Security and Privacy of a smart healthcare devices data using attribute based encryption

Nikita Navale, Asst. Prof. Pradnya Kasture,
Department of Computer Engineering R.M.D. SINHGAD SCHOOL OF ENGINEERING Pune, India

Abstract- In the projected system, we will work on Smart Health IOT Device that takes patients health recordings from the IOT device. On the cloud, to sustain data privacy and attain access control, Administrator can use attribute-based encryption to encrypt health recordings. At the time of encryption, the access policies are not sufficient. The work has been done to achieve the most influential form of access control, to build the circuit encryption system. In system coding based on the attributes of the encrypted text policy is used. This system introduces a Privacy aware S-health access control system, in which the key constituent is a large set. CP-ABE with access policies are hidden to some extent. In Privacy aware S-health, the values of the attributes of the access policies are hidden in the encrypted Smart Health Records and only the names of the attributes i.e characteristics are forwarded. That is, attribute values contain most private information than collective attribute names. Privacy aware S-health system performs an powerful Smart Health Records decryption test. The attributes set can be exponentially large and the size of public parameters is minute and constant. The readings are getting from Smart Health IOT Device. Recordings are type of body temperature, pulse rate which are stored securely. The health recordings will be placed on a node after that concept of T-coloring will be applied for dividing recordings into number of files.

Index Terms- Cloud storage, Attribute-based encryption, Decryption Privacy protection, Smart health

I. INTRODUCTION

Cloud computing allows users to keep their confidential data on unreliable cloud service providers to obtain on- demand request services. The main security requirements of this data storage and management system include the security and confidentiality of data and require the use of advanced cryptographic techniques with detailed access to data security in cloud computing. SMART health is the context-sensitive improvement in mobile health in smart cities and offers an opportunity for accurate and efficient prevention of various diseases and incidents As a type of key technology in smart cities, the Internet of Things has been widely applied to interconnect available medical resources and provide reliabil- ity and effective health services for the elderly and patients. In particular, data security and privacy issues have become the main concerns of healthy people. For example, a patient generally expects their health records (SHR), such as blood pressure and heart rate, to be consulted only by licensed health professionals. Bearing in mind that, if traditional access control techniques are adopted, the security of the data is violated or only general access policies are allowed.

A. MOTIVATION

As we move towards digitization, archives of medicinal images and medicinal recording are growing rapidly,large health care enterprises keep a large amount of data on third party i.e. nothing but cloud. It is done in purpose to diminish information storage costs and sustain medicinal assistance. As the server present on the cloud is not completely trustworthy, the encrypted storage file is an efficient path to prevent confidential information from being thriven or interfered with. Advanced technologies like Internet of Things and cloud com- puting are being developed at immense speed. smart health is developed to considerably boost the quality of medicinal care. Smart Health currently has issues like user privacy and data security which are not been adequately approached. On these issues,a cipher text-policy hiding attribute- based encryption has the capabilities to gain data security and privacy in smart health.

