IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008076 |

SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud Using IOT

Nikita Sunil Patil[1], Dr. D P Gaikwad[2]

Department of Computer Engineering, AISSMS College of Engineering, Pune, India

ABSTRACT: Although Personal Health Records(PHR's) are a useful and supportive source for exchange of data of patients in the healthcare arena. This is majorly achieved by storing the health information to cloud servers. This data needs to be private and secured. Cloud Servers though secured can be exposed to the possibility of being misused for disclosure or theft by hackers. Thus they need strategic schemes to ensure the security and privacy check of the PHR's. The system proposed utilizes three schemes to ensure security of PHR. The schemes are encryption of PHR, distributing PHR data over multiple clouds and giving authenticity to share PHR through secret key only. First system is designed for sharing of PHR's through secure channel of encryption wherein Lightweight algorithm is used for encryption of PHR data , the PHR is distributed over different clusters with help of DROP algorithm and data is replicated over clouds to contain any loss. Third only private key can give access to different segments of PHR's to explicit people who need to know the information. Trapdoor is generated to detect any unethical request to share PHR , request are blocked and identity of the person is pursued. The system also includes the use of IoMT(Internet of Medical Things) to capture the live data of patient through WSN(Wireless Sensor Network). IoMT contains Temperature Sensor, Pulse Rate Sensor. These sensors are embedded surface mounted on the body of a patient which continuously monitor the vital physiological parameters of the patient such as body temperature, pulse rate. The values collected from these different sensors are stored in text or pdf file as part of PHR and then shared in the cloud.

KEYWORDS: Personal Health Records (PHRs),IoMT, Cloud Server, Healthcare Services, Trapdoor, Encrytion.

I. INTRODUCTION

Cloud computing and IoMT is transforming healthcare industry by providing large scale connectivity for medical devices, patients, physicians, clinical and nursing staff who use them and facilitate real-time monitoring based on the information gathered from the connected things. The cloud computing additionally incorporates different imperative elements such storage of vast data of healthcare domain. The security and privacy constraints for IoMT cloud includes confidentiality, integrity , authentication and accountability as prime key aspect. 'Privacy', guarantees that the health data is completely covered to the unsanctioned gatherings, while 'Integrity', manages to keep up the originality of the information. 'Authenticity' ensures that the health information is accessed by an authorized entity only, whereas 'Accountability' refers to the fact that the data access policies must comply with the agreed-upon procedures. Methodology called Secure Sharing of PHRs in the Cloud is enhanced with use of Advanced encryption algorithm (AES) which gives PHR more security and also as a control component managed by patients, limiting unauthorized users. PHR's are managed by patients such that they are be allowed to upload encoded form on the cloud. These PHR's can be used by patients themselves and by other people who are authorized by patient such as doctors , friends, family, insurance agent, etc. Access to these PHR depends on the role of user of PHR who are classified according to Access Control List(ACL) provided by patient himself for instance family might be given full access to the records whereas only Mediclaim related records are shred with insurance agency. The system also includes the use of IoMT(Internet of Medical Things) to capture the live data of patient through WSN(Wireless Sensor Network).IoMT contains Temperature Sensor, Pulse Rate Sensor, Micro-controller. These sensors are embedded surface-mounted on the body of a patient which continuously monitor the vital physiological parameters of the patient such as body temperature, pulse rate. The values collected from these different sensors are stored in text or pdf file as part of PHR and then shared in the cloud.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008076 |

II. HISTORY & BACKGROUND

A. Abbas and S. U. Khan[7], This paper aimed to encompass the state-of-the-art privacy preserving approaches employed in the e-Health clouds. Automated PHRs are exposed to possible abuse and require security measures based on the identity management, access control, policy integration, and compliance management. The privacy preserving approaches are classified into cryptographic and non-cryptographic approaches and taxonomy of the approaches is also presented. Furthermore, the strengths and weaknesses of the presented approaches are reported and some open issues are highlighted. The cryptographic approaches to reduces the privacy risks by utilization of certain encryption schemes and cryptographic primitives. This includes Public key encryption, Symmetric key encryption, Alternative primitives such as Attribute based encryption, Identity based encryption, proxy-re encryption.

