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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

HealthCare Monitoring Solution with Decryption Outsourcing by Parallel Computing in Cloud

Mr.K.Ganesan, Mr.C.Vijayakumaran

PG Student, M.E (CSE), Valliammai Engineering College, Chennai, India[1]

Assistant professor, Department of CSE, Valliammai Engineering College, Chennai, India[2]

ABSTRACT— Mobile devices have reached a wide development range and proved its assistance in health care with the combination of Cloud Server. The health monitoring offers various services such as monitoring of physiological data through remote sensors. These are achieved in collaboration with Cloud Servers providing software as a service, thus providing healthcare solutions at low cost. But there is a high risk of security violation of patient's private data as there is a lack of data management. The proposed approach identifies the existing system's design problems and proposes private key proxy re-encryption scheme that helps in reduction of computation complexity of securing data. This system is used to transmit patient's personal information from smart mobile phone to a monitoring system installed by a health service provider in cloud, such that the third party collaborator of the healthcare company is then responsible for private key distribution to clients which can be used for querying his data. When the user requires accessing his data, he/she passes the private key and the healthcare company index to the collaborator, who in turn inputs the master key to the cloud that provide parallel access to the databases. The user finally receives a token from collaborator and pass to the cloud, which respond back to the user with semi-decrypted data and final decryption takes place at the end user's place. Hence the cloud has no reach to unencrypted private data of the user. Also the advantage of this model is drastically reduces the workload of encryption/decryption tasks by outsourcing them to the cloud server.

KEYWORDS— Private key proxy re-encryption, Outsourcing Decryption, Triple DES algorithm, Security

I. INTRODUCTION

In recent years, cloud computing is gaining much momentum in the IT industry. Especially, we have seen the dramatic growth of public clouds, in which the computing resources can be accessed by the general public. Advancing the field of health informatics has been listed as one of the engineering grand challenges for the current century. Activities in this field include acquiring, controlling, and using biomedical information, from personal level to global levels, to improve the quality and efficiency of medical care and the response to widespread public health emergencies. Predominantly, in the personal level, biomedical engineers envision "a new system of distributed computing tools that will collect authorized medical data about people and store it securely within a network designed to help deliver quick and efficient care. In this direction, several technological advances and new concepts, such as medical devices, Body Area Networks, pervasive wireless broadband communications and Cloud computing are enabling advanced mobile health-care services that benefit both patients and health professionals. Especially, they enable the development of a system to perform remote real-time collection, distribution and analysis of medical data for the purpose of managing chronic conditions and detecting health emergencies. The key problem of storing encrypted data in the cloud lies in revoking access rights from users. A user whose authorization is revoked will still retain the keys issued previously, and thus can still decrypt data in the cloud. This solution will lead to a performance bottleneck, particularly when there are frequent user revocations [1].

In such a remote mHealth monitoring system, a client could arrange portable sensors in wireless body sensor networks to collect various physiological data, such as blood pressure (BP), breathing rate (BR), Electrocardiogram (ECG/EKG),

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

peripheral oxygen saturation (SpO) and blood glucose. Such physiological data are sent to a central server, which could run various web medical applications on these data to return timely guidance to the client[2].

Besides, the current trend is more focused on protection against intrusions while there is little effort on protecting clients from business collecting private information. Many companies have significant commercial interests in collecting clients' private health data [3] and sharing them with either insurance companies, research institutions or the government agencies. The collected information from an mHealth monitoring system could contain clients' personal physical data such as their heights, weights, blood types, and ultimate personal identifiable information such as their fingerprints and DNA profiles [4].

