www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 1 January 2015, Page No. 9999-10004

Improving **Security and Reduce Overhead in Mobile Health Monitoring**

***Dr.N.Tajunisha*[1], *V.Archana*[2]**

[1]Department of Computer Science,
Sri Ramakrishna College of Arts and Science for Women,
Coimbatore, India
tajkani@gmail.com

[2]Department of Computer Science,
Sri Ramakrishna College of Arts and Science for Women,
Coimbatore, India
archumca2010@gmail.com

Abstract: Cloud-assisted mobile health (mHealth) monitoring, which applies the prevailing mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a revolutionary approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could deter the wide adoption of mHealth technology. This paper is to provide better privacy and security in a mobile health monitoring system and also to protect the privacy of the involved parties and their data. Moreover, a newly proposed Diffie Hellman algorithm and Homomorphic encryption technique are adapted. Finally, the security and trust worthiness demonstrates the effectiveness of our proposed design. One service provider operates the encryption and decryption system while other providers operate the storage and application systems, according to the core concept of the proposed Health monitoring model. Our work further includes suggestions for multi-party Service- Level Agreement (SLA) suitable for use in the proposed Health monitoring model.

Keywords: Mobile Health (mHealth), Healthcare, Privacy.

1. Introduction

Cloud computing is Internet based development and use of computer technology. In concept, it is a paradigm shift whereby details are abstracted from the users who no longer need knowledge of, expertise in, or control over the technology infrastructure "in the cloud" that supports them. It typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet.

The term cloud is used as a metaphor for the Internet, based on how the Internet is depicted in computer network diagrams and is an abstraction of the underlyinginfrastructure it conceals. Typical cloudcomputing services provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers.

The five essential characteristics of the NIST (National Institute of Standards and Technology)definition are shown below. They are On-Demand Self-Service, Broad Network Access, Resource Pooling, Rapid Elasticity, Measured Service. Some Issues And Challenges are Security and Privacy, Service Delivery and Billing, Interoperability and Portability, Reliability and Availability, Performance and Bandwidth Cost.

Health Monitoring

A secured patient healthcare monitoring in cloud infrastructure which helps to keep the communication between doctor and patient confidential. The cloud server respects the privacy of a patient and keeps it secured by protecting the medical history of the patient. The main objective of the proposed system is preserving the privacy of the information ensuring that this information cannot be misused.

Problem Definition

Decryption complexity is very high in client side.It is not suitable for high level of trust in the methods by which service providers protect their data. High overhead for small scale network. Although cloud-assisted mHealth monitoring could offer a great opportunity to improve the quality of healthcare services and potentially reduce healthcare costs, there is a stumbling block in making this technology a reality. The privacy issue is tackled with anonymization technique such as k-anonymity or l-diversity. Another major problem in addressing security and privacy is the computational workload involved with the cryptographic techniques. With the presence of cloud computing facilities, it will be wise to shift intensive computations to cloud servers from resource-constrained mobile devices. However, how to achieve this effectively without compromising privacy and security becomes a great challenge, which should be carefully investigated.

2. Background Study

M.Barni and R.Lazzeretti et al [11], says that privacy protection is a crucial problem in many biomedical signal processing applications. So that there should be a particular attention has been given for secure multiparty computation techniques for processing biomedical signals, where by non-trusted parties are able to manipulate the signals although they are encrypted. The authors focused on the development of a privacy preserving automatic diagnosis system thereby a remote server classifies a biomedical signal without getting any information about the signal. This paper uses a highly efficient version of cryptographic primitives which gives a good efficiency from both communication and computational complexity.

M.Layouni and K.Verslype et al [13], proposed a privacy preserving telemonitoring protocol for healthcare. Patients are still resisting the idea of medical telemonitoring because privacy may not be properly protected. The protocol used in this paper allows patients to selectively manifest their identity information and guarantees that no health data is sent to the monitoring Centre without the patient's approval. The approval process needs only an initial configuration by the patient.

J.Brickell and D.Porter et al [4], they presented an efficient protocol for privacy-preserving evaluation of diagnostic programs, represented as binary decision trees or branching programs. The protocol applies a branching diagnostic program with classification labels in the leaves to the user's attribute vector. The user learns only the label assigned by the program to his vector; the diagnostic program itself remains secret. The program's owner does not learn anything. Their construction is significantly more efficient than those obtained by direct application of generic secure multi-party computation techniques. They use their protocol to implement a privacy-preserving version of the Clarify system for software fault diagnosis, and demonstrate that its performance is acceptable for many practical scenarios.

