

The specified number of the data-transactions has been merged to block-chains . The above figure 12 shows the block-creation input page and the blocks can be viewed in the same page.

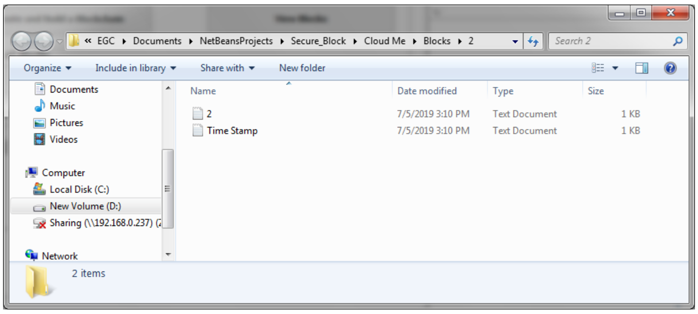


Blocks Created Successfully

Fig 13. Successful acknowledgment

The figure 13 depicted the successful page of the acknowledgement.

View Blocks



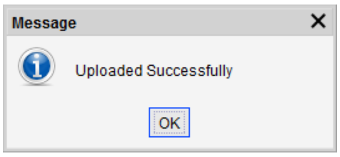
Name	Date modified	Type	Size
2	7/5/2019 3:10 PM	Text Document	1 KB
Time Stamp	7/5/2019 3:10 PM	Text Document	1 KB

2 items

Fig 14. View Blocks

The above figure 14 illustrates the viewing of the blocks which has been combined .

Upload Acknowledgement



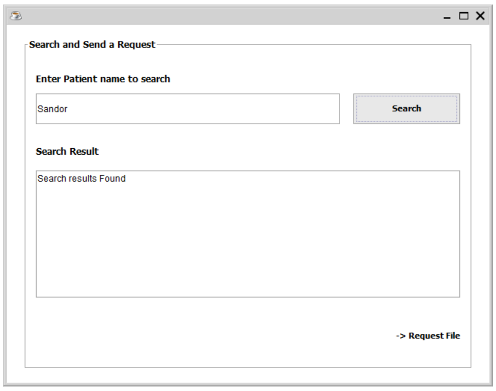
Uploaded Successfully

Fig 15 Upload Acknowledgement

The figure 15 denotes the upload acknowledgement of the server in cloud-computing.

Healthcare Provider: Download Page

Search:



Search and Send a Request

Enter Patient name to search: Sandor

Search Result: Search results Found

Figure 16 . Healthcare Provider: search Page

The figure 16 implies the searching mechanism of patient records in respective to the search keyword.

Request a key to download:

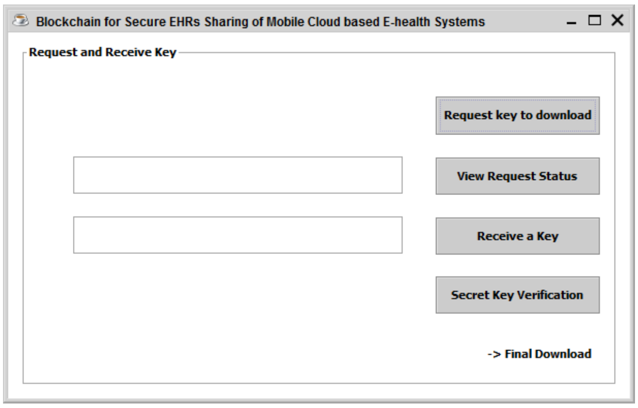
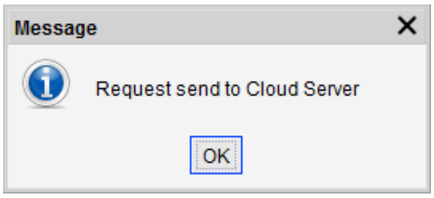


Fig 17 Key requisition

Once any requisition is moved to the cloud-server, the key is necessary for the decryption process. The key is manipulated by receiving or the verification process is carried out in the above figure

Request status:

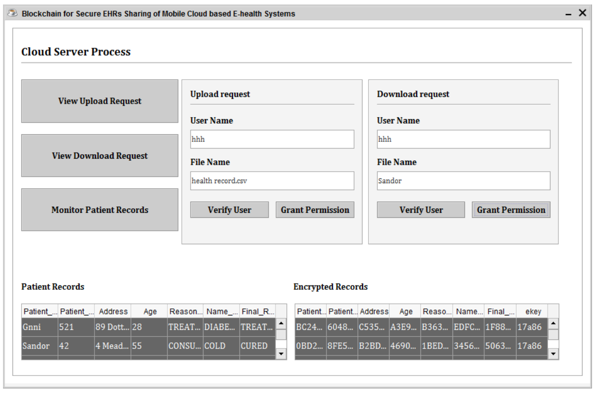


Request send to Cloud Server

Fig 18 Request status

The figure 18 depicted the successful message acknowledgement from the cloud-server.

Cloud Sever: View Download Request



Upload request

User Name: hhh

File Name: health record.csv

Download request

User Name: hhh

File Name: Sandor

Patient Records

Patient_...	Patient_...	Address	Age	Reason...	Name_...	Final_R...
Gnni	521	89 Dott...	28	TREAT...	DIABE...	TREAT...
Sandor	42	4 Mead...	55	CONSU...	COLD	CURED

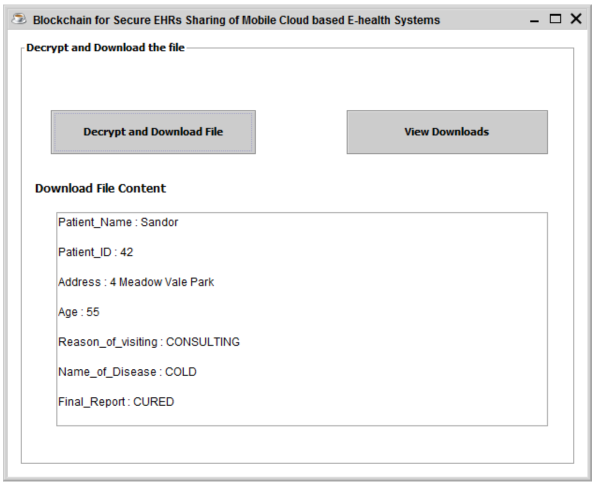
Encrypted Records

Patient...	Patient...	Address	Age	Reaso...	Name...	Final_...	ekey
BC24...	6048...	C535...	A3E9...	B363...	EDFC...	1F88...	17a86
0BD2...	8FE5...	B2BD...	4690...	1BED...	3456...	5063...	17a86

Fig 19 Download Request

The above figure 19 depicts the various requisition process of the users in cloud -server

Decrypt and Download the file


Blockchain for Secure EHRs Sharing of Mobile Cloud based E-health Systems
Decrypt and Download the file
Decrypt and Download File
View Downloads

Download File Content

Patient_Name : Sandor

Patient_ID : 42

Address : 4 Meadow Vale Park

Age : 55

Reason_of_visiting : CONSULTING

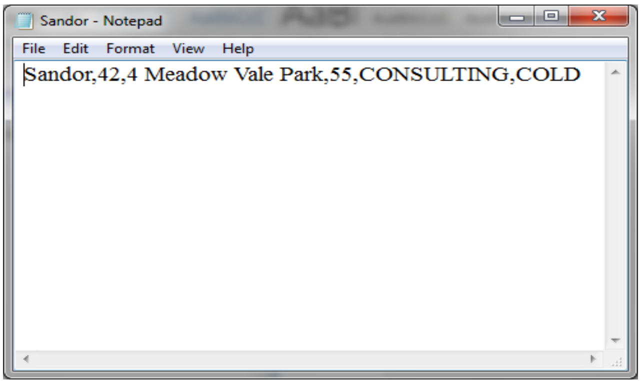
Name_of_Disease : COLD

Final_Report : CURED

Fig 20 . Decryption

The above figure describes the decryption process of the data requested. The downloads can also viewed in the interface.