Another major problem in addressing security and privacy is the computational workload involved with the cryptographic techniques. With the presence of cloud computing services, it will be wise to shift thorough computations to cloud servers from mobile devices. However, achieving this effect without compromising privacy and security becomes a great challenge, which should be suspiciously investigated. As an important remark, our design here mainly focuses on insider attacks, which could be provided by either malicious or nonmalicious insiders. For instance, the insiders could be unhappy employees or healthcare workers who enter the healthcare business for criminal purpose [5], [6]. It was reported that 32% of medical data breaches in medical establishments between January 2007 and June 2009 were due to insider attacks [7], and the incident rate of insider attacks is rapidly increasing [7]. The insider attacks have cost the victimized institutions much more than what outsider attacks have caused [8]. Furthermore, insider attackers are generally much harder to deal with because they are generally sophisticated professionals or even criminal rings who are adept at escaping intrusion detection [6]. On the other hand, while outsider attacks could be easily prevented by directly adopting cryptographic mechanisms such as encryption, it is nontrivial to design a privacy preserving mechanism against the insider attacks because we have to balance the privacy constraints and maintenance of normal operations of mHealth systems.

We integrate the recently proposed outsourcing decryption technique [9] into the underlying multidimensional range queries system to shift clients' computational complexity to the cloud without revealing any information on either clients' query input or the decrypted decision to the cloud. We recommend a further improvement, which is most important to our final scheme. It is based on a new alternative key private proxy reencryption scheme, in which the company only needs to accomplish encryption once at the setup phase while shifting the rest computational tasks to the cloud without compromising privacy, additionally reducing the computational and communication burden on clients and the cloud[10].

II. RELATED WORK

A. Mobile Cloud for Assistive Healthcare (MoCAsH)

This paper proposes a Mobile Cloud for Assistive Healthcare infrastructure. The infrastructure addresses the limitations of our earlier Active Grid infrastructure, invoke Cloud computing features such as user easy access, elasticity of resources demands, scalability of infrastructure, and metered usage and accounting of resources. The innovative infrastructure also addresses a number of issues with current Cloud architecture including some security and privacy issues, data protection and ownership. P2P paradigm is deployed to federate clouds that may belong to different administrators to address security, data protection and ownership. Part of the infrastructure has been implemented or migrated from the Active Grid [11].

B. The Era of Cloud Computer

Cloud-Computing helps provide the best efficiency for human beings, and it presents acquisition (user interface service), business (marketing driven usage), access (internet & intranet), and technology (unlimited, dynamic and flexible). For example, the heart beat detection can be detected by the portable sensors which typically send the health information though the RFID, gather into the media gateway, and then upload it to the public server system. Within a few seconds, the animated heart graphic with the calculated data soon replies back to the wireless network gateway, displaying the 3D graphics of heart in order to prevent the heart stroke or monitor diseases. All this concert is going through the wireless RF methodology, and its arithmetic process is finished by the remote computing servers that decrease the loading of mobile

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

media devices. The remarkable value is the lowest cost for common users and the capability to provide the best medical care from the integration of the cyber system [12].

C. A Cloud Based Web Analysis and Reporting of Vital Signs

The solution was built by converting an ordinary stethoscope into a digital one by implanting a Bluetooth microphone in the stethoscope ear piece. This enables a smart phone to record and store stethoscope audio signal. A Matlab program is written to demonstrate analysis of audio recording. The program contains a set of configuration parameters that can be customized based on patient conditions and recording environment. The program analyzes the signal to extract S1 and S2 timing instants. Before analysis, the noise is reduced by passing the signal through filter that removes frequency bands outside the signal range. A new algorithm is presented based on two passes search of signal peaks. The paper also presents a new approach for visualizing regularity of heart beats by fitting the measured S1 and S2 timing and plotting norms of residues [13].

D. Leveraging Mobile Cloud for Telemedicine

Leveraging the modern advances in mobile technologies and cloud computing, telemedicine is on the limit of a substantial transformation that will make stronger the effectiveness and efficiency of healthcare delivery.

In this paper, we present a preliminary performance study of mobile cloud to demonstrate its potential in performing continuous health monitoring in daily life and achieving higher diagnostic accuracy. Our findings also unveil the limitations of existing mobile devices in performing telemedicine by themselves. As shown in Fig: 2.1 mobile devices can be used to acquire various physiological signals from a set of ambient/body sensors. To alleviate intensive computations and extend the battery life of mobile devices, the acquired physiological signals will be transferred to a cloud service environment to perform desired, computation-intensive algorithmic signal processing. The processed results, recognized abnormalities, or analytical alarms will be automatically archived in the cloud or sent to the mobile devices owned by patients, physicians, or emergency teams. This application mode can be of particular significance to patients whose physiological signals need to be monitored continuously [14].

