ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

An Effective Approach to Preserve Privacy of Health Data in Cloud Using SA-CPABE

Deepashree N S

Department of Computer Science, R V College of Engineering, Bangalore, India

ABSTRACT: Cloud computing is an emerging technology where people can store their large amount of data. It is a new and virtually precise concept of computing technique, by which computer resources are shared dynamically through the Internet thus by appealing considerable and remarkable attention and interest from both academia and industry. Anywhere, anytime accessibility of data in cloud by the authenticated person is the major concern. This computing virtualization enables flexible and low cost computing enabling it outsources to the cloud servers thus making privacy a least concern. Hence, in this paper, we present a control on a Cipher-text policy which decentralizes the central authority to limit the identity leakage and thus achieves semi -anonymity. The data is encrypted in two ways one way is by using CPABE in which encryption occurs in server host side and another uses AES which encryption occurs at the local slot. In considering this entire scenario we can see the cipher-text generation can be done by protocols which results in thorough encryption which avoids the security breach thus making it semi anonymous to the respective attributes and thus enhancing the privileges to individual authority.

KEYWORDS: Emergency medical Technician (EMT), privacy, K-Anonymity, mHealth, Sever aided CPABE, Third party auditor (TPA).

I. INTRODUCTION

Cloud computing is a buzzword that conveys everything as a service over the web on user demand, like network, storage, hardware, software. Benefits of cloud storage are scalability access of the data to one's knowledge anyplace, anyhow, anytime. So every organization is moving its data to the cloud, it uses the secure storage service provided by the cloud provider. Number of businesses using cloud computing has increased dramatically over the last few years due to the attractive features such as flexibility, fast start-up ,scalability, and low costs. Health data accessing is slow evolvement and its procuring enables a well serviced health provisioning, enhances the quality of life and helps in reducing time for analysis and increase the fast treatment in medical emergencies anywhere-anytime. Benefits of cloud storage are easy access of the data to one's awareness anyplace, anytime, anyhow [2]. The proposed cloud-assisted mobile health networking is motivated by the power, flexibility, convenience, and cost efficiency of the cloud-based data/computation outsourcing paradigm. This paper introduces the private cloud security which can be considered as a service offered to mobile users. The proposed solutions are built on the service model. A software as a service (SaaS) provider provides private cloud services by using infrastructure of the public cloud providers (e.g., Amazon, Microsoft, yahoo, Google). An efficient encryption technique can be used for secure access to and storage of data on public cloud server, moving and searching encrypted data through communication channels while protecting data confidentiality [1]. Mobile devices (e.g. smartphone, PDA and laptop) have become the primary computing platform for many users because of their mobility and network connectivity [3]. Mobile users outsource the data processing tasks to the private cloud which stores the processed results on the public cloud. The cloud-based service model supports the implementation of privacy mechanisms since intensive computation and storage can be shifted to the cloud, leaving mobile users with the lightweight tasks [9]. Pros do not merely help in diversifying the technology thus making analysts to keep a look on the challenges. The cloud emphasizes or helps us to analyze our proposed system thorough scenario and thus would provide a basement for the invention of new algorithms which is really what the technology needs. The main entities involved in our system are illustrated in Fig. 1. The system involves in user collecting their health data through the health tracking patches, electrocardiogram sensors. Emergency medical technician (EMT) is a physician who performs the emergency treatment. By user and EMT refer to the person and the associated computing facilities. The computing facilities are mainly mobile devices that carried around such as smart-phone, tablet, or personal digital assistant. Each user is associated with one particular private cloud. Multiple private clouds are supported on the same physical server. Private clouds are always available to handle health data on behalf of the users because private clouds are always online [10].

However the above environment does not suit the requirements of the methodology. At this present scenario small and medium scaled organizations cannot afford to build up an own cloud environment to use the fundamentals of identity. In this scene there is much less effort has been made during those interactive protocols. User's identities, which are reported with their attributes, are opened to key generators, and the generators issue private keys according to their attributes. But it appear natural that users might want to keep their identities secret while they still get their private and accessing this information should not cause reentrancy and an overhead during the communication.

In considering this entire scenario we can see the cipher-text generation can be done by protocols which results best with the key generation tactics to avoid the security breach.