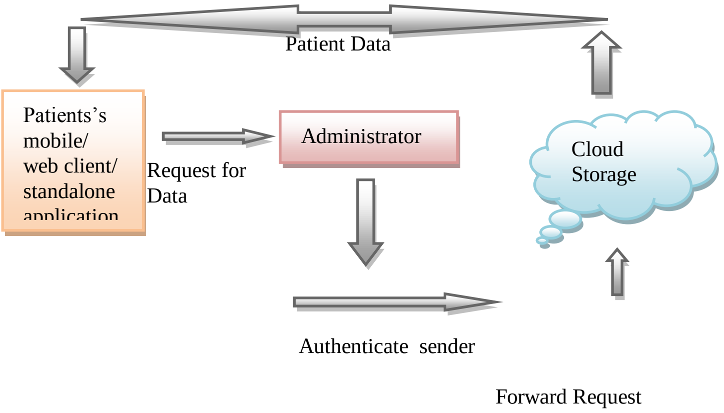
K.Benson and S.Hohenberger et al [1], they proposed a key-private (or anonymous) re-encryption keys as an additional useful property of PRE schemes. Proxy re-encryption (PRE) allows a proxy to convert a cipher text encrypted under one key into an encryption of the same message under another key. The proxy should not be able to learn the keys of the participants or the content of the messages it re-encrypts. However, in all prior PRE schemes, it is easy for the proxy to determine between which participants a re-encryption key can transform cipher texts. This can be a problem in practice. In a secure distributed file system, content owners may want to use the proxy to help re-encrypt sensitive information without revealing to the proxy the identity of the recipients.

A.Sahai and B.Waters et al [15], they introduced a new type of Identity-Based Encryption (IBE) scheme that is Fuzzy Identity-Based Encryption. In Fuzzy IBE the author view an identity as set of descriptive attributes. Additionally, the author indicates that Fuzzy-IBE can be used for a type of application that we term "attribute-based encryption". IBE schemes are both error-tolerant and secure against collusion attacks.

3. Proposed Method

Enterprises usually store data in internal storage and install firewalls to protect against intruders to access the data. In cloud computing, the data will be stored in storage provided by service providers. Service providers must have a viable way to protect their client's data, especially to prevent the data from disclosure by unauthorized insiders. Storing the data in encrypted form is a common method of data privacy protection. If a cloud system is responsible for both tasks of storage and encryption/decryption of data, the system administrators may simultaneously obtain encrypted data and decryption keys. This allows them to access information without authorization and thus poses a risk to information privacy. This study proposes an efficient encryption and decryption service for cloud computing by separating the encryption and decryption service from the storage service of data. An ideal service utilizes three cloud systems, including an encryption and decryption system, a storage system, and a health application system. One service provider operates the encryption and decryption system while other providers operate the storage and application systems, according to the core concept of the proposed monitoring model.

Architecture Diagram



Methodology

Step 1: Dataset are taken from patient's record.

Step 2: Data owner, then encrypts the user's data and stored in the cloud.

Step 3: When the user logged into the cloud, key is generated, which is generated by the key distribution centre using Diffie Hellman Algorithm.

Step 4: Then user enters to the login page and checking for the authentication, whether the users have the authorization or not. Then the user enters their current data like Blood Pressure, Glucose Level, Breathing Rate, ECG (ElectroCardioGram), SpO (Peripheral Oxygen Saturation).

Step 6: Decision Tree will be constructed and the data are traversed through the Decision Tree, to get the accurate result.

Step 7: When the data are matched with the Decision Tree Structure, then the accurate report will be given to the user.

Step 8: Then the report produced by the data owner is opened in an encrypted format.

Step 9: To decrypt the report, Homomorphic Encryption Algorithm is used to retrieve the data.
Step 10: Then the user will receive their original report.