II. REVIEW OF LITERATURE

This document presents Privacy aware smart health access control sysytem in which main constituent is a huge set CP-ABE with accces policies are hidden to some extent In Privacy aware smart health, the values of the attributes of the access policy are hidden in the encrypted SHRs and the names of the attributes are revealed[17].It presents two constructions of fuzzy IBE schemes. This IBE schemes are tolerant of errors and safe against collusion attacks. In addition, This system basic construction does not use oracles at random.System prove the security of This system schemes under the Selective- ID security model[14]. Introduces a new model for CP-ABE with partially hidden access structures. In This system model, each attribute consists of two parts: an attribute name and its value; If the attributes of a users private key do not match the access structure associated with an encrypted text, the attributes specific to the attributes of the access structure are hidden, while other information about the access structure is public [16]. The current system proposes a subcontracted construction of ABE that provides the capacity to Check the computational results efficiently. The extensive safety and performance analysis shows that the proposed schemes have proven to be safe and practical [3]. This system will use the concept of economically viable cloud selection in this article. The system also refers to the heuristic data placement algorithm for the selection of the cloud. The storage of data in the cloud redefines the security problems that are being attacked in the data subcontracted by the client. From the customer's point of view, it is not safe to trust a service provider just for your recovered data. In this project, a new information hosting system (called CHARM) that integrates two desired key functions. The first is to select several suitable clouds and an adequate redundancy plan to store data with reduced financial costs and ease of use [10].Present The concept of fragmentation and cryptography on the user's side refers to this document. This technique provides security at the server, network and cloud server level. [6]. In the present document reference is made to the current concept of a color graph T to position fragments as a system such as the fragment placement algorithm. When the fragments are lost with the help of the replica, you can cover[7]. Present Before data is stored on the cloud server, the data can be encrypted. The attribute-based encryption technique is a public-key cryptography that allows access control over encrypted data using different access policies and attributes. The personal health record (PHR) is a model of emerging health information exchange, which is always available to be stored in third parties, such as the server in the cloud. Attribute-based encryption is applied before storing personal medical and patient health information. A public audit scheme is used to verify the manipulated data in the cloud server. This scheme can completely free up the burden of PHR users to store and maintain their data on the server in the cloud [2]. Encryption-based cryptography of the current cryptographic text policy is a cryptographic solution that promises these problems for the application of access control policies defined by the owner of the data in the subcontracting data. In this document, the system proposes an access control mechanism that uses cryptography based on cryptographic attributes to apply access control policies with characteristics to discard attributes and efficient users. The control of the detailed access obtained through a double encryption mechanism that uses the ABE and the distribution of selective group keys in each group of attributes. The system demonstrates how to apply the proposed mechanism to securely manage the outsourced data[1].

Live survey 1.Blockchain 2.IT -Sector

III. SYSTEM ARCHITECTURE/ SYSTEM OVERVIEW

In proposed system Administrator will get data from IOT device that is sensed from temperature sensor and that patient will allocate to specialists according to specialists position location and experience. Hospitals patient distributor will assign the patients to specialist by generating access policies considering specialists attribute location and experience after entering encryp- tion key then file will fragment and store with fragment and its replica. When Authenticated specialist login then he will get the file with which his policy attribute matches. Then he can request for the file key and download the file after entering secrete key. Third party auditor will check data integrity of stored fragment that means placed fragment content is changed or not if changed then integrity auditor will inform to Administrator about that file. integrity auditor will then replace changed fragment with original copy of fragment and provide integrity.

In proposed system Firstly, As its a web application OS, Cloud will be Amazon ec2 Secondly, This uses IOT Here microcontroller and sensors are used. In project NodeMCU microcontoller is used. NodeMCU is an free IoT platform. It includes firmware which executes on the ESP8266 Wi-Fi SoC from Espress if Systems, and hardware which is based on the ESP-12 module. The LM35 series are precision integrated- circuit temperature devices In proposed system the LM35 device has an advantage over linear temperature sensors as the user is not required to subtract a large constant voltage from the output to obtain convenient Centigrade scaling.

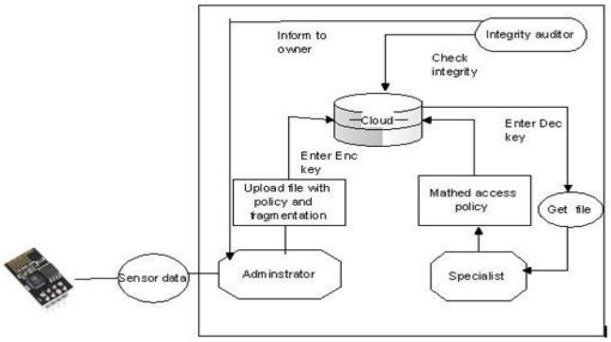


Fig.1: Proposed System Architecture

A.

Algorithms

1) Advanced encryption standard (AES) Algorithm For Encryption

AES(advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text.The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider as weak.

