A Cloud Assisted Secure Privacy Perpetuating System for M-Health Monitoring

Sreethi S [1*], Neetha Alex[2]
[1*]PG Scholar, Dept. of computer science and engineering
Professor, Dept. of computer science and engineering
TKM Institute of Technology
Kollam,India

***Abstract*— Recent advancement in wireless communication and smart phone technology has shown great improvement in health monitoring services. Cloud-assisted mobile health (m-Health) monitoring poses a serious risk on both client's privacy and holding of observation service providers. This paper introduces a Secured Healthcare Monitoring system in cloud that helps to keep the communication among clients and service providers confidential and provide various services especially decision support for better security with extended privacy. To protect the privacy of data, the anonymous Boneh Franklin identity-based encryption (IBE) and decryption outsourcing is applied. To ensure more security, an efficient Audit scheme is applied, for logging up and for reporting anonymous access attempts and overheads experienced in a cloud server and thus avoid the risk of clients for missing or corrupted data. Moreover an offline education material is also provided that discusses about various aspects of diseases. System provides a simple user interface which can be easily understandable.**

Index Terms*— Identity Based Encryption, Outsourcing Decryption, m-Health, Auditing.

I. INTRODUCTION

Cloud-assisted mobile health monitoring (CAM) applies the predominant mobile communications and cloud computing technologies that helps in making decisions regarding issues related to health. M-Health or mobile health is a term used for the practice of medicine and public health supported by mobile devices. Mobile Health applications use mobile devices for collecting clinical health data, delivery of healthcare information to researchers, practitioners, and patients, real-time monitoring of patient crucial signs etc. Cloud is a next generation platform that reduces IT complexity by taking advantage of a shared pool of computing resources to deliver applications and services. Cloud computing is the provisioning of services and applications on demand over the Internet, ie ,it is internet (cloud) based development and use of computer technology. (computing). Simply, Cloud is a network of computers. Cloud computing is in a period of strong growth but still it has some issues of security and privacy and somewhat it is immature. Since the management of data and infrastructure in cloud is provided by a third-party, there exists always a risk to handover the sensitive information to such providers. Without properly addressing the data in cloud, client's privacy may be misused during the diagnosis, collection, communications, storage, and computing. which could deter the wide adoption of M- Health technology.

Cloud assisted mobile health observation is an approach that enhances the quality of health care service and lowers the health care price but it holds a heavy risk on privacy of client's and service suppliers intellectual property. The main aim of this paper is to handle this necessary drawback and style a cloud-assisted privacy protective mobile health observation system to safeguard the privacy of the concerned parties and their information. The outsourcing decryption technique and identity based encryption area unit tailored to shift the procedure quality of the concerned parties to the cloud while not compromising clients' privacy and repair providers holding.

To guarantee data integrity, audit services are vital. It plays a significant role to ensure the integrity and accessibility of outsourced data and to achieve digital forensics and reliability on cloud computing. Audit is an evaluation of a system, organization, process, enterprise, person, system, project or product. Auditing is the process for evaluating claims against the actual facts to ensure compliance. It is done to ensure systems are what they claims to be. Audits are of mainly two types. Internal audits evaluate the structure and processes within a service to ensure that service can continue to meet objectives. External audits evaluate the quality of service through external available interfaces. Third party audit is an accepted method for establishing trust in data. Here users ask an external audit party to check the integrity of their outsourced data. External audit party is called a Third Party Auditor (TPA).TPA has expertise and capabilities that users and service providers don't have. TPA is trusted to assess the cloud servers data & audit all server activities and provide an audit report to clients and company.