S. Yu, C. Wang, K. Ren, and W. Lou[14], addressed challenging open issue by, on one hand, characterizing and authorizing access policies dependent on information characteristics and then again enabling the data owner to assign a large portion of the task computation engaged with fine grained information access control to untrusted cloud servers without revealing the hidden information. It accomplished this objective by misusing and interestingly joining strategies of Attribute based encryption (ABE), proxy re-encryption, and sluggish re-encryption. This scheme likewise has notable properties of user access to benefit confidentiality and user secret key responsibility. Broad analysis demonstrates that this plan is exceptionally proficient and provably secures under existing security models.

M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang[3], gave a confirmed response to the issue by showing a general structure for secure sharing of PHRs. The presented framework empowers patients to safely store and share their PHR in the cloud server (for instance, to their careers), and moreover the treating doctors can refer the patients' medical record to specialist for research purposes, at whatever point they are required, while guaranteeing that the patients' data remain private. This framework additionally supports cross area activities (e.g., with various nations regulations).

P. V. Gorp and M. Comuzzi, present MyPHRMachines, a cloud-based PHR framework taking a profoundly new compositional answer for health record compactness. In MyPHRMachines, health related information and the application software to see and additionally analyze it are independently deployed in the PHR system. After uploading their medical information to MyPHRMachines, patients can get to them again from remote virtual machines that contain the correct software to visualize and analyze them with no requirement for transformation. Patients can share their remote virtual machine session with selected guardians, who will require just a Web browser to get to the pre-stacked sections of their long lasting PHR. There was a model of MyPHRMachines connected to two use cases, i.e., radiology picture sharing and customized medication[9].

D. Daglish and N. Archer[15], addressed design and architectural issues of PHR systems, and focused on privacy and security issues which must be addressed carefully if PHRs are to become generally acceptable to consumers.

III. DESIGN ISSUES

PROPOSED METHOLOGY

The system proposed utilizes three schemes to ensure security of PHR. The schemes are encryption of PHR, distributing PHR data over multiple clouds and giving authenticity to share PHR through secret key only. First system is designed for sharing of PHR's through secure channel of encryption wherein Lightweight algorithm is used for encryption of PHR data , the PHR is distributed over different clusters with help of DROP algorithm and data is replicated over clouds to contain any loss. Third only private key can give access to different segments of PHR's to explicit people who need to know the information. Trapdoor is generated to detect any unethical request to share PHR , request are blocked and identity of the person is pursued. The system also includes the use of IoMT(Internet of Medical Things) to capture the live data of patient through WSN(Wireless Sensor Network). IoMT contains Temperature Sensor, Pulse Rate Sensor. These sensors are embedded surface mounted on the body of a patient which continuously monitor the vital physiological parameters of the patient such as body temperature, pulse rate.

Proposed System shows an approach that grants patients to regulate the sharing of their own PHR's in the cloud. The methodology utilizes the encryption and decryption to guarantee the PHR confidentiality. The approach enables the PHR owners to specifically allow access of their PHR to users over the segments based on the access level determined in the ACL for various groups of users. KGC produces the re-encryption keys , for various groups of PHR users in this manner , eliminating the key management overhead at the PHR owners end. Formal analysis and verification of the

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008076 |

proposed approach are performed to approve its working as indicated by the determinations.

SYSTEM ARCHITECTURE

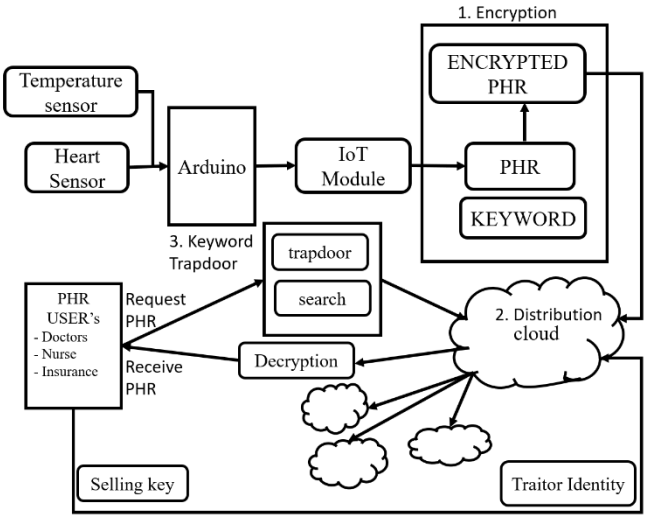

Fig.3. A System Architecture

Fig 3A. shows the architecture of proposed system for Secure Sharing of Personal Health Records in the Cloud using IoT.