Input: 128 bit/192 bit/256 bit input(0,1) secret key(128 bit)+plain text(128 bit). Output: cipher text(128 bit).

Steps
1. 10/12/14-rounds for:128_bit /192 bit256 bit input
2. Xor state block (i/p)
3. Final round:10,12,14
4. Each round consists:sub byte, shift byte, mix columns, add round key.

2) T-coloring Technique

The fragmented data is stored in T-Coloring manner that follows Store the fragment in non-adjacent node that hacker will not identified the sequence of stored fragment. So data will store in secure form.This T- coloring concept will be applicable while uploading data on node the file will replicate on nodes and the node selection process will be based on T-Coloring concept.File will placed and its replica will place at non- adjacent node based on T-coloring concept.

B. Mathematical Model

Notation
1.NNik Nearest neighbor of Si holding Ok
2. Ok kth fragment of file
3. OkSizeofOk
4. Wik Aggregate write cost of Wik
5. Rik Aggregate read cost of Rik
6. Si -Size of Si
7. r^i -Number of reads for Ok from Si
8. w^i -Number of writes for Ok from Si

Equation
Fragment=Size of file/No.of fragments.
The total read time of Ok by Si from NNik is denoted by
Rik and is given by:

C. HARDWARE AND SOFTWARE REQUIREMENTS

Hardware Requirements
1) Processor - Intel i5 core
2) Speed - 1.1 GHz
3) RAM - 2GB
4) Hard-Disk space - 40 GB
5) Key Board - Windows Keyboard
6) Mouse - Two or Three Button Mouse
7) Monitor - SVGA
8) Microcontroller -nodemcu ESP8266
9) Sensor -LM35 Precision Centigrade Temperature Sen- sors

Software Requirements
1) Operating System - XP, Windows7/8/10
2) Coding language - Java, MVC, JSP, HTML, CSS etc
3) Software - JDK1.7
4) Tool - Eclipse Luna
5) Server - Apache Tomcat 7.0
6) Database - MySQL 5.0

IV. SYSTEM ANALYSIS AND RESULT

A. Screen

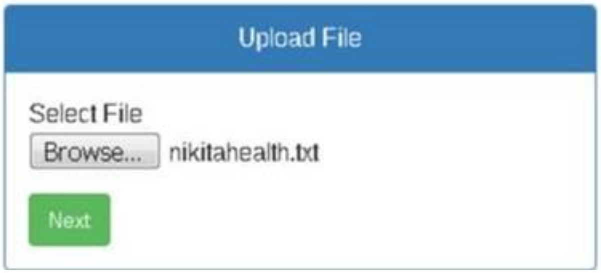
Ri i

k=rk (i,NNik)

The total time due to the writing of Ok bySi addressed to the Pk is represented as Wik and is given:

k=wk(C(i, Pk) + P(J R),j∈/i) c(Pk, j)
W i I k

Fig.2: Node-MCU Microcontroller



Upload File

Select File

nikitahealth.txt

Fig.3: Select File

T-coloring
This T-coloring concept will be applicable while uploading data on node the file will replicate on nodes and the node selection process will be based on T-Coloring concept.File will placed and its replica will place at non-adjacent node based on T-cooring concept.

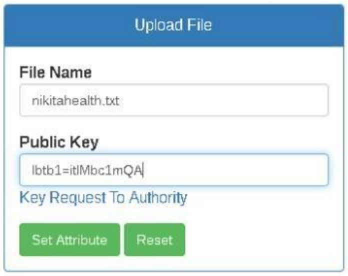
In graph theory, a T-Coloring of a graph

$$G = (V, E)$$

given the set T of nonnegative integers that contains 0, is a function c : V (G) → Nc : V (G) → Nthat maps each vertex of G to a positive integer (color) such that

$$(u, w) \in E(G) \Rightarrow |c(u) - c(w)| \in/ T$$

In the perfect value of the difference between two colors of adjacent vertices should not belong to fixed set T. The concept was introduced by William K. Hale. If T = 0 it decreases to common vertex coloring.