II. RELATED WORKS

A cloud assisted privacy preserving mobile health monitoring system, which can effectively protect the privacy of clients and the intellectual property of m-Health service providers [1]. To protect the privacy of data, bilinear pairing, homomorphic encryption, multidimensional range query based on anonymous ibe, decryption outsourcing, and key private proxy reencryption (PRE) cryptographic techniques are used. A Secured Patient Healthcare Mobile Monitoring

using Cloud computing [2] that helps to keep the communication between doctor and patient confidential is developed. Here the patient's report will reach the doctor in encrypted format, while a master key helps to deliver the report to the doctor in decrypted format. Then the doctor's prescription will reach the patient in encrypted format by using the Outsourcing Decryption Technique while a master key helps to deliver the prescription to the patient in decrypted format. To achieve the high privacy on the mobile health care system a work is proposed [3] that uses the re-encryption scheme to encrypt the all the information into one time ,and produce the token for the information retrieval on cloud. The reencryption scheme to reduce the complexity of the encryption . Medi-Net system aims to provide a high level of service to its users in the face of communication failures [4]. It ensures that patients continue to use the system despite failures that may occur when transferring data between healthcare devices and mobile phones and between mobile phones and web server components. A survey concerning the current models of health that are switching to solutions based on cloud computing, is proposed in [5]. Different applications and services are explored and concluded that the use of cloud computing and in particular of hybrid cloud solution can represent a significant opportunity to increase the development of the health sector in all its aspects. A secure cloud storage system supporting privacy-preserving public auditing.[6] enable the TPA to perform audits for multiple users simultaneously and efficiently. This scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy preserving manner. To avoid the security risks, audit services are critical to ensure the integrity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing. [7].Changes from individual lab systems to a grid and cloud based environment for Biomedical Informatics are revised in [8]. Many observers believe that clouds represent the next generation of computing paradigm for biomedical application. It help users at biomedical laboratories, funding agencies, and especially consortia to understand where cloud computing may be appropriate and to describe how to assess a particular cloud. The rapidly-growing cloud literature suffices to guide labs that simply wish to acquire cheaper compute resources.A mobile phone SMS-based system for self management of Diabetes [9] can be a long term health companion for patients with diabetes. This paper presents the ongoing development, with regards to design and technical implementation, of a large scale, community-based self-management system for diabetes. It focuses on achieving a user-friendly approach to SMS input methods. The system is designed to be a free, community-based service, capable of handling a large number of users, with the potential for multiple input modes, online reporting and group management for medical professionals.Here a neutral cloud server is assumed, which means it neither colludes with the company nor a client to attack the other. Clients may collude with each other. We do not consider the possible side-channel attack [10] due to the coresidency on shared resources either because it could be mitigated with either system level protection or leakage resilient cryptography. Thus, our CAM design assumes an honest but curious model, which implies all parties should follow the prescribed operations and cannot behave arbitrarily malicious.Besides, the private computation or processing of medical information over cloud has also attracted attention from both the security community and signal processing community[11]. It introduces the fusion of signal processing and cryptography as an emerging paradigm to protect the privacy of users. The viability and practicality of privacy-agile computational genomic tests in the portable and pervasive setting of modern smart phones. We combined domain knowledge in biology, genomics, ubiquitous computing, and applied cryptography, to design and build a personal genomic toolkit, called GenoDroid [12].

III. SYSTEM ARCHITECTURE DESIGN

We now highlight our design of the proposed cloud-assisted m-Health monitoring system (CAM). CAM consists of five parties as shown in Fig. 1.

1) Cloud server or simply the cloud
2) Company which provides the health monitoring service i.e, the health service provider
3) Semi-trusted authority (TA).
4) Third party auditor (TPA)
5) Clients

The company stores its health monitoring program as a branching program in encrypted format in cloud and upload query results based on branching program. Clients collect their medical information and send their relative query to the cloud in encrypted format. Trust authority is responsible for distributing private keys to the client. The TA can be considered as a management agent for a company (or several companies) and shares certain level of mutual interest with the company. Third party auditor helps to audit the data. Cloud server acts as an offline storage. All data are saved in encrypted format even passwords of users. TPA helps to audit the data.

