May - June 2020
ISSN: 0193-4120 Page No. 3340-3344

Secure the Big Data of Patient Health Care using IOT Sensor

[1]Badi Alekhya, [2]Menaka. S, [3]R.Sasi Kumar

[1]Research scholar, [2]Assistant Professor, [3]Professor,
[1]Department of ICE, [2,3]Department of Computer science and Engineering,
[1,3]R.M.D Engineering College, Kavaraipettai,
[2]Saveetha School of Engineering, Saveetha Institute of Medical and Technical Science, India
[1]alekhyareddy1@gmail.com, [2]menakas311@gmail.com, [3]rsn.cse@rmd.ac.in

Article Info
Volume 83
Page Number: 3340-3344
Publication Issue:
May - June 2020

Article History
***Article Received:** 19 August 2019*
***Revised:** 27 November 2019*
***Accepted:** 29 January 2020*
***Publication:** 12 May 2020*

Abstract

Internet of Things consist of extending the internet connectivity isolated standard devices of digital gadgets such as smartphones, tablets and laptops, to wide range of traditionally dumb or non-internet-enabled of physical devices on everyday objects. With users shattering and stand in line up for the upcoming big thing, who identify that the setting is persistently updating, and recognise their responsibility preserve up. Entrenched with technology of devices can lead into over the internet, and they can be monitored and controlled. Despite of keep information safe has familiar with vulnerability assessment, ethical hacking, public key infrastructure (PKI) security, and wireless network security will be key performers. Most of the IOT devices will be perform through digital devices and smartphones. External hardware and sensors are involves to develop apps that can communicate even more.

Keywords: *Diffie-Hellman, AES, Cloud Service Provider, Encryption, Decryption, Health care, Data owner.*

1. Introduction

In healthcare applications, IOT sensors / devices are involved to store the patient health record. Integrity of data to provide the secure information about the health care of each and every sensors in IOT network in the field of Healthcare. Safety of data is more trust on data collection affected by cyber threats /attacks. Patient's Healthcare is affected on privacy sensitive data. Conventional solutions often offer security to patient's health monitoring information all through the communique. Cloud computing gives a possibility for people and businesses to offload to effective servers the burden of handling huge quantities of records and performing computationally annoying operations. Because of the growing recognition of cloud computing, increasingly more facts proprietors are prompted to outsource their facts to cloud servers for amazing convenience and reduced value in information control. Data proprietors provide offerings to a huge wide variety of corporations and companies, they keep on with excessive protection standards to enhance information security through following a layered approach that includes facts encryption, key management, sturdy get right of entry to controls, and security intelligence. The cloud server executes the query and returns the encrypted documents with a further evidence consistent with the token generated by way of data owners. The statistics users will acquire the result with the corresponding evidence in order to verify the correctness and decrypt encrypted documents after the verification is correct.

2. Literature Review

[1] Smart sensors are small wireless computing gadgets that feel records consisting of mild and humidity at extremely high resolutions. A smart sensor query-processing structure the use of database generation can facilitate deployment of sensor networks.

[2] It organizes the sensor nodes into clusters with the aid of dividing the sensor discipline and allows sensor nodes to transmit records to the Cluster Head (CH), that's liable for records transmission closer to the sink. Numerous clustering routing protocols are proposed with a view to maximize the network lifetime the usage of a

static sink, however the conventional static sink has some obstacles.

[3] An access to control framework supported by using identity-primarily based encryption for a at ease cellular-PHR gadget. Consequences from our prototype assessment (laboratory and discipline studies) imply that the proposed IBE scheme correctly secures PHRs past the healthcare provider's safety domain and is efficient overall performance-smart.