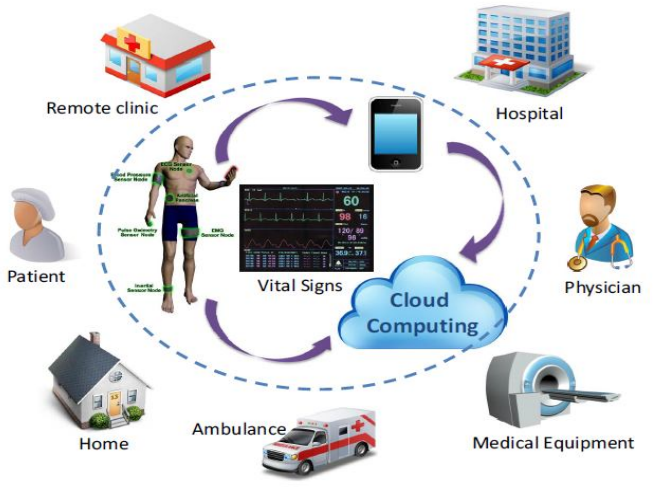

Fig: 2.1 Telemedicine based on Mobile Cloud Medical Monitoring.

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

III. IMPORTANT CRYPTOGRAPHIC BUILDING BLOCKS

Many encryption schemes are used in cloud for security. These algorithms are Homomorphic Encryption, Private Key Proxy re-encryption ,Attribute based encryption, Outsourcing Decryption scheme and triple-DES encryption schemes are given below.

1. Homomorphic Encryption:

Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. The homomorphic encryption describes the transformation of one data set into another while preserving relationships between elements in both sets. Uses of Homomorphic encryption is expected to play an important part in cloud, allowing companies to store encrypted data in a public cloud and take advantage of the cloud providers analytic services[15][16].

Intuitively, for homomorphic encryption HEnc(.), given two encrypted messages HEnc(m1) and HEnc(m2) , the encryption of the addition of the two underlying messages can be computed as follows: HEnc(m1+m2)= HEnc(m1) *HEnc(m2) , where * is the corresponding operation in the ciphertext space. A typical homomorphic encryption scheme was proposed by Paillier cryptosystem [17], [18].

2. Private Key Proxy re-encryption:

We initiate by specifying the input/output behavior of a proxy re-encryption scheme [19]. For simplicity, we consider a definition for unidirectional, single-hop PREs. By single-hop, we indicate that only original ciphertexts (and not re-encrypted ciphertexts) can be re-encrypted. One might extend the basic notions of our security and key privacy definitions for multi-hop schemes, but this requires a more involved definition of when users become distort, and may be more appropriate for CCA-secure schemes.

A unidirectional, single-hop, proxy re-encryption scheme is a tuple of algorithms $\prod$= (Setup, KeyGen, ReKeyGen, Enc, ReEnc, Dec) for message space M:

- Setup(1^k) → PP. On input security parameter 1^k, the setup algorithm outputs the public parameters PP.
- KeyGen(PP) → (pk, sk). On input public parameters, the key generation algorithm KeyGen outputs a public key pk and a secret key sk.
- ReKeyGen(PP, sk_i, pk_j) → $rk_{i\rightarrow j}$. Given a secret key ski and a public key pkj , where $i \neq j$, this algorithm outputs a unidirectional re-encryption key $rk_{i\rightarrow j}$. The restriction that $i \neq j$ is provided as re-encrypting a message to the original recipient is impractical.
- Enc(PP, pk_i,m) →C_i. On input a public key pki and a message m Ɛ M, the encryption algorithm outputs an original ciphertext C_i.
- ReEnc(PP, $rk_{i\rightarrow j}$,C_i) →C_j . Given a re-encryption key from i to j and an original ciphertext for i, the re-encryption algorithm outputs a ciphertext for j or the error symbol ⊥.
- Dec(PP, sk_i,C_i) →m. Given a secret key for user i and a ciphertext for i, the decryption algorithm Dec outputs a message m Ɛ M or the error symbol ⊥.