This can be very advantageous in the situations like medical emergencies. The private cloud will process the data to add security before it is stored on the public cloud. Public cloud is the cloud infrastructure owned by the cloud providers like Amazon and Google which offers massive storage and rich computational resource. We assume that at the bootstrap phase, there is a secure way between the user and his/her private cloud, e.g., secure home Wi-Fi network, to obtain a long-term shared-key. After the bootstrap phase, user will send health data over insecure network to the private cloud residing via the Internet backbone. Nowadays, physicians are increasingly utilizing mobile health (mHealth) applications in clinical care [6].

II. RELATED WORK

According to Shamir et al In the IBE, the sender of a message can define an identity such that only a receiver with exactly identical identity can decrypt it. This is totally a sound variation from Public-key Encryption. However this method provides good resiliency but compromises if the technology development is known. To mitigate this IBE – Fuzzy Identity-Based Encryption which is also synonymously known as Attribute-Based Encryption (ABE) is introduced [8]. In their work, an identity is observed as a set of descriptive attributes. Different from the IBE, where the decryption could decrypt the message if and only if his/her identity is exactly the same as what specified by the encryption, this fuzzy IBE enables the decryption in which there are 'identity overlaps' exceeding a pre-set threshold between the one specified by encryption and decision of encryption policy is made by different parties.

Personal Health Record (PHR) service is an emerging model for health information exchange [4-5]. Mobile devices help in reducing this clutter, such as home care and remote monitoring enable the people in their flexible lifestyle and cause minimal interruption to their daily activities. In addition, it significantly reduces the hospital occupation, allowing patients with higher need of in-hospital treatment to be admitted. Fine! All these scenarios are possible but people admit to realize that they would completely lose their personal information and identity once it activates in the cyber space. This take place around because in a survey 8 million patients' health information was leaked over a couple of years. But why this medical data should be kept private rather than allowing somebody to have a research on it. Of course there are some quite good reasons for it. An employer may not find convenient to hire someone with certain diseases. A mutual fund or brokerage insurance firm may refuse to provide features once they know about the history of the disease of the patient. Despite the paramount importance, privacy problems are not addressed adequately at the technical level and efforts to keep health data secure have continually fallen short. This is because protecting privacy in the cyberspace is significantly more challenging. Thus, there is an important need for the development of viable protocols, architectures, and systems assuring privacy and security to protect sensitive and personal digital information.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

III. PROPOSED SYSTEM

The Proposed system deals with the design and working of the implementation of practical privacy mechanisms in e-health care systems. The third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Users rely on the Cloud Server (CS) for cloud data storage and maintenance. They may additionally dynamically interact with the CS to access and update their stored data for various application purposes. The users may resort to TPA for ascertaining the storage security of their outsourced data, protect their data from TPA. The man source that comes to rescue in the system is anonymity i.e hiding some specific set of attributes based on the user authority. The data is passed for partial encryption using AES and SA-CPABE and uploaded to the server (cloud). The patient data is updated by the authority and TPA verifies it by extracting the file from the cloud. Block diagram of a proposed system shown in the Fig 1.

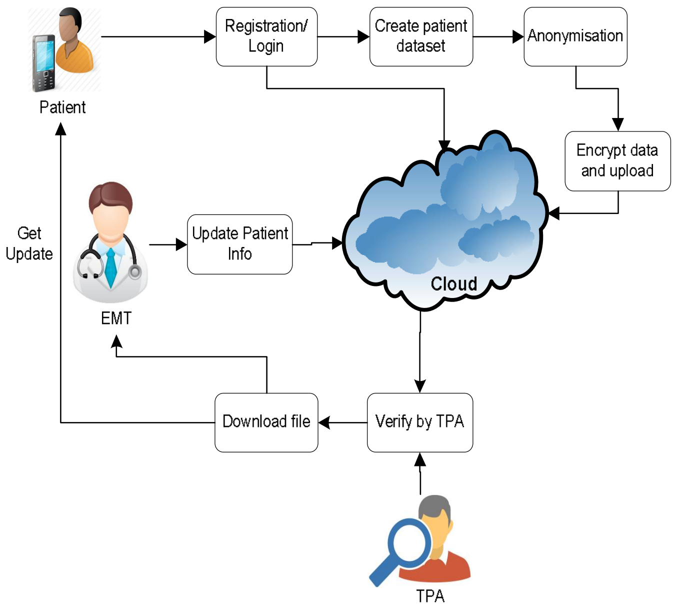

Fig 1: Block diagram of Proposed System

3.1 AES Encryption

The encryption process made up of the combination of various classical techniques like substitution, rearrangement and transformation encoding techniques. The modifications include addition of an arithmetic operation and a route transposition cipher in the attacks iterative rounds. The encryption and decryption modules in this algorithm include the Key Expansion module which generates Key for all iterations The Key expansion module is extended to double the number of iterative processing rounds in order to increase its exception against unauthorized attacks. Advanced Encryption Standard (AES) algorithm is not only for security but also for great speed. Both hardware and software implementation are faster still and replaces DES. AES encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size as explained above can be implemented on various platforms especially in small devices. It is carefully tested for many security applications.