Yin Zhang, Meikang Qiu, Chun-Wei Tsai, Mohammad Mehedi Hassan, and Atif Alamri, 2017. “Health-CPS: Healthcare cyber-physical system assisted by cloud and big data”. To provide a more convenient service and environment of healthcare, this paper proposes a cyber-physical system for patient-centric healthcare applications and services, called Health-CPS, built on cloud and big data analytics technologies. This system consists of a data collection layer with a unified standard, a data management layer for distributed storage and parallel computing, and a data-oriented service layer. The results of this study show that the technologies of cloud and big data can be used to enhance the performance of the healthcare system so that humans can then enjoy various smart healthcare applications and services.

Stojmenovic and W. Sheng, 2014. “The fog computing paradigm: situations and safety problems”. Fog computing is a paradigm that extends cloud computing and offerings to the edge of the network. Fog computing affords information, storage, and application offerings to give up customers. In Fog computing consumer information is outsourced and user’s control over dated is surpassed over to fog node, which introduces same protection threats as it's far in cloud computing. Fog computing is properly acceptable for actual time analytics and big data.

Y. Cao, S. Chen, P. Hou and D. Brown, 2015. “FAST: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation”. Fog computing is a these days proposed computing paradigm that extends Cloud computing and services to the edge of the network. The brand new functions presented by means of fog computing (e.g., distributed analytics and area intelligence), if successfully applied for pervasive health monitoring programs, has wonderful ability to accelerate the discovery of early predictors and novel biomarkers to support clever care choice making in a related health scenarios.

[3] A novel dynamic switching-based dependable flooding (DSRF) framework that is designed as an enhancement layer to provide efficient and dependable transport for an expansion of current flooding tree systems in low-obligation-cycle WSNs. The key novelty of DSRF lies within the dynamic switching decision making when encountering a transmission failure, where a flooding tree structure is dynamically adjusted based totally at the packet reception results for strength saving and postpone reduction.

3. Existing System

Healthcare concerns were involved secure each sensor/tool in the IOT network with the integrity of its information. Even though the safety and luxury of patients’ normal fitness relies on this data series, the safety of the statistics is significantly laid low with cyber threats/attacks. Further, patient’s privateer’s sensitive statistics also can be affected.

4. Proposed System

To conquer the safety problem here we define the secret sharing approach and numerous types of encryption algorithm. Then here we're using IOT to get the records from the data proprietor. Even though many current work provide security to affected person’s records privacy over communication, they'll now not protect the facts once a cloud server is negotiated, specifically while a cloud server is under attacks by means of the insider or cloud company. The IOT paradigm nevertheless requires efficient solutions to defend patient facts towards cyber threats/attacks at some point of the manner from the IOT sensors in the direction of the healthcare issuer.

5. Preliminaries

Data Owner and Data User Login

The overall patient records is maintained by the data owner. User can login with their username and password if it is valid, it will be redirected to another form. The data owner will manage all the patient details. The user can login with their username and password if it is a new user, the user have to be registered before login. Then the data user will search a record to download. After getting an approval from server, the data user will download the records.

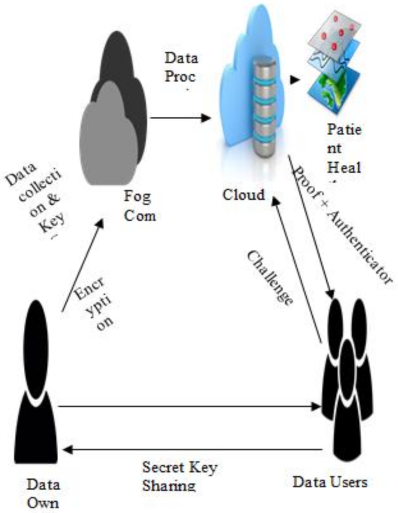


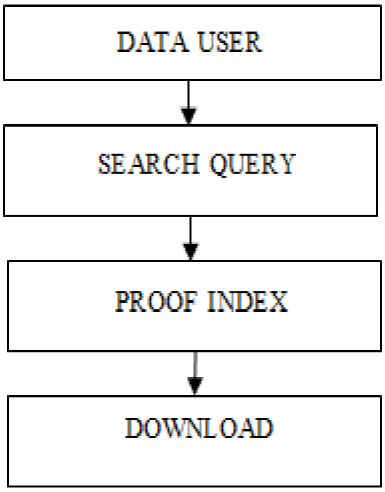
Figure 1: Data uploading

Data Selection and Loading

Data selection is a process of selecting appropriate dataset for processing. In which contains all the information about the patient healthcare records. The healthcare records are selected for securely maintaining all the patient details.