A unidirectional, single-hop PRE scheme $\prod$ is correct with respect to domain M if:

i. For all (pk, sk) Ɛ KeyGen(PP) and all m Ɛ M, it holds that Dec(PP, sk, Enc(PP, pk,m)) = m.

ii. For all pairs (pk_i, sk_i), (pk_j , sk_j) Ɛ KeyGen(PP) and keys $rk_{i\rightarrow j}$ Ɛ ReKeyGen(PP, sk_i, pk_j), and m Ɛ M, it holds that Dec(PP, sk_j , ReEnc(PP, $rk_{i\rightarrow j}$, Enc(PP, pk_i,m))) = m.

3. Attribute Based Encryption:

Attribute based encryption (ABE) , a recently invented one-to-many public-key cryptography, has the possible to enforce the fine-grained access policies for large-scale systems. In attribute based encryption data are associated with attributes. Access policies, defined on attributes, are compulsory within the encryption procedure. Different form traditional

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

broadcast encryption, ABE offers the ability to encrypt data without exact knowledge of the receiver set. In this sense the concept of ABE is closely related to Role-Based/Attribute-Based access control and suitable for large-scale application. In attribute-based encryption (ABE), user secret key revocation is also a challenge issue[20].

4. Outsourcing Decryption:

We give new methods for efficiently and securely outsourcing decryption of ABE ciphertexts. The core change to outsourceable ABE systems is a modified Key Generation algorithm that produces two keys. The first key is a short El Gamal [21] type secret key that must be kept by the authorized user. The second key called as a TK(transformation key), that is shared with a proxy (and can be publicly distributed). If the proxy then receives a ciphertext CT for a function f for which the user's credentials satisfy, it is then able to use the key TK to transform CT into a simple and short El Gamal ciphertext CT′ of the same message encrypted under the user's key SK. The user is then able to decrypt with one simple exponentiation. Our system is secure against any malicious proxy[22].

Let S represent a set of attributes, and A an access structure. For generality, we will define (I_{enc}, I_{key}) as the inputs to the encryption and key generation function respectively. In a CP-ABE scheme (I_{enc}, I_{key}) = (A,S), while in a KP-ABE scheme we will have (I_{enc}, I_{key}) = (S,A). A CP-ABE (resp. KP-ABE) scheme with outsourcing functionality consists of five algorithms:

- Setup(λ,U).The setup algorithm takes security parameter and attribute universe description as input. and outputs are public parameters PK and a master key MK.
- Encrypt(PK,M,I_{enc}).The encryption algorithm takes as input the message M, public parameters PK, and an access structure (resp. attribute set) I_{enc}. It outputs the ciphertext CT.
- $KeyGen_{out}$ (MK, I_{key}).The key generation algorithm takes as input the master key MK and an attribute set (resp. access structure) I_{key} and outputs a private key SK and a transformation key TK.
- Transform(TK,CT).The ciphertext transformation algorithm takes as input a transformation key TK for I_{key} and a ciphertext CT that was encrypted under I_{enc}. It outputs the partially decrypted ciphertext CT′ if S Ɛ A and the error symbol ⊥ otherwise.
- $Decrypt_{out}$ (SK,CT′).The decryption algorithm takes as input a private key SK for I_{key} and a partially decrypted ciphertext CT′ that was originally encrypted under I_{enc}. It outputs the message M if S Ɛ A and the error symbol ⊥.

5. Triple-DES algorithm:

Triple Data Encryption algorithm is an encryption algorithm that is based on the Data Encryption Standard encryption algorithm. The size of block is 64 bits and the key sizes are 168, 112, or 56 bits. The input key sizes are 3 64 bit keys, which are shortened to 56 bits because of the internal key scheduler. The block of data is encrypted 3 times with each of the keys according to the keying options:

Keying Option 1: All the keys are independent.
Keying Option 2: K1 & K2 are independent and K3 = K1.
Keying Option 3: All keys are identical (i.e. K1=K2=K3).

It reinforces DES by expanding the key space which is it's main weakness and protects itself from brute force attacks. Today TDEA is widely used.