Cloud Setup

Cloud setup is developed by using java. The cloud server nothing but the cloud, the industry who gives the mHealth monitoring service nothing but providers of healthcare service, the individual users and third party or a semi-trusted authority (TA). The industry preserves its encrypted monitoring information or program in the server of cloud. Individual users gather their medical information and preserve them in their cell phones, which then manipulate information into attribute vectors. The attribute vectors are given to the monitoring program as inputs in the cloud server via a smart phone or a mobile device. A semi-trusted authority or third party is responsible for sharing private keys to the individual users and gathering the service fee from the users as per that a certain business model like as pay-as-you-go. The TA or third party can be under taken as a management agent or a collaborator for a company or lots of companies and thus distributes certain level of mutual interest with the industry.

Diffie Hellman Algorithm

The Diffie–Hellman key exchange algorithm solves the following dilemma. Alice and Bob want to share a secret key for use in a symmetric cipher, but their only means of communication is insecure. Every piece of information that they exchange is observed by their adversary Eve. How is it possible for Alice and Bob to share a key without making it available to Eve? At first glance it appears that Alice and Bob face an impossible task. It was a brilliant insight of Diffie and Hellmanthat the difficulty of the discrete logarithm problem for Bob to agree on a large prime p and a nonzero integer g modulo p. Alice and Bob make the values of p and g public knowledge; for example, they might post the values on their web sites, so Eve knows them, too. For various reasons to be discussed later, it is best if they choose g such that its order in F ∗p is a large prime. (See Exercise 1.31 for away of finding such a g.)The next step is for Alice to pick a secret integer a that she does not reveal to anyone, while at the same time Bob picks an integer b that he keeps secret. Bob and Alice use their secret integers to compute

$$\underbrace{A \equiv g^a \pmod p} \quad \text{and} \quad \underbrace{B \equiv g^b \pmod p}$$

They next exchange these computed values, Alice sends A to Bob and Bob sends B to Alice. Note that Eve gets to see the values of A and B, since they are sent over the insecure communication channel. Finally, Bob and Alice again use their secret integers to compute

$$\underbrace{A' \equiv B^a (\mathrm{mod}\ p)} \quad \text{and} \quad \underbrace{B' \equiv A^b (\mathrm{mod}\ p)}$$

The values that they compute, A0 and B0 respectively, are actually the same, since
$A' \equiv B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \equiv B'(\mathrm{mod}\ p)$
This common value is their exchanged key. The Diffie–Hellman key exchange algorithm is summarized.

Public Paramater Creation
A trusted party chooses and publishes a (large) prime p and an integer g having large prime order in F^*p.

Private Computations Alice	Bob
Choose a secret integer a. Compute A ≡ g^a(mod p)	Choose a secret integer b. Compute B ≡ g^b(mod p)

Further Private Computations Alice	Bob
Compute the number B^a(mod p)	Compute the number A^b(mod p)
The shared secret value is Ba ≡ $(g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b$(mod p)	

Public Exchange of Values		
Alice sends A to Bob	⟶	A
B	⟵	Bob sends B to Alice

Alice and Bob agree to use the prime p = 941 and the primitive root g = 627. Alice chooses the secret key a = 347 and computes A = 390 ≡ 627^{347} (mod 941). Similarly, Bob chooses the secret key b = 781 and computes B = 691 ≡ 627^{781} (mod 941). Alice sends Bob the number 390 and Bob sends Alice the number 691. Both of these transmissions are done over an insecure channel, so both A = 390 and B = 691 should be considered public knowledge. The numbers a = 347 and b = 781 are not transmitted and remain secret. Then Alice and Bob are both able to compute the number470 ≡ $627^{347\cdot781}$ ≡ A^b ≡ B^a(mod 941), so 470 is their shared secret.Suppose that Eve sees this entire exchange. She can reconstitute Alice's and Bob's shared secret if she can solve either of the congruences

$$627^a \equiv 390 \ (\mathrm{mod}\ 941) \text{ or } 627^b \equiv 691 \ (\mathrm{mod}\ 941),$$