Sub Bytes: The first transformation, Sub Bytes, is used at the encryption site. To substitute a byte, we interpret the byte as two hexadecimal digits.

Shift Rows: In the encryption, the transformation is called Shift Rows.

Mix Columns: The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Add Round Key: Add Round Key precedes one column at a time. Add Round Key adds a round key word with each state column matrix; the operation in Add Round Key is matrix addition. The last step consists of XO Ring the output of the previous three steps with four words from the key schedule. And the last round for encryption does not involve the "Mix columns" step.

It is very important to know that the cipher input bytes are mapped onto the state bytes in the order $a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, a_{2,1}, a_{3,1}$ and the bytes of the cipher key are mapped onto the array in the order $k_{0,0}, k_{1,0}, k_{2,0}, k_{3,0}, k_{0,1}, k_{1,1}, k_{2,1}, k_{3,1}$. At the end of the cipher operation, the cipher output is extracted from the state by taking the state bytes in the same order. AES uses a variable number of rounds, which are fixed: A key of size 128 has 10 rounds. A key of size 192 has 12 rounds. A key of size 256 has 14 rounds.

It is very important to know that the cipher input bytes are mapped onto the state bytes in the order $a_{0,0}, a_{1,0}, a_{2,0}, a_{3,0}, a_{0,1}, a_{1,1}, a_{2,1}, a_{3,1}$ and the bytes of the cipher key are mapped onto the array in the order$k_{0,0}, k_{1,0}, k_{2,0}, k_{3,0}, k_{0,1}, k_{1,1}, k_{2,1}, k_{3,1}$. At the end of the cipher operation, the cipher output is extracted from the state by taking the state bytes in the same order. AES uses a variable number of rounds, which are fixed: A key of size 128 has 10 rounds. A key of size 192 has 12 rounds. A key of size 256 has 14 rounds.

Decryption: Decryption involves reversing all the steps taken in encryption using inverse functions like Inverse shift rows, Inverse substitute bytes, Add round key, and Inverse mix columns. The third step consists of XOR-ing the output of the intermediates

3.2 Server aided-CPABE

On the other hand, CP-ABE has a solution to all these problems and thus solves partially the overhead involved. In the CP-ABE, cipher-texts are created with an access structure, which specifies the encryption policy, and private keys are generated strictly based on the users attributes. A user can access the cipher-text only if his attributes in the private key and the access tree specified in the cipher-text match. By doing so, the encrypted holds the ultimate authority about the encryption policy. Also, the already issued private keys will never be modified unless the whole system crashes and the system's master key are lost.

There is a model called multi-authority system, where each user has an ID and they can interact with each key generator (authority) using different pseudonyms this technique finds no replications to the method above. One user's different pseudonyms are tied to his private key, but key generators never know about the private keys, and thus they are not able to link multiple pseudonyms belonging to the same user. In fact they are even not able to distinguish the same user in different transactions. Also, the whole attributes set is divided into N disjoint sets and managed by N attributes authorities. That is, an attribute authority will only issue key components which it is in charge of. In this setting, even if an authority successfully guesses a user's ID, it knows only parts of the user's attributes, which are not enough to figure out the user's identity. In addition, many similar literature works have been published to create more advanced schemes where data needs to be securely and efficiently protected, which in turn served as the base of the research on security protocol in cloud computing environment. This attributes about the CP-ABE. However, we additionally tag it with the server for the second way of encryption which is called Server aided CP-ABE which happens at the host side providing along the security and the access privileges for the unit. However the detailed step which associates with SA-CPABE is illustrated with the six steps below.