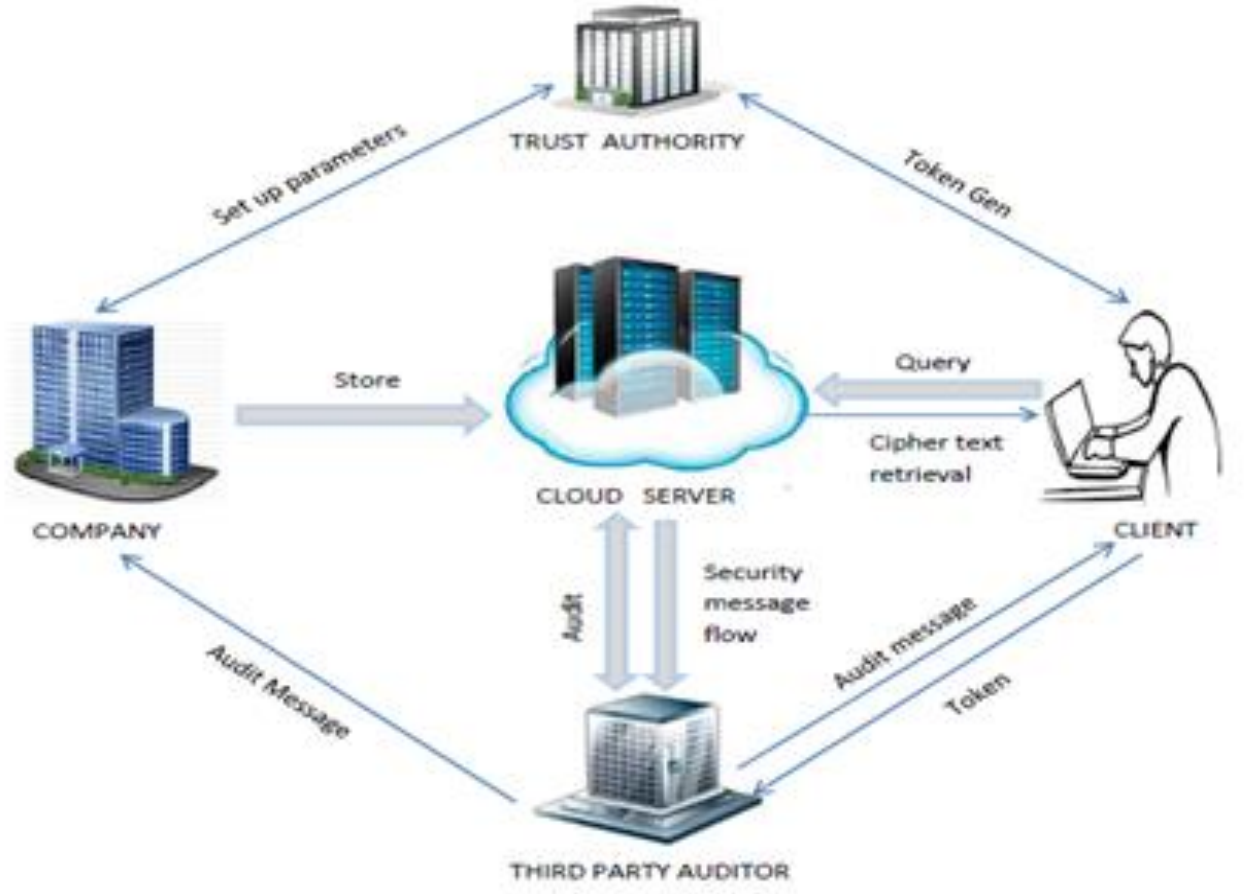

Fig1. CAM System architecture

The major steps are: *Set up, Store, Token Generation, query and audit*.