since then she will know one of their secret exponents. As far as is known, this is the only way for Eve to find the secret shared value without Alice's or Bob's assistance. Of course, our example uses numbers that are much too small to afford Alice and Bob any real security, since it takes very little time for Eve's computer to check all possible powers of 627 modulo 941. Current guidelines suggest that Alice and Bob choose a prime *p* having approximately 1000 bits (i.e.,*p* ¼ 21000) and an element *g* whose order is prime and approximately *p*=2. Then Eve will face a truly difficult task.In general, Eve's dilemma is this. She knows the values of *A* and *B*, so she knows the values of $g^a$and g^b. She also knows the values of *g* and *p*, so if she can solve the DLP, then she can find *a* and *b*, after which it is easy for her to compute Alice and Bob's shared secret value *gab*. It appears that Alice and Bob are safe provided that Eve is unable to solve the DLP, but this is not quite correct. It is true that one method of finding Alice and Bob's shared value is to solve the DLP, but that is not the precise problem that Eve needs to solve. The security of Alice's and Bob's shared key rests on the difficulty of the following, potentially easier, problem. Definition. Let *p* be a prime number and *g* an integer. The Diffie Hellman Problem (DHP) is the problem of computing the value of g^{ab} (mod *p*) from the known values of g^{a}(mod *p*) and g^{b}(mod *p*). It is clear that the DHP is no harder than the DLP. If Eve can solve the DLP, then she can compute Alice and Bob's secret exponents *a* and *b* from the intercepted values $A = g^{a}$ and $B = g^{b}$, and then it is easy for her to compute their shared key *gab*. (In fact, Eve needs to compute only one of *a* and*b*.)

Decision Tree Contrution

In this work the decision about the client information is taken effectively by constructing the decision tree. Initially the decision tree construction will be done in order to make the decision for user query with more accuracy. Then the trust value of the cloud service providers is calculated to make sure the satisfaction of users. Whenever the user submits the query, the answer will be replied with the help of the decision tree. The medical data access to the user is provided by using the algorithm call Improved Key Private Proxy Re-encryption.

The decision tree construction is done as like follows: Assume there is a data set D = {t1, t2, …,t_N}, where $t_i \le \vec{x}, c > \in \vec{x} \times C.$ $\vec{x} \overset{def}{=} < x1,\ldots.,xm >$ is the data associated with the instance and c is the class label. Each xj is called a field or attribute of the data instance. $\vec{X} \overset{def}{=} X_1,\ldots..,X_m$ is the domain of data instances and Xj is the domain of the attribute xj. The domain of an attribute can either be a categorical set, such as {red, blue, yellow}, or a numerical set, such as [1,…,100]. C is the domain of class labels.

The classification problem is to find a computable function f : X→C, such that for any instance t extracted from the same distribution as D, f (t, x) will give an accurate as possible prediction of t.c. Decision tree classifiers are frequently used for achieving the above functionality. A decision tree classifier is typically a binary tree, where every non-leaf node t is associated with a predicate p. A predicate partition the set of data instances associated with node based upon the value of a particular attribute xi. If xi belongs to a categorical domain, p is the subset predicate, for example p =true, if xi ϵ {red, blue}. If xi belongs to a numerical domain, p is a range predicate, for example, p =true if xi <= 50. Here 50 is the cutting or the split point.

Trust Value Calculation

Trust value is defined as “the firm belief in the capability of an entity to act consistently, securely and reliably within a specified context”. And also, the trust is the composition of multiple attributes such as reliability, honesty, truthfulness, dependability, security, competence, timeliness, Quality of Service (QoS) and Return on Investment (ROI) in the context of an environment.

As it is mentioned above, we compute trust from the credentials of the resource provider. We consider the credential attributes such as availability, reliability, turnaround efficiency, and data integrity to compute trust value.

Availability

Availability is the degree to which a system or component is operational and accessible when required for use. In software engineering, availability is measured in terms of mean time between failures and mean time to repair. When a job is submitted to a cloud resource, the resource is said to be unavailablein one of the following situations:

1. A part of service of the resource is denied to the user
2. The resource is shut down
3. The resource is too busy to process the job request.

Let us assume that R1, R2 … Rm are the cloud resources. For each k = 1, 2 … m, let Nk denote the number of jobs submitted to cloud resource Rk over a period T. Out of Nk jobs submitted to Rk, let Ak denote the number of jobs accepted by the resource Rk over the period T.