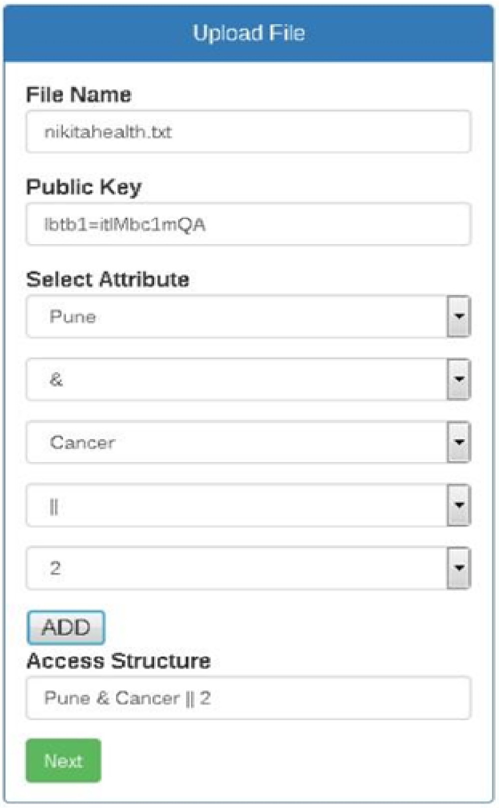


Upload File

File Name: nikitahealth.txt

Public Key: lbtb1=itlMbc1mQA

Fig.4: Enter key



Upload File

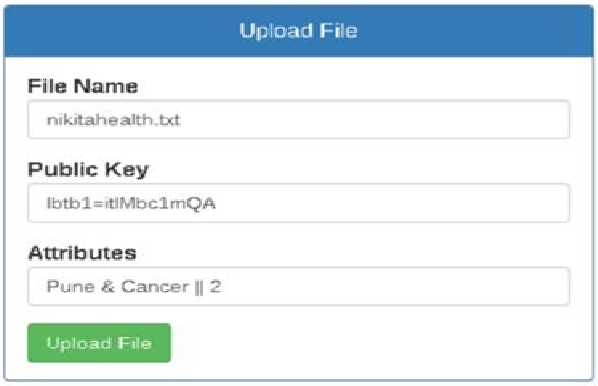
File Name: nikitahealth.txt

Public Key: lbtb1=itlMbc1mQA

Select Attribute: Pune & Cancer || 2

Access Structure: Pune & Cancer || 2

Fig.5: Apply policy



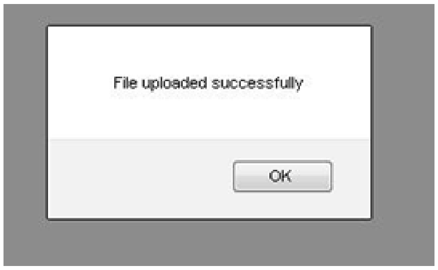
Upload File

File Name: nikitahealth.txt

Public Key: lbtb1=itlMbc1mQA

Attributes: Pune & Cancer || 2

Fig.6: selected policy



File uploaded successfully

Fig.7: Uploaded success

TABLE I
SHOWS FILE SIZE AND TIME (MS)TO UPLOAD FILE

Index Number	File size	Time in ms
1	120kb	60
2	320kb	155
3	400kb	160
4	450mb	200
5	510mb	220

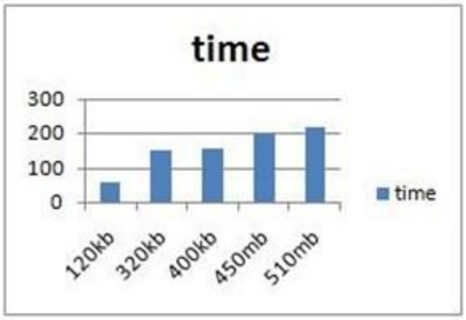


Fig.8: Shows file size on x axis and time (ms)to upload on Y-axis

V. CONCLUSION

Present the system efficiently addressed data security and user privacy issues in smart healthcare system by introducing Privacy aware smart health, a privacy aware s-health access control system. The porpose of Privacy aware smart health is a CP-ABE scheme which supports large universe and partially hidden access policies. In Privacy aware smart health, sensitive attribute values involved in access policies are hidden and generic attribute names are public. Data integrity is checked by integrity auditor. Security of data is improved by T- Coloring attribute.