.At the initial phase, Trust authority runs the *set up* phase and publishes the system parameters like length of message, type of data that can be used etc. Then, the company develop the flow chart of a Health monitoring program as a branching program, and store its resulting cipher text and its company index to the cloud in encrypted format, which corresponds to the store algorithm in the ambience. When a client wishes to send a query to the cloud, the client and TA run the token generation algorithm. Then the client receives the token corresponding to its query while trust authority gets no useful information on query. Then the client hand over the token along with the encrypted query to the cloud, which runs query the phase. Then company's service provider uploads results of clients query based on the branching program in encrypted format in cloud. Then the cloud admin completes the major computationally severe task for the client's decryption and returns the partially decrypted cipher text to the client. Inorder to view results, the client then performs the remaining decryption, corresponds to the decision from the monitoring program on the client's query. And thus we can ensure that the cloud obtains no useful information on either the client's query input or decryption result after running the phase. In the audit phase the third party auditor (TPA) performs audit on whatever data that is stored in cloud server and delivers an audit response to the company regarding the branching program and clients regarding the query , query results, failed logins, password changes, last login time etc.

A. Branching Program

Health monitoring program works on branching program, which is based on binary classification or decision trees. Here illustrates how a branching tree works. Fig 2 shows an example of a branching program that is used in medinet project. Clients input their health data such as systolic blood pressure, missed daily medications or have an abnormal diet, a to the system, and system then return recommendations on how the clients can improve their conditions such as modify daily diet, and take regular medication. Example-Query is Blood Pressure 80 missed medication.

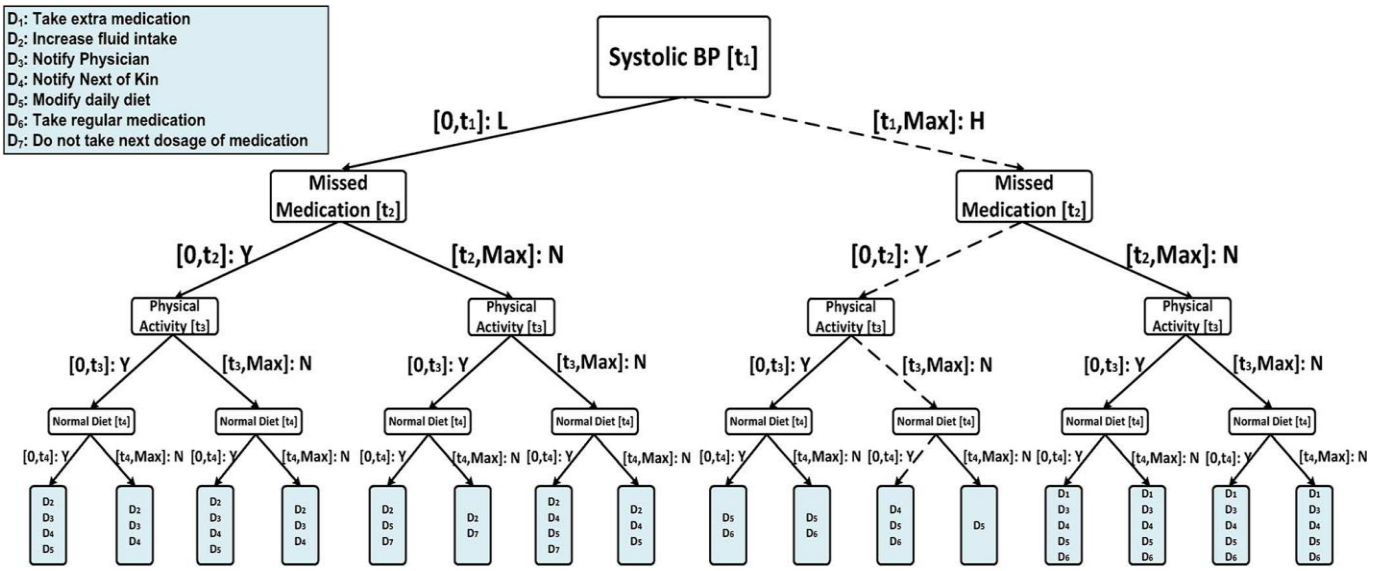

Fig.2. Branching program in MediNet project

B .Token Generation

STA generates token for user. STA cannot view token as it is generated & send to client. Token can be in the form of jzcv1ERHziowFuiPLfcgdbtBv84NJJNNgg8SiBg.User system gets token to retrieve query result.