MODULES

WSN(Wireless Network)

WSN includes small remote sensors that are inserted inside or surface-mounted on the body of a patient. These sensors constantly monitor the vital physiology parameters of the patient, for example, body temperature beat rate .Collected individual health information is aggregated and transmitted through a remote interface, for example, Bluetooth or WLAN. Keyword to delineate the health data is extricated from the health record. At that point, the keyword and PHR are encoded into a ciphertext under a particular access policy.

Personal Health Record (PHR)

Doctors, nursing staff, pharmacies, clinical lab workers, insurance suppliers, and the service providers are the information users in Health network. Every data user has a lot of characteristics, for example, alliance, office, and sort of hospital services staff, and is approved to look on encoded PHR's dependent on his set of properties. In system, a data utilizes asset constrained terminals to create secret keys and direct the data recovery activity. The secret keys are sent to the general public cloud by remote channel and recovered PHR documents are returned. At that point, the data user decrypts the PHR records and confirms the accuracy of decoding.

Public Cloud

The Public Cloud has practically boundless storage and computing capacity. This is to embrace the PHR remote storage assignment and react on information recovery request. Lightweight test algorithm is structured in this proposed framework to enhance performance.

Key Generation Center(KGC)

KGC creates open parameters for the whole system and distributes secret keys to data users. A data users, set of qualities is inserted in his secret key to acknowledge access control. If the traitor sells his secret key for financial profit, the KGC can trace the character of the malicious user and revoke his secret key

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008076 |

ALGORITHM

Algorithm 1: Advanced Encryption Standard (AES)

AES algorithm helps to encrypt the PHR.The algorithm uses 10 or 14 rounds for encryption with given key depending on 128 bytes or 256 bytes respectively . Each Round consist of 4 steps which includes SubByte where one each byte is substituted with another byte.The next is row shifteing were whole row is shifted.next is mixcolumn where columns are mixed and the last one is adding round key.One round is shown in Fig 3B

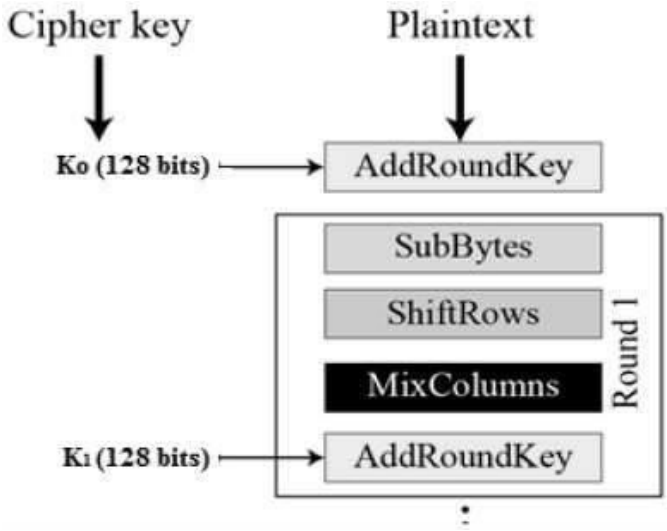

Fig 3.B. AES

Algorithm 2: Data in the Cloud for Optimal Performance and Security (DROPS)