Availability of resource Rk (AV) = Ak / Nk

Reliability

Reliability is an important component of trust. It is also called success rate. Reliability is the ability of a system or component to perform its required functions under stated conditions for a specified period of time. Once a cloud resource accepts a job, how reliably does it complete the job? Reliability of a cloud resource is a measure of successful completion of accepted jobs by the cloud resource. Out of Ak jobs accepted by resource Rk, let Ck denote the number of jobs completed successfully by resource Rk over the period T.

Reliability of resource Rk (RE) = Ck / Ak

Data Integrity

A key issue that needs special attention in clouds is security. Data integrity is a broad term and it includes security, privacy and accuracy of the data. Security includes data safety and accuracy includes data precision. Data loss might happen due to poor network latency. Precision loss might happen due to obsolete computing infrastructure. Out of Ck jobs completed successfully by resource Rk, let Dk denote the number of jobs data integrity preserved by resource Rk over the period T.

Data integrity of resource Rk (DI) = Dk/ Ck

Turnarund Efficiency

The turnaround time is the difference between T4 and T1 (T4–T1). The actual turnaround timeis the exact time between the submission of a job by a user and the delivery of the completed job to the user. The promised turnaround timeis the expected time by a resource provider between the submission of a job and the delivery of the completed job. It is promised by the resource provider to the user in the SLA. This actual turnaround time is normally different from the turnaround time promised by the resource provider in the SLA. Turnaround Efficiency for a job by resource Rk =

$$\frac{\text{Promised turn around time by Rk in the SLA}}{\text{Actual Turn around time by Rk to complete the job}}$$

Turnaround efficiency is 1 if the promised turnaround time is greater than the actual turnaround time. Turnaround efficiency of a resource Rk (TE) is the average of turnaround efficiency over all the jobs submitted during the period T. Turnaround efficiency incorporates the Computing Power and Networking Speed (in general, Utilization). In addition, it also incorporates throughput which is the number of transaction per second.

Trust Value of a resource:

Trust Value of a resource =w1*AV+w2*RE+w3*DI+w4*TE.

where w1, w2, w3, and w4 are positive weights of the trust parameters such that w1+w2+w3+w4 = 1. The weights of the trust attributes are predetermined based on their priority. For example, w1 = 0.2, w2 = 0.2, w3 = 0.5, w4 = 0.1. In this example, data integrity is given the highest priority whereas turnaround efficiency is given the lowest priority.

Improved Key Private Proxy Reencryption

Setup

This algorithm performed by the TA, which runs the Setup algorithm of the proxy re-encryption scheme and publishes the respective system parameters.

Store

This algorithm is performed by the company. Let PRF (s_0, i) and PRF (s_1, i) be two pseudo random functions which take as inputs a secret key s_j, j ϵ {0,1} and an I, ie., PRF: $\{0, 1\}^{\lambda} * [1, N * k] \rightarrow \{0, 1\}^{C,C',}$ where N denotes the maximum number of the clients accessing the company's data in a time slot. The company first computes

$$\delta_{ij}^{(0)} = PRF(s_0, (i-1)*K+j), \delta_{ij}^{(1)} = PRF(s_1, (i-1)*k+j)$$

and $\delta_{ij} = \delta_{ij}^{(0)} + \delta_{ij}^{(1)}$, where j ϵ [1, k]. For jϵ [1, k], the company obtains all the identity representation set $S_{[0,\ tj+\delta ij]}$and $S_{[tj+\delta ij+1,\ max']}$

Let Q be a random permutation of the set [1, k] = (1, 2, ..,K) with Q[1] = 1. The company delivers PRF (s_0, .), {t_j + $\delta_{ij,}$ a_j|i ϵ [1, N], j ϵ [1, k]} and Q to TA, which computes the identity representation set as the company does.

For j ϵ [1, k], TA runs the ReKey (id1, id2, msk) algorithm on id_1 ϵ $S_{[0,\ tj+\delta ij]}$and id_2 ϵ $S_{[0,\ tj+\delta(i+1)j],}$ or id_1 ϵ S $_{[tj + \delta ij + 1,\ max']}$and id_2 ϵ S $_{[tj + \delta (i+1)j +1,\ Max'].}$ Although the respective two representation sets might not have the identical number of elements, the re-key generation process can simply start from the first identity element of both sets until the set containing fewer identities exhausts all its identity elements. TA then returns all the generated re-keys according to the permuted order Q[j] to the cloud.