Triple DES uses a "key bundle" which comprises three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits).

The encryption algorithm is: ciphertext = $E_{K3}(D_{K2}(E_{K1}(plaintext)))$

i.e., DES encrypt plaintext with K_1, and DES decrypt with K_2, finally DES encrypt with K_3.

Decryption is the reverse: plaintext = $D_{K1}(E_{K2}(D_{K3}(ciphertext)))$

i.e., decrypt ciphertext with K_3, and encrypt with K_2, finally decrypt with K_1.

In each case the middle operation is reverse of the first and last. This algorithm mainly improves the strength of the security [23].

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. PROBLEM DEFINITION

In our existing system with the pervasiveness of Cloud-assisted networks the Healthcare which extends the operation of Healthcare provider into a pervasive environment for better health monitoring is not governed properly by the trust authority. The privacy disclosure and the high reliability of distributed system over single cloud process and transmission in Healthcare emergency monitoring is not an efficient user-centric privacy access control on CAM. For healthcare infrastructure there may be several serious issues concerning security, data protection and ownership and quality of services need to be resolved before Cloud computing can be widely adopted. This analysis exhibit the key for an authenticated token providence in the Cloud for Assistive Healthcare as an infrastructure for assistive healthcare. Healthcare business with criminal purposes may affect our system which is a drawback in our existing algorithm, and also Several serious issues concerning security and data protection paradigm [10].

V. PROPOSED WORK

In this paper, propose a secure and privacy-preserving opportunistic computing framework for the Healthcare Emergency. To improves the performance evaluation via extensive simulations and parallel database. We can provide high reliability and transmission for minimizing the privacy disclosure .Cloud computing can be widely adopted to address these concerns, and this paper propose a new solution that includes in a cloud platform designed to deal with those issues that are relevant for an assistive healthcare infrastructure.

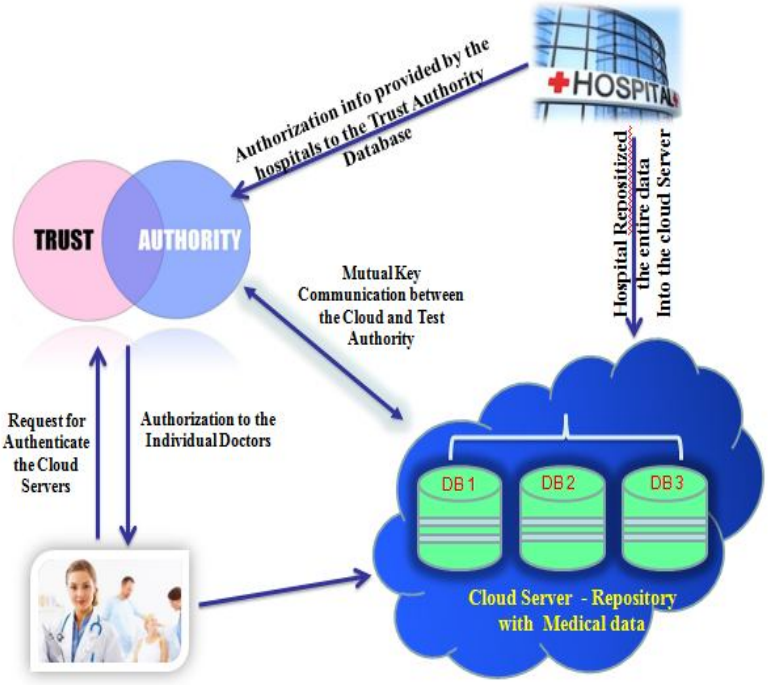

Fig: 5.1 Architecture diagram

Our design of the proposed system consists of four parties: the cloud server (simply the cloud), the company which provides the mHealth monitoring service (i.e., the healthcare service provider), and the individual clients (simply clients),

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

and a trust authority (TA), as shown in Fig: 5.1. The company stores its encrypted monitoring data in the cloud. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into cloud. TA is responsible for distributing private keys to clients and collecting service fees from clients according to a certain business model such as "pay-per-use" model. TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual business interest with the company. In the following, we will briefly introduce steps for this paper. We only illustrate the functionality of these components here. Because the detailed input and output of those steps might vary in different schemes, we leave more details wherever needed.