IV . IMPLEMENTATION

Cloud-assisted mobile health monitoring (CAM) system is implemented as a web application that is ready to host on cloud. Development tool used is Microsoft Visual Studio 2010 based on Microsoft .NET Framework 4.0 and development language is Microsoft Visual C#. Algorithms used are:

1. Identity Based Encryption

Identity Based Encryption is a public key based cryptographic system that uses 2 keys: public key and a private key. Public key is known to everyone and private key is known only to the recipient of the message. The IBE algorithm [13] consists of four operations: setup, extract, encrypt and decrypt.
For example, If Alice wants to send a secure message to Bob , Alice uses Bob's public key to encrypt the message and Bob uses his private key to decrypt the message.

Step 1: Alice encrypts the mail using "bob@b.com", Bob's mail address, as the public key.
Step 2: When Bob gets the message, he contacts the key server. The key server contacts an external authentication source to authenticate Bob's identity.
Step 3: Key server then returns his private key after authenticating Bob, which then Bob uses to decrypt the message. The private keys are issued by a trusted third party called the private key generator (PKG).

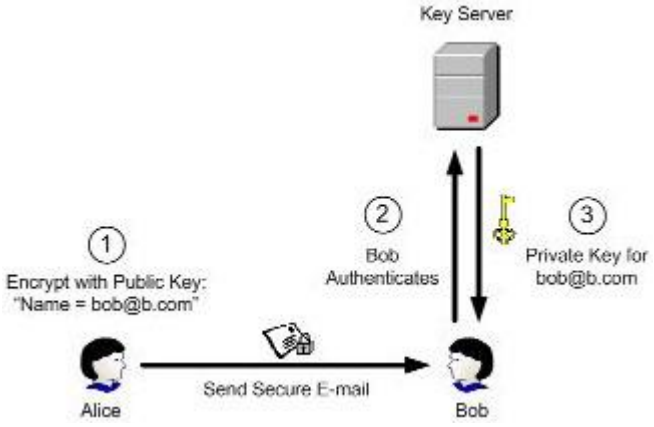

Fig 3: Example for IBE

The IBE algorithm consists of four algorithms:
1) **Setup**: This algorithm initializes a key server. It is run by the PKG for creating the total IBE environment. The master key is kept secret which is used to derive users private keys, while the system parameters are kept public. It takes as input a security parameter gives as outputs system parameters and a master key. System parameters gives description of a finite message space and cipher text space.
2) **Extract**: This algorithm extracts a private key from a given public key. It is run by the PKG when a user requests a private key. It takes as input master key and an identifier and returns the private key for user.
3) **Encrypt**, This algorithm encrypts a message returns the corresponding cipher text for a given user.
4) **Decrypt**, using the given private key, it decrypts a message.
These algorithms must satisfy the standard consistency constraint

Decrypt(params ;C;d) = M where C = Encrypt(params; ID ;M)

TABLE I: INPUTS AND OUTPUTS IN IBE ALGORITHMS

Algorithms	Inputs	Outputs
Setup	security parameter k	params and master-key
Extract	params, master-key, and an ID	private key
Encrypt	params, ID, and M	Ciphertext C
Decrypt	params, C , and a private key	Message M

2. Outsourcing Decryption

Outsourcing Decryption is a new paradigm for Attribute Based Encryption (ABE) that largely eliminates the decryption overhead for users. ABE is a public key based one to many encryption that allows users to encrypt and decrypt messages based on user attributes. In such a system decryption of a cipher text is possible only if the attributes of user key matches attributes of cipher text. One of the main drawbacks of existing ABE is that decryption involves expensive pairing operations and the size of the cipher text and the time required to decrypt it grows with the complexity of access formula. Outsourced decryption eliminates the decryption overhead for users. Simply Outsourced decryption is a process to maximize the decryption speed . Usually it is performed by another cloud server or proxy server who will be dedicated to do the decryption process.