Setup: is identified with the small expression. The setup point issues two arguments one is the security parameter and the other one is total attribute description and thus showcasing the output with the public parameters PP (the data to be encrypted) and the master secret key MSK.

$$(\lambda, U) \rightarrow PP, SK \quad (1)$$

KeyGen: The key generation function accepts three parameters as the argument one is the PP (public parameter), the secret key (MSK), and an attribute set S (User's Attribute) and outputs a user key K_{user} (Private Key)and a server key K_{server} (Public Key). The user keeps K_{user}locally, and gives K_{server} to its decryption server.

$$(PP, MSK, S) \rightarrow K_{user}, K_{server} \quad (2)$$

Pre-compute: The pre-computation algorithm takes as input the public parameters PP and outputs a temporal key TK and an intermediate cipher-textIC. The user keeps TK locally, and stores IC on its storage server to save local storage resources.

$$(PP) \rightarrow IC, TK \quad (3)$$

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Encrypt: In the encryption side, three arguments are passed to the function as inputs an intermediate cipher-text IC, a temporal key TK, a message M, and an access structure A thus producing an intermediate encrypted output CT.

$$(IC, TK, M, A) \rightarrow CT \quad (4)$$

Transform: The cipher-text transformation algorithm takes as input a server key K_{server} for attribute set S and a cipher-text CT that was encrypted under A. It outputs the partially decrypted cipher-text CT if $S \in A$ and the error symbol $\perp$ otherwise.

$$(K_{server}, CT) \rightarrow CT \quad (5)$$

Decrypt: The decryption algorithm takes as input a user private key K_{user} for S and a partially decrypted ciphertext CT that was originally encrypted under A. It outputs the message M if $S \in A$ and the error symbol $\perp$ otherwise.

$$(CT, K_{user}) \rightarrow M \quad (6)$$

3.3 Anonymity

Health data service is a common and popular approach for attracting wide application users. K-anonymity is an important measure for privacy to avoid the disclosure of personal data [7]. Software as a Service is one of the best and preferable methods in cloud computing that can be implemented by cooperation of various services and provides real-time services through the network.

The main idea is to provide secure and also anonymous online services of medical data among cloud computing infrastructure in specific organizations. Security can be enhanced in many ways like access control, anonymity, cryptography protocols and etc although there is a tradeoff between security enhancement level and system performance. Since Security implications should be applied thoroughly and specifically thus imposing to heavy burden on system processes. In all these cases we see that securing identity of an individual is primary task and selecting on how many attributes we need to perform is to be chosen based on the requirement and the criterion.

The k-anonymity model was first described in the context of data table releases. In this section we reiterate their definition and then proceed to analyze the merits and shortcomings of k-anonymity as a privacy model. The k-anonymity model distinguishes three entities: individuals, whose privacy needs to be protected; the database owner, who controls a table in which each row describes exactly one individual; and the attacker. The k-anonymity model makes two major assumptions: The database owner is able to separate the columns of the table into a set of quasi-identifiers, which are attributes that may appear in external tables the database owner does not control, and set private columns, the values of which need to be protected. The term referred as two sets as public attributes and private attributes, respectively. Secondly the attacker has full knowledge of the public attribute values of individuals, and no knowledge of their private data. The attacker only perform linking attacks' linking attack is executed by taking external tables containing the identities of individual, and some or all of the public attributes that appear in a row of a table released by the database owner then we say that the individual is linked to that row. Specifically the individual is linked to the private attribute values that appear in that row. A linking attack will succeed if the attacker is able to match the identity of an individual against the value of a private attribute. As accepted in other privacy models (e.g., cryptography), it is assumed that the domain of the data and the algorithms used for anonymization are known to the attacker. The assumption reflects the fact that knowledge about the nature of the domain is usually public and in any case of a different nature than specific knowledge about individuals. For instance, knowing that every person has a height between zero and three meters is different than knowing the height of a given individual. Under the k-anonymity model, the database owner retains the k-anonymity of individuals if none of them can be linked with fewer than k rows in a released table. This is achieved by making certain that in any table released by the owner there are at least k rows with the same combination of values in the public attributes. Since that would not necessarily hold for every table, most of the work under the k-anonymity model focuses on methods of suppressing, altering, and eliminating attribute values in order that the changed table qualify as k-ananymous

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

IV. RESULTS AND DISCUSSIONS

The fig 2 described below invokes the interface of the proposed system which supports various features which include the navigational ability for home, patient, emt, tpa.