Key Generations

Key generation is the technique of producing keys in cryptography. A secret Key is used to encrypt and decrypt whatever information is being encrypted/decrypted. The Diffie-Hellman set of rules is used for generating a key for encrypting the patient healthcare data.



Data Encryption and Upload

Encryption is the most effective way to attain records safety. To examine an encrypted document, the records consumer should have access to a secret key that enables us to decrypt it. Unencrypted information is called plain text; encrypted information is called cipher text. The AES algorithm is used for encrypting the data. Finally the encrypted data's are uploaded into the cloud server for comfortable protection.

Cloud Service Provider

The Cloud provider can view all of the uploaded and downloaded files within the Cloud. The CSP gets the document request from the records person, verifies the authentication before granting permission. Then the CSP executes the query and returns the encrypted file in line with the quest token. And also returns an extra evidence with the report, to verify the search end result.

Public Verification Key

Public verification key is a safety measure designed to ensure that your document outsourced in cloud doesn't get hacked. By means of verifying public key, the facts proprietor and the records consumer including some other layer of safety to the documents or documents in the cloud by using confirming every different identities.

Data User

User send a request to the cloud server. After request granted from the Cloud, the data user receiving the public Verification Key from the Cloud generated via information proprietor. The facts user now decrypt and download the encrypted files, after verifying with the public Verification Key. After receiving a verification from cloud, the data person will down load the record within a selected time restriction.

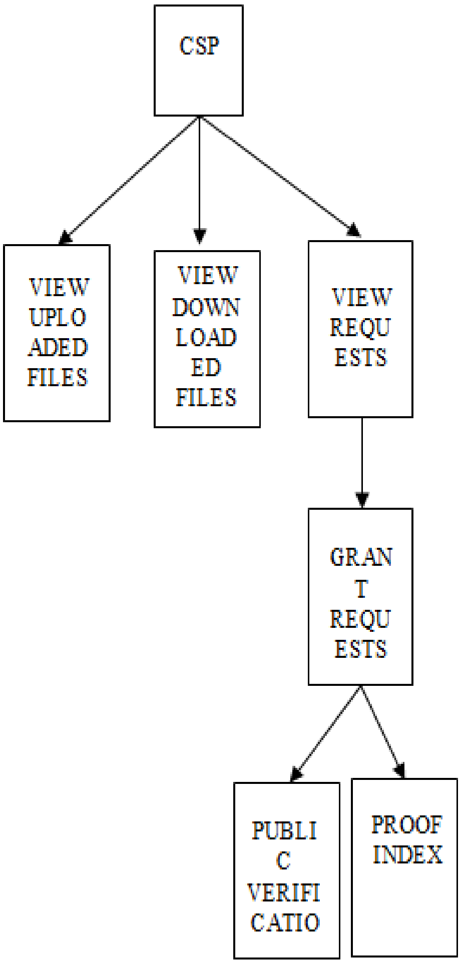


Figure 2: Architecture Diagram

Verification with Proof Index

It is evidence generating device for verifying cloud search via Public Verification Key, here the information customers or others can confirm the correctness of the search end result by Verification key.