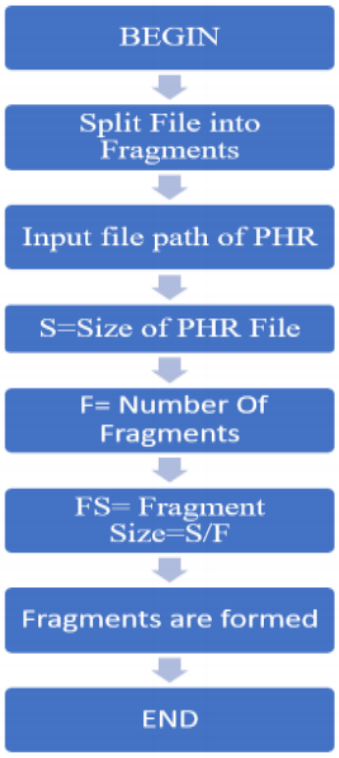

Fig 3 C: DROPS

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008076 |

Drops Algorithm is used for distribution of PHR data over multiple clouds in distributed form.File is divided in number of fragments and replicated over number of clouds.the Fig3C shows flow for division of file into number of fragments.

IV. RESULT AND ANALYSIS

GUI Interface

The GUI Interface gives graphical interface for making PHR Record . The Patient creates his record and uploads it in encryted form. Separate login are provided for owner of record and users of record. Fig 4A shows the interface.

Fig 4 A:GUI Interface

Collecting Data from Sensors

Data is collected from two sensors for temperature and pulse rate.This data is directly trasferred to PHR which is encryted to cloud.

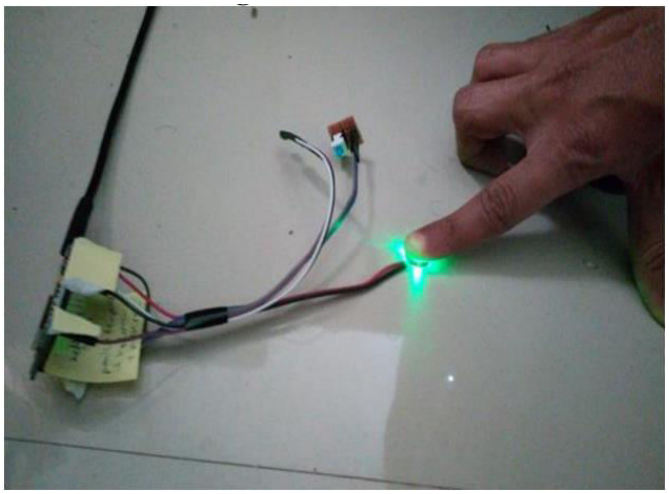

Fig 4 B: Collecting Data from Sensors

File Uploading Result

In the proposed system, storage of data is done on clouds.In enhanced system,before uploading files on the cloud, files are encrypted with use of AES algorithm as per above result and then they are stored on the cloud. DROP algorithm is used for fragmenting the file to addon one more feature to security while storing files on the cloud, thus it takes some time to write files on the cloud. In our development, we have considered the evaluation time for file upload used with encrypting and fragmenting. File size is in kb(kilobyte), as the file size increases, required time for uploading increases exponentially.Fig 4C shows graph for uploading the encryted PHR file.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008076 |

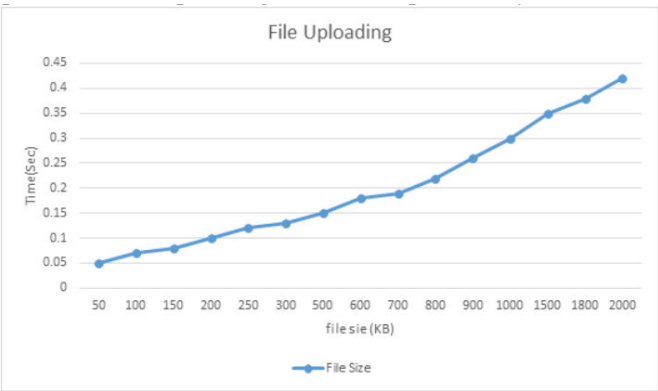

Fig 4 C: File Upload Time

Blocking Attacker Request

Hackers try to request for PHR if the key is leaked or sold Trapdoor Geanaration helps to block request of attcjers .the graph Fig 4D shows number of request send by attacker and number of genuine request,It also shows number request blocked.