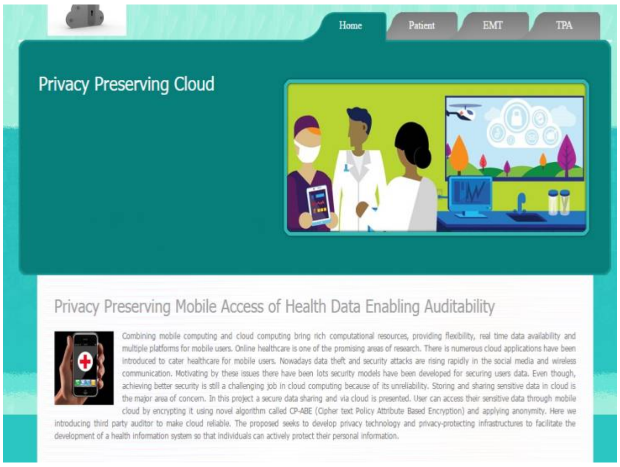

Fig 2: Block Diagram of the proposed system

Table 1 gives information about encryption and Decryption time of various cryptographic algorithm with SA-CP ABE based on the file size. Compare to ABE, CP-ABE new algorithm called SA-CPABE is efficient in terms of time complexity and it requires less space. Since the information related to users are stored in cloud server the system does not need extra utilization resources like power, memory...etc.

	File size	100 KB	200 KB	300 KB
Encryption time	ABE	12	24.1	39.0
	CP-ABE	11.8	24	35
	SA-CPABE	10.5	20	30.5
Decryption time	ABE	8	15.9	19.2
	CP-ABE	7	8.2	19.4
	SA-CPABE	6.3	11.2	16.8

Table 1: Performance Evaluation of SA-CP-ABE with existing Encryption algorithm

V. CONCLUSION

In this paper protection of the medical details and its anonymity in cloud is presented. The proposed system is used to build privacy into mobile health systems with the help of the private cloud. This system provided a solution for privacy-preserving data storage by integrating a CP-ABE based key management for unlink ability and also investigated techniques that provide access control (in both normal and emergency cases) and audit ability of the authorized parties to prevent misbehavior, by combining anonymity with advanced encryption standard encryption. As

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

a future work devises a new model which automatically find out the illegal distribution of data by the trusted party and also find any leakage of data during transmission.

ACKNOWLEDGEMENTS

I express my immense gratitude to my guide Dr.S.R.Swamy, Professor, Department of Computer Science and Engineering, R V College of Engineering, Bangalore, for his estimated guidance and valuable suggestions in bringing out this work successfully

REFERENCES

[1] P. Umaeswari"Achieving Secure Data Access in Cloud Computing" *Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 363-369,* 2015.

[2] Raseena M ,Harikrishnan G R, "Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Broadcast Encryption" *International Journal of Computer Applications (0975 8887)Volume 102 - No. 16,* September 2014

[3] Chang-Ji Wang, Xi-Lei Xu, Dong-Yuan Shi and Wen-Long Lin "An Efficient Cloud-based Personal Health Records System Using Attribute-Based Encryption and Anonymous Multi-Receiver Identity-Based Encryption" *Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing* 2014.

[4] Vassiliki Koufi1, Flora Malamateniou1, George Vassilacopoulos. "Privacy-Preserving Mobile Access to Personal Health Records through Google's Android" *International Conference on Wireless Mobile Communication and Healthcare - "Transforming healthcare through innovations in mobile and wireless technologies" (MOBIHEALTH)*

[5] Khuong Vu and Rong Zheng JieGao" Efficient Algorithms for K-Anonymous Location Privacy in Participator Sensing". *2012 proceedings IEEE INFOCOM*

[6] K.S.Suresh M.Tech, Prof K.V.Prasad**,**"Security Issues and Security Algorithms in Cloud Computing" *International Journal of Advanced Research in Computer Science and Software EngineeringVolume 2, Issue 10***,** October 2012

[7] Assad Abbas and Samee U. Khan, "A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds*" IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 4,* July 2014.

[8] Surender Sharma and Venki Balasubramanian "A Biometric Based Authentication and Encryption Framework for Sensor Health Data in Cloud" *International Conference on Information Technology and Multimedia (ICIMU),* November 18 – 20, 2014.

[9] Hasan Omar Al-Sakran , "Accessing Secured Data In Cloud Computing Environment " *International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.1,* January 2015.

[10] Yu Jin, Chuan Tian Heng He, Fan Wang," A Secure and Lightweight Data Access Control Scheme for Mobile Cloud Computing" *2015 IEEE Fifth International Conference on Big Data and Cloud Computing*

.