Starting with p1, the company selects two symmetric keys $_{KQ[L(j)]}$, $k_{Q\ [R(j)]}$for each decision node pj whose children arennot leaf nodes. Then it runs the encryption algorithm Enc (id_1, $k_{Q[L(j)]}$ ‖ Q[L (j)]) and Enc (id_2, kQ[R(j)] ‖ Q [R(j)]), where id_1 ϵ S [0, t_j+δ_{ij}] and id2 ϵ $S_{[tj+\delta ij+1,\ max'],}$ respectively , using a semantically secure symmetric key encryption scheme. When pj is the parent node of the leaf nodes, the two symmetric are used to encrypt the information attached to the two leaf nodes.

TokenGen

To generate the private key for the attribute vector V = (v1, …, vn), the ith client first generates a public/ private key pair of a homomorphic encryption scheme, and sends the public key and HEnc (vj) to TA.

Query

The client delivers his index i to the cloud which will then return the respective cipher text. The client can either download all the cipher texts and transformation key and perform the rest decryption steps, or he could start to run Dec (sk_{id}, C_{id}), where id ϵ $S_{[0,\ t1+\delta i1]}$or $S_{[t1+\delta i1+1,\ max']}$to decrypt from p1 and then download the cipher text and the transformation key for the next node according to the decryption result.

User Revocation

User revocation can be easily achieved through a novel revocation list without generate new keys for each revocations. The unused keys are updated for remaining users after revocation. This method reduces the key generation cost very effectively. The privacy protection level is dynamically adjusted according to the trust worthiness of the cloud servers. The privacy protection level is avoiding unnecessary complex computation in privacy protection process.

4. Results Analysis

The performance evaluation of these works is done based on two metric. Those are time metric and cost metric. The comparison of existing work with the proposed work is shown in the following.

Time Performance

The time taken to retrieving the result for the client request is evaluated for the proposed methodology. The time complexity taken by the proposed method is compared with the existing methodologies are compared as in the following figure. The below graph proves that the processing time taken by the proposed methodology is lesser than the existing methodologies.

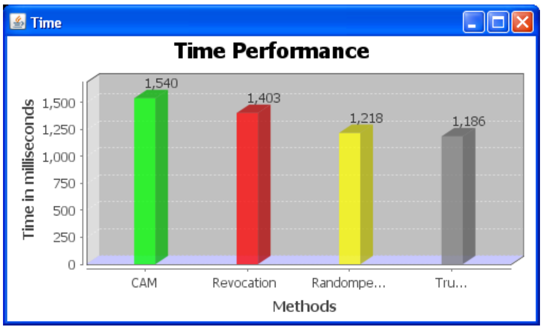


Figure1: Time Performance Comparison

Cost Performance

The cost of implementing the health care monitoring system may exceed based on the sensors used, the processing cost, etc.,

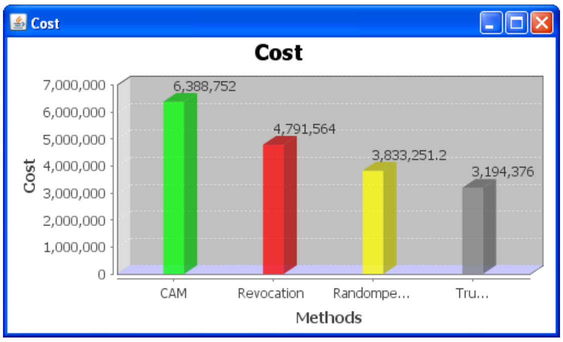


Figure2 :Cost Performance Comparison

The costs consumed by the existing methodologies are compared with our proposed methodology in order to prove the effectiveness of our algorithm. The comparison of the proposed methodology with the existing methodology is shown below.

5. Conclusion and Future Work

Conclusion

Mobile health monitoring is the effective and improving technology nowadays, which is used to reduce the burden of the users. The user can retrieve their medical treatment through the mobile health care monitoring system without the need of approaching hospitals. In this mobile health monitoring system, the sensitive information about the users are stored in the public/ private cloud, where the security and privacy of users becomes trivial complexity. In our work, the efficient novel approach is proposed which aims to enhance the privacy of user information. The user revocation is also handled efficiently in the proposed methodology in case of the illegal activities done by the intruders. The randomized balance tree concept is introduced in our work to enhance the more privacy which will hide the user information rather than the details which are required to handle the user query. The experimental results show that the proposed methodology computes efficient result than the existing methodology.