Fig: 5.2 shows First step the company collect the patients, doctors and hospitals information's, which is encrypted under the respective triple-DES algorithms. Then the company will deliver the resulting ciphertext and its company index to the cloud, which corresponds to the algorithm in the context.

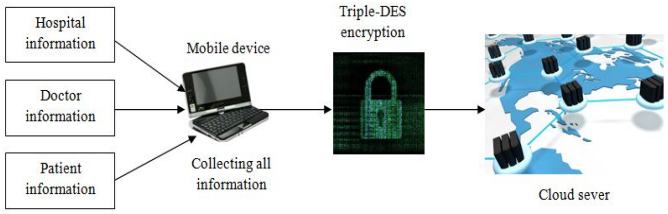

Fig: 5.2 Information storing in cloud

Fig: 5.3 shows the clients request the particular patient information from the cloud server. Then the client sends the company index to TA, and the trust authority (TA) provides authorization to the requested individual clients. After that TA generates the token and provided to the particular client.

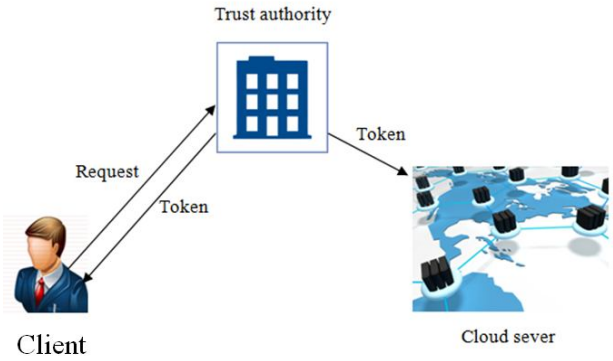

Fig: 5.3 Token Generations

Finally, the client delivers the token to the cloud, which runs the phase. The cloud using the parallel concept to completes the major computationally intensive task for the client's decryption (triple-DES) and returns the partially decrypted ciphertext to the client. The client then completes the remaining decryption (triple-DES) task after receiving the partially decrypted ciphertext and obtains its decryption result. These are shown in fig: 5.4. The cloud obtains no useful information on either the client's private key input or decryption result after running the phase.

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

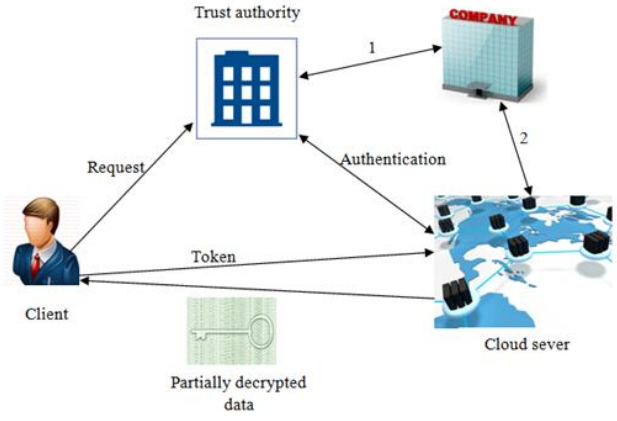

Fig: 5.4 Partial decryption processes

- Advantages of Proposed system:
  1. The Security level is increased in the health care monitoring solution.
  2. Using the parallel computing concept to increase the performance.

VI. CONCLUSION

It is cost prohibitive for many individual healthcare systems to support the investment in the equipment, technology, personnel, and ongoing training required to deliver the highest level of data security. To protect the clients' privacy, we apply the triple-DES encryption. To reduce the decryption complexity, we apply recently anticipated decryption outsourcing with privacy protection to shift clients pairing computation to the cloud server. We also introduce the parallel computing concept to accessing the database. So the accessing time are reduced. Finally, to enable resource-constrained small companies to participate in mHealth business, our design helps them to shift the computational burden to the cloud by applying newly developed key private proxy reencryption technique. Our system has been shown to achieve the design objective.