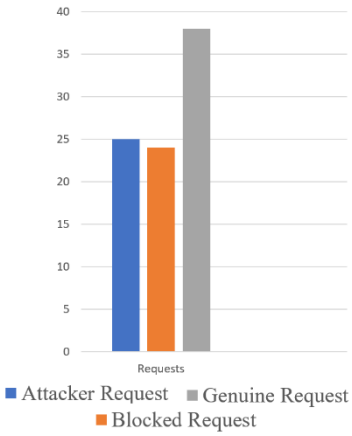

Fig 4 D: No Of Request

V. CONCLUSION

The enhanced methodology of securely stores data with help of Advanced Encryption Algorithm(AES) and transmits PHR's to the authorized users through use re encryption key issued by a semi-trusted authority. The activity of the semi-trusted authority is to deliver and store public/private key sets for the data-users in the framework. The technique preserves the security of the PHR's and authorizes a patient-driven access control. It is executing a fine-grained access control method so that even the valid system users can't access the fragments of the PHR for which they are not authorized. Use of IoMT features the advances made in healthcare with help of technology. The performance evaluation is done dependent on the time required to generate keys, encryption, decryption and turnaround time. Results the GUI interface for capturing sensor and maintaining PHR The upload time for each created PHR is tested with increasing file size..Future work can be done for PHR's in an advent towards machine learning and AI.

REFERENCES

[1] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multichannel communication in Edge-of- Things", Future Generation Computer Systems, 2018.

[2] K. Gai, M. Qiu, and X. Sun, "A survey on FinTech", Journal of Network and Computer Applications, 2017.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008076 |

[3] M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L.Jiang, "A general framework for secure sharing of personal health recordsin cloud system", Journal of Computer and System Sciences, 2017.

[4] A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach, Future Generation Computer Systems, 2015.

[5] B. Qin, R. H. Deng, S. Liu, S. Ma, "Attribute-based encryption with efficient verifiable outsourced decryption", IEEE Trans. Inf. Forensics Security, vol. 10, no. 7, pp. 1384-1394, JULY 2015.

[6] J. Han, W. Susilo, Y. Mu. "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption", IEEE Transactions on Information Forensics and Security, 2015.

[7] A. Abbas, S. U. Khan, Senior Member, "A Review on the State-of-the-Art Privacy Preserving Approaches in the e-Health Clouds", IEEE 2014.

[8] M. S. Dohan, M. Abouzahra and J. Tan, Mobile Personal Health Records: Research Agenda for Applications in Global Health, Hawaii InternationalConference on System Science, 2014.

[9] P. V. Gorp and M. Comuzzi, "Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud", IEEE Journal Of Biomedical And Health Informatics, Vol. 18, No. 1, January 2014.

[10] L. Guo, C. Zhang, J. Sun, Y. Fang, "A privacy-preserving attribute based authentication System for Mobile Health Networks", IEEE Trans-actions on Mobile Computing, 2014.

[11] J. Li, "Electronic personal health records and the question of privacy", Computers, 2013.

[12] A. Banerjee, P. Agrawal and R. Rajkumar, "Design of a Cloud Based Emergency Health-care Service Model", Spvryan's International Journal of Engineering Sciences & Technology (SEST) ISSN : 2394-0905, 2013.

[13] M. Li, S. Yu, Y. Zheng, K. Ren,W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute based encryption", IEEE transactions on parallel and distributed systems, 2013.

[14] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing", in Proceedings of the IEEE INFOCOM, March 2010.

[15] D. Daglish and N. Archer, "Electronic Personal Health Record Systems: A Brief Review of Privacy, Security, and Architectural Issues", IEEE 2009.

[16] M. Green, S. Hohenberger, B. Waters, "Outsourcing the decryption of ABE ciphertexts", in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.

[17] J. Yang, J. Li, Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment", Future Generation Computer Systems, 2015.

[18] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-based encryption for ne-grained access control of encrypted data", Proc. 13thm ACM Conf. Computer and Comm. Security (CCS'06), pp. 89-98, 2006.

[19] R. Ostrovsky, A. Sahai, B.Waters, "Attribute-based encryption with nonmonotonic access structures", in: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, 2007.

[20] http://www.pbs.org/newshour/updates/has-health-care-hacking -becomean-epidemic/

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details