Future Work

In future we can use some other encryption and decryption techniques and compare it with existing system. By this comparison we can find the accuracy which one gives more privacy in cloud storage.

6. References

[1] Ateniese. G, K. Bensonand S. Hohenberger, “Key-private proxy reencryption,” in *Proc. CT-RSA*, 2009, pp. 279–294.

[2] Baldi. P, 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.

[3] Barni. M, P. Failla, R. Lazzeretti, A. Sadeghi, and T. Schneider, “Privacy-preserving ECG classification with branching programs and neural networks,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 452–468, Jun. 2011.

[4] Brickell. J, D. Porter, V. Shmatikov, and E. Witchel, “Privacy-preserving remote diagnostics,” in *Proc. 14th ACM Conf. Computer and Communications Security*, 2007, pp. 498–507, ACM.

[5] De Cristofaro. E, S. Faber, P. Gasti, and G. Tsudik, “Genodroid: Are privacy-preserving genomic tests ready for prime time?,” in *Proc. 2012 ACM workshop on Privacy in the Electronic Society*, 2012, pp. 97–108.

[6] Fu. K, G. Ateniese, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” *ACM Trans. Inf. Syst. Secur.*, vol. 9, no. 1, pp. 1–30, 2006.

[7] Goyal. V, O. Pandey,A. Sahai, and B.Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in *Proc. ACM Conf. Computer and Communications Security*, 2006, pp. 89–98

[8] Green. M and G. Ateniese, “Identity-based proxy re-encryption,” in *ACNS*, ser. Lecture Notes in Computer Science, J. Katz and M. Yung, Eds. New York, NY, USA: Springer, 2007, vol. 4521, pp. 288–306.

[9] Hii, P, C. Chung, W.Y. A comprehensive ubiquitous healthcare solution on an android mobile device. Sensors 2011, 11, 6799–6815.

[10] Hohenberger. S, M. Green and B.Waters, “Outsourcing the decryption of abeciphertexts,” in Proc. Usenix Security, San Francisco, CA, USA, Aug. 8–12, 2011, pp. 34–49.

[11] Kolesnikov. V, Barni. M, P. Failla, R. Lazzeretti, A. Sadeghi, and T.Schneider, “Secure evaluation of private linear branching programs with medical applications,” *Computer Security-ESORICS 2009*, pp.424–439, 2009.

[12] Lagendijk. R, Z. Erkin, and M. Barni, “Encrypted signal processing for privacy protection,” *IEEE Signal Process.Mag.*, vol. 30, no. 1, pp.82–105, Jan. 2013.

[13] Layouni. M, K. Verslype, M. Sandikkaya, B. De Decker, and H.Vangheluwe, “Privacy-preserving telemonitoring for ehealth,” *Data and Applications Security XXIII*, pp. 95–110, 2009.

[14] Lin. H, X. Zhu,Y. Fang, C. Zhang, and Z. Cao, “Efficient trust based information sharing schemes over distributed collaborative networks,” in Proc.Milcom, Baltimore,MD, USA, Nov. 7–10, 2011, pp. 1399–1403.

[15] Sahai. A and B. Waters, “Fuzzy identity-based encryption,” in *Proc.EUROCRYPT*, 2005, pp. 457–473.

[16] Shi. E, J. Bethencourt, H. T.-H. Chan, D. X. Song, and A. Perrig, “Multidimensionalrange query over encrypted data,” in *Proc. IEEE Symp. Security and Privacy*, 2007, pp. 350–364.

[17] Szakacs-Simon, P. Moraru, S.A. ; Perniu, L. Dept. of Autom., “Transilvania” Univ., Brasov, Romania , “ Android application developed to extend health monitoring device range and real-time patient tracking”.

[18] Tsanas. A, 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.

[19] Wang M-Y, Zao JK, Tsai PH, Liu JWS.Wedjat: “A Mobile Phone Based Medicine in-take Reminder and Monitor”. Proceedings of the 9th IEEE International Conference on Bioinformatics and Bioengineering; Taichung, Taiwan. 22–24 June 2009; pp. 423–430.