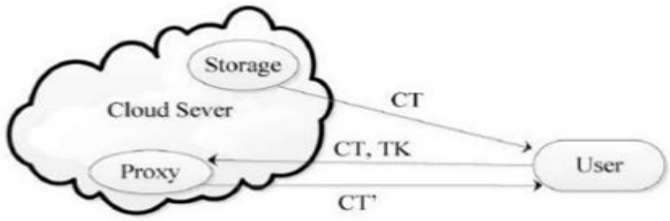

Fig. 3: outsourced decryption

In this system using a single transformation key from the user cloud translate any ABE cipher text satisfied by the user attributes into a short simple cipher text using a single transformation key. Outsourced ABE systems use a modified key generation algorithm that produces 2 keys: a secret key that must be kept private by the user and a transformation key that is shared with the proxy.
If the proxy then receives a cipher text(CT) for which the user credentials satisfy proxy uses the transformation key to transform CT into a simple & short cipher text CT'.
3. Interactive Audit Algorithm

An interactive audit scheme is proposed to support our audit system in clouds. This scheme is constructed on the standard model of interactive proof system, which can ensure the confidentiality of secret data and decidability of invalid tags. Audit rules are defined to determine if the correct data is processed. Also in case of audit rule failure there is a provision to generate notification of audit failures. This scheme enables an external auditor to audit user's cloud data without learning the data content. It allows TPA to track failed login, invalid token and branching programs authentification. It is done by using the CHECKSUM Audit Function. It helps to audit based on the hash values generated. Here checksum is created by taking sectors from data and periodically verifies the data for consistency. A checksum is a count of the number of bits in a transmission unit that is included with the unit so that the receiver can check to see whether the same number of bits arrived.

TABLE II: STEPS IN AUDIT ALGORITHM

Algorithms	Functions
KeyGen	key generation algorithm is run by the user to setup the scheme
MetaDataGen	Generate metadata by TPA based on data storage by client and company
AuditDataGen	Checks the integrity of data on cloud storage using metadata and generates audit output

V .PERFORMANCE EVALUATION

On evaluating the proposed system it is found that the cloud or trust authority or third party auditor will not obtain any useful
information on either the client's query vector or company's branching program. It is achieved by using the powerful identity based encryption and outsourcing decryption cryptographic techniques. Being attribute based there is no key hijacking possible. Since it is a token based system, any user cannot decrypt data alone. Audit schemes introduced here helps to ensure more security and thus avoid the chances for the data to get missed or corrupted. The computation overhead of the company is reduced due to the usage of encryption scheme.

VI. EXPERIMENTAL RESULTS

Registration is a mandatory process to get into the health monitoring system for any clients or company's service provider or TA or TPA. The following modules are created for effective generation of the proposed system output.

1) Service provider module:

Company's service provider (Health care service provider) store health monitoring program as a branching program in cloud and add the corresponding medical data details. He can view user details, user queries and upload results of client's query based on branching program. An offline education material is also provided by him to clients that discusses about various aspects of diseases.

2) Cloud admin module

Cloud admin can view service providers details and he has the right to allow or discard the service provider by checking their details. To reduce the decryption overhead for users he perform partial decryption of results. If any query is tagged emergency by the client cloud admin sent a message to mobile phone of company's service provider to respond immediately.

3) Trust authority module

Trust authority is responsible for generating the token and send the token as mail to the client.

4) User module

Users add their basic details, raise queries, encrypt query using token that is received in their email address and decrypt query results using the same token. There is also provision for them to add their suggestions, comments, feedbacks etc.

5) Auditor module

TPA assesses all data's on cloud and send audit reports to clients and