B. System analysis

Experimental setup Table 1-gives the information of up-loading time for 120kb, 320kb, 400kb, 450mb and 510mb file size.Fig.2-size of file and time to upload that file after performing fragment and t-coloring .As size of file increases the time will increase. X-ais size of file and in ms.The file will replicated based on T-coloring concept.

VI. REFERENCES

[1]. Junbeom Hur and Dong Kun Noh,' Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems', Volume 22, NO. 7, JULY 2011 IEEE.

[2]. J. Han, W. Susilo, Y. Mu, and J. Yan, 'Privacy-preserving decentralized key-policy attribute-based Encryption,' IEEE Trans. ParallelDistrib. Syst., Volume 23, no. 11, Nov. 2012.

[3]. J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, 'Securely outsourcing attribute-based encryption with checkability,' IEEE Trans. Parallel Distrib. Syst., Volume 25, no. 8, Aug. 2013.

[4]. K. Kurosawa and Y. Desmedt, A new paradigm of hybrid encryption scheme,' in Proc. 24th Int. Cryptol. Conf., 2004,

[5]. R. Cramer and V. Shoup, 'A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack,' inProc. 18th Int. Cryp- tol. Conf., 1998,

[6]. Jun Feng, Yu Chen, Wei-Shinn Ku, Zhou Su ,D-DOG: Securing Sensitive Data in Distributed Storage Space by Data Division and Out-of-order keystream Generation.2010

[7]. Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE, Samee U. Khan, Senior Member, IEEE, Bharadwaj Veeravalli, Senior Member, IEEE, Keqin Li, Senior Member, IEEE, andAlbert Y. Zomaya, Fellow, IEEE,DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security.2015

[8]. Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian.Privacy- Preserving Public Auditing for Regenerating-Code-Based Cloud Storage. May 2015

[9]. Shristi Sharma,Shreya Jaiswal,Priyanka Sharma,Prof. Deepshikha Patel, Prof. Sweta Gupta.An Approach For File Splitting And Merging.

[10]. Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, and Yafei DaiCHARM: A Cost-efficient Multi-cloud Data Hosting Scheme with High Availability .2015

[11]. L. M. Kaufman, 'Data security in the world of cloud computing,'IEEE Security and Privacy, Volume 7, No. 4, 2009,

[12]. D. Boru, D. Kliazovich, F. Granelli, P. Bouvry, and A. Y. Zomaya, 'Energy-efficient data replication in cloud computing datacenters,' In IEEE Globecom Workshops, 2013, pp. 446-451.

[13]. B. Xu, L. Xu, H. Cai, L. Jiang, Y. Luo, and Y. Gu, 'The design of an m-health monitoring system based on a cloud computing platform,' Enterprise Information Systems, Volume 11, no. 1, 2017.

[14]. A. Sahai and B. Waters, 'Fuzzy identity-based encryption,' in Advances in Cryptology (EUROCRYPT05), 2005,

[15]. A. Lewko and B. Waters, 'Decentralizing attribute-based encryption,' in Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT11), 2011.

[16]. J. Lai, R. H. Deng, and Y. Li, 'Expressive cp-abe with partially hidden access structures,' in Proceedings of ACM Symposium on Information, Computer and Communications Security (ASIACCS12), 2012.

[17]. Yinghui Zhang, Member, IEEE, Dong Zheng, Robert H. Deng, Fellow, IEEE"Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control" IEEE TRANSACTIONS ON CLOUD COMPUTING,Volume3,NO.1,APRIL2018