View Downloads

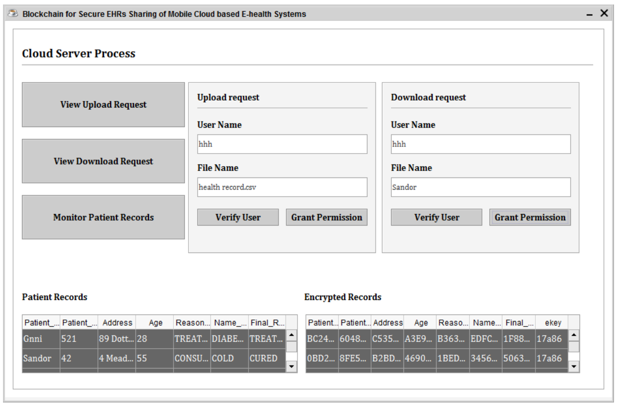


```
Sandor,42,4 Meadow Vale Park,55,CONSULTING,COLD
```

Figure 21. Download view

The above figure 21 describes the downloaded records of the outcomes

Cloud Server Record Maintenance



Upload request

User Name: hhh

File Name: health record.csv

Download request

User Name: hhh

File Name: Sandor

Patient Records

Patient_...	Patient_...	Address	Age	Reason...	Name_...	Final_R...
Gnni	521	89 Dott...	28	TREAT...	DIABE...	TREAT...
Sandor	42	4 Mead...	55	CONSU...	COLD	CURED

Encrypted Records

Patient...	Patient...	Address	Age	Reaso...	Name...	Final_...	ekey
BC24...	6048...	C535...	A3E9...	B363...	EDFC...	1F88...	17a86
0BD2...	8FE5...	B2BD...	4690...	1BED...	3456...	5063...	17a86

Figure 22. Cloud Server Record Maintenance Interface

The above figure 22 enumerates the cloud-server mechanism, depicting that the participants for viewing the upload request, downloading requests and monitoring process through block chain framework model in cloud-computing environment. The patient records has been displayed in the outcomes.

5. Conclusion:

This paper employs the novel EHR-sharing and secure framework model enabled in mobile computing, in block-chain approach. In this model, the present HER-sharing models complications has been rectified through this AES-algorithm. In this framework model, the trustworthy access-control model has been designed on the basis of smart-contract mechanism. This framework model facilitates the participants of health-care system or the health-care providers for efficient and secure access of the electronic-health records in this health-care system. This framework model addresses the reliability of the data-sharing within the network, consistency and also majorly prevents the data-leakage between the nodes. This is attained by key-generation techniques employed by AES algorithm. The model has been depicted as peer-peer storage system with block-chain network for acquiring efficient and faster data access from the cloud-server.

References:

[1] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," *Computers & Security,* vol. 88, p. 101653, 2020.

[2] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1-6.

[3] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *Ieee Access,* vol. 6, pp. 38437-38450, 2018.

[4] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. Tavares, and V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cognitive Systems Research,* vol. 52, pp. 1-11, 2018.

[5] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, "Design of a secure medical data sharing scheme based on blockchain," *Journal of medical systems,* vol. 44, pp. 1-11, 2020.

[6] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," *Journal of medical systems,* vol. 42, pp. 1-11, 2018.

[7] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of medical systems,* vol. 42, pp. 1-18, 2018.

[8] K. O.-B. Obour Agyekum, Q. Xia, E. B. Sifah, J. Gao, H. Xia, X. Du*, et al.*, "A secured proxy-based data sharing module in IoT environments using blockchain," *Sensors,* vol. 19, p. 1235, 2019.

[9] K. Fan, Q. Pan, K. Zhang, Y. Bai, S. Sun, H. Li*, et al.*, "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," *IEEE Transactions on Vehicular Technology,* vol. 69, pp. 5826-5835, 2020.

[10] A. Mubarakali, "Healthcare services monitoring in cloud using secure and robust healthcare-based BLOCKCHAIN (SRHB) approach," *Mobile Networks and Applications,* vol. 25, pp. 1330-1337, 2020.

[11] T. Rupasinghe, F. Burstein, and C. Rudolph, "Blockchain based Dynamic Patient Consent: A Privacy-Preserving Data Acquisition Architecture for Clinical Data Analytics," in *ICIS*, 2019.

[12] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain," *IEEE Access,* vol. 7, pp. 136704-136719, 2019.

[13] Y. Gao, Y. Chen, H. Lin, and J. J. Rodrigues, "Blockchain based secure IoT data sharing framework for SDN-enabled smart communities," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2020, pp. 514-519.