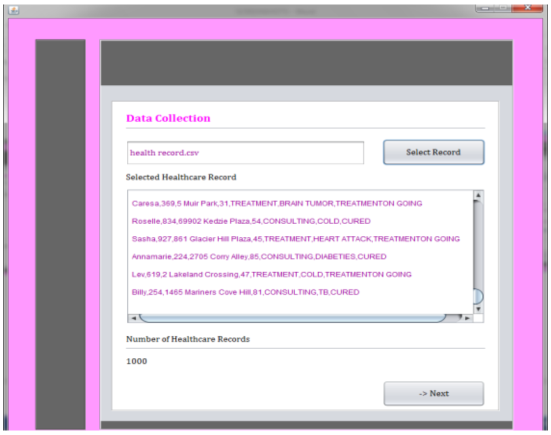
Decryption

The conversion of encrypted information into its original form is called Decryption. It is usually a reverse technique of encryption. It decodes the encrypted records so that a licensed user can most effective decrypt the information due to the fact decryption requires a secret key.

Download Patient Records

After the successful verification of secret key, the data user will download the patient healthcare records. Finally all the records are securely decrypted and send to the user.

6. Result and Discussion



Data Collection

health record.csv

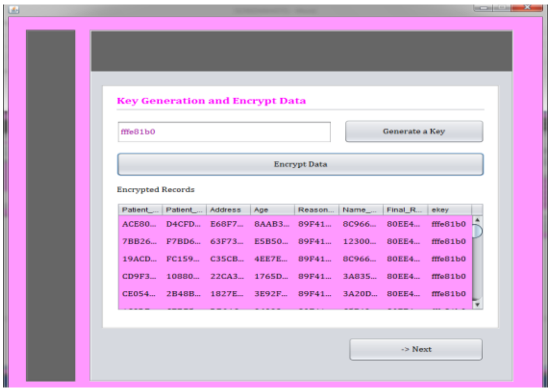
Selected Healthcare Record

```
Caresa,369,5 Muir Park,31,TREATMENT,BRAIN TUMOR,TREATMENTON GOING
Roselle,834,69902 Kedzie Plaza,54,CONSULTING,COLD,CURED
Sasha,927,861 Glacier Hill Plaza,45,TREATMENT,HEART ATTACK,TREATMENTON GOING
Annamarie,224,2705 Corry Alley,85,CONSULTING,DIABETIES,CURED
Lev,619,2 Lakeland Crossing,47,TREATMENT,COLD,TREATMENTON GOING
Billy,254,1465 Mariners Cove Hill,81,CONSULTING,TB,CURED
```

Number of Healthcare Records

1000

Figure 3: Data Collection



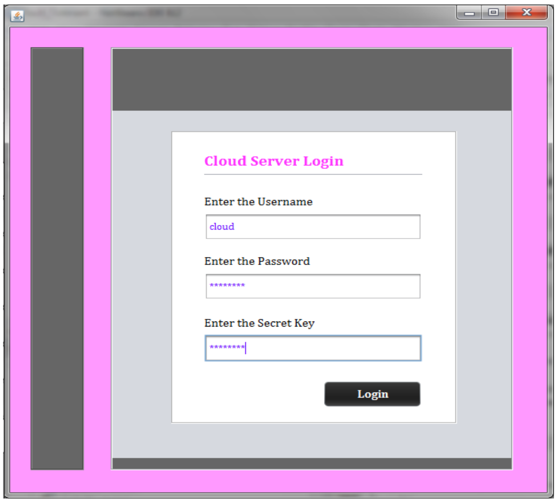
Key Generation and Encrypt Data

fffe81b0

Encrypted Records

Patient_...	Patient_...	Address	Age	Reason...	Name_...	Final_R...	ekey
ACE80...	D4CFD...	E68F7...	8AAB3...	89F41...	8C966...	80EE4...	fffe81b0
7BB26...	F7BD6...	63F73...	E5B50...	89F41...	12300...	80EE4...	fffe81b0
19ACD...	FC159...	C35CB...	4EE7E...	89F41...	8C966...	80EE4...	fffe81b0
CD9F3...	10880...	22CA3...	1765D...	89F41...	3A835...	80EE4...	fffe81b0
CE054...	2B48B...	1827E...	3E92F...	89F41...	3A20D...	80EE4...	fffe81b0