VII.FUTURE ENHANCEMENT

It can also secure health care information in the form of images in an encrypted form once after getting authenticated through trust authority. Preserving health care information in an globalised way can also be helpful in pattern matching strategy to analyze new diseases.

REFERENCES

[1] http://en.wikipedia.com.
[2] A. Tsanas, M. Little, P. McSharry, and L.Ramig, "Accurate telemonitoring of parkinson's disease progression by noninvasive speech tests," IEEE Trans. Biomed. Eng., vol. 57, no. 4, pp. 884–893, Apr. 2010.
[3] N. Singer, "When 2 2 equals a privacy question," New York Times, Oct. 18, 2009 [Online]. Available: http://www.nytimes.com/2009/10/18/business/18stream.html.
[4] P. Baldi, R. Baronio, E. D. Cristofaro, P. Gasti, and G. Tsudik, "Countering gattaca: Efficient and secure testing of fully-sequenced human genomes," in Proc. ACM Conf. Computer and Communications Security, 2011, pp. 691–702.
[5] P. Institute, Data Loss Risks During Downsizing, 2009.

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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[6] P. Dixon, "Medical identity theft: The information crime that can kill you," in Proc. The World Privacy Forum, 2006, pp. 13–22.
[7] K. E. Emam and M. King, The Data Breach Analyzer 2009 [Online].Available: http://www.ehealthinformation.ca/dataloss.
[8] E. Shaw, K. Ruby, and J. Post, "The insider threat to information systems: The psychology of the dangerous insider," Security Awareness Bull., vol. 2, no. 98, pp. 1–10, 1998.
[9] M. Green, S. Hohenberger, and B.Waters, "Outsourcing the decryption of abe ciphertexts," in Proc. Usenix Security, San Francisco, CA, USA, Aug. 8–12, 2011, pp. 34–49.
[10] Huang Lin, Jun Shao, Chi Zhang, and Yuguang Fang, Fellow "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring," IEEE transactions on information forensics and security, vol. 8, no. 6, june 2013.
[11] Doan B. Hoang, Lingfeng Chen," Mobile Cloud for Assistive Healthcare (MoCAsH)," 2010 IEEE Asia-Pacific Services Computing Conference.
[12] Chih-Chin Yang, J. T. Huang," The Era of Cloud Computer thru Bio-Detecting and Open-Resources to Achieve the Ubiquitous Devices," 2012 International Symposium on Computer, Consumer and Control.
[13] Yazan A Alqudah, Esam A AlQaralleh," A Cloud Based Web Analysis and Reporting of Vital Signs," IEEE 2012.
[14] Xiaoliang Wang, Qiong Gui, Bingwei Liu, Yu Chen, and Zhanpeng Jin," Leveraging Mobile Cloud for Telemedicine: A Performance Study in Medical Monitoring," 2013 39th Annual Northeast Bioengineering Conference.
[15] Pierluigi Failla, Riccardo Lazzeretti, Ahmad-Reza Sadeghi, and Thomas Schneider, Privacy-Preserving ECG Classification With Branching Programs and Neural Networks, IEEE transactions on information forensics and security, vol. 6, no. 2, june 2011.
[16] http://en.wikipedia.com.
[17] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. UROCRYPT, 1999, pp. 223–238.
[18] I. Damgard and M. Jurik, "A generalisation, a simplification and some applications of paillier's probabilistic public-key system," in Public Key Cryptography, ser. Lecture Notes in Computer Science, K. Kim, Ed. New York, NY, USA: Springer, 2001, vol. 1992, pp. 119–136.
[19] Giuseppe Ateniese, Karyn Benson, Susan Hohenberger," Key-Private Proxy Re-Encryption," January 22, 2009.
[20] Shuchengyu, Data sharing on untrusted storage with Attribute-based encryption,july2010.
[21] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In CRYPTO, pages 10–18, 1984.
[22] Matthew Green, Susan Hohenberger, Brent Waters, "Outsourcing the Decryption of ABE Ciphertexts," University of Texas at Austin.
[23] http://en.wikipedia.org/wiki/Triple_DES.