Figure 4: Encrypted Data



Cloud Server Login

Enter the Username

cloud

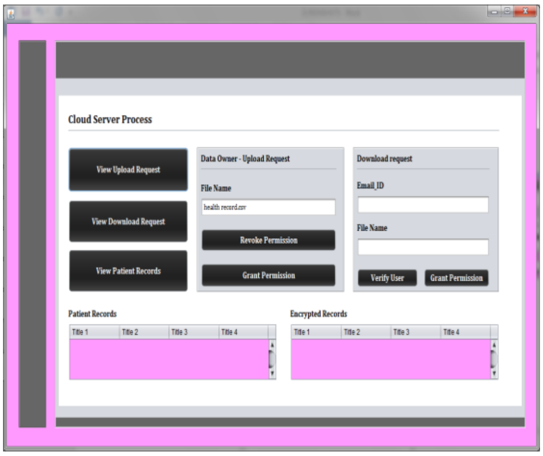
Enter the Password

****

Enter the Secret Key

****

Figure 5: Cloud Login



Cloud Server Process

Data Owner - Upload Request

File Name

health record.csv

Download request

Email_ID

File Name

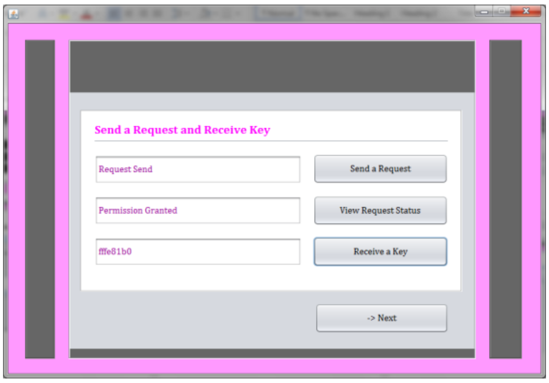
Patient Records

Title 1	Title 2	Title 3	Title 4

Encrypted Records

Title 1	Title 2	Title 3	Title 4

Figure 6: View Upload Request and Grant Permission



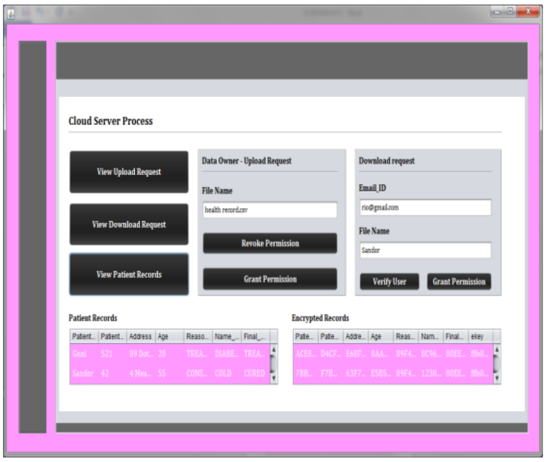
Send a Request and Receive Key

Request Send

Permission Granted

fffe81b0

Figure 7: View Request Status and Receive Key



Cloud Server Process

Data Owner - Upload Request

File Name

health record.csv

Download request

Email_ID

rio@gmail.com

File Name

Sandor

Patient Records

Patient...	Patient...	Address	Age	Reaso...	Name_...	Final_...
Gnni	521	89 Dot...	28	TREA...	DIABE...	TREA...
Sandor	42	4 Mea...	55	CONS...	COLD	CURED

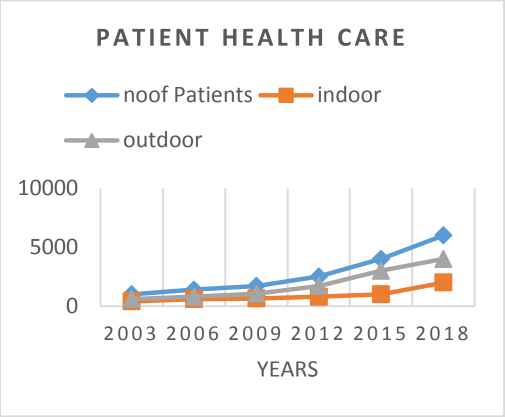
Encrypted Records

Patie...	Patie...	Addre...	Age	Reas...	Nam...	Final...	ekey
ACE8...	D4CF...	E68F...	8AA...	89F4...	8C96...	80EE...	fffe8...
7BB...	F7B...	63F7...	E5B5...	89F4...	1230...	80EE...	fffe8...

Figure 8: Cloud Server - Maintaining all the Patient Records

Graph:

This graph shows how the data has been stored in the cloud and updating the details of the patient with corresponding years(X), No.of Patients in (Y)..



7. Conclusion

It enhance the reliability and increase the performance of information transmission. Obtained records quickly to enhance processing speed. It reduces the records load transmitted to e-health clients extensively. By means of building authentication and a evidence index, it affords green seek result verification, while preventing records attacks and statistics integrity attacks.

References

[1] A. K. M. Azad, J. Kamruzzaman, B. Srinivasan, K. M. Alam, and S. Pervin, 2010 "Query Processing over Distributed Heterogeneous Sensor Networks in Future Internet: Scalable Architecture and challenges".

[2] S. K. Singh, M. P. Singh, and D. K. Singh, 2010. "A survey of energy efficient hierarchical cluster-based routing in wireless sensor networks"

[3] Kun Wang, Yun Shao, Lei Xie, Jie Wu, Song Guo. "Adaptive and Fault-Tolerant Data Processing in Healthcare IoT Based on Fog Computing", IEEE Transactions on Network Science and Engineering, 2020

[4] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE TPDS, vol. 22, no. 5, pp. 847–859.

[5] E. Stefanov, M. van Dijk, A. Juels, and A. Oprea, "Iris: A scalable cloud file system with efficient integrity checks," in Proc. of Annual Computer Security Applications Conference (ACSAC), 2012.

[6] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in Proc. of International Conference on Financial Cryptography and Data Security(FC), 2013.

[7] W. Sun, X. Liu, W. Lou, Y. T. Hou, and H. Li, "Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data," in Proc. of INFOCOM, 2015.

[8] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. of S&P, 2000.

[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, pp. 895–934, 2011.

[10] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in Proc. of CCS, 2012, pp. 965–976.

[11] Menaka. S, Rohini. S, "Secure the Data by using Image Compression in Multi-Cloud Storage," International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-9, Issue-1S2, December 2019.

[12] Menaka.S et al.." PROVIDING INTEGRITY VERIFICATION FOR DATA DYNAMICS IN CLOUD," International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST), ISSN (Online) : 2456-5717, Vol. 3, Special Issue 34, March 2017.

[13] D. Cash, J. Jaeger, S. Jarecki, C. S. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, "Dynamic searchable encryption in very-large databases: Data structures and implementation," Proc. of NDSS, 2014.

[14] R. Bost, P.-A. Fouque, and D. Pointcheval, "Verifiable dynamic symmetric searchable encryption: Optimality and forward security," Cryptology ePrint Archive: Report 2016/062, Tech. Rep., 2016.

[15] K. Kurosawa and Y. Ohtaki, "Uc-secure searchable symmetric encryption," in Proc. of International Conference on Financial Cryptography and Data Security (FC), 2012.

[16] Menaka.S, M.Naveen, T. Devi,"Data Security in Cloud Computing using Image Compression with Reversible Data Hidden", Test Engineering and Management, ISSN:0193-4120, Vol.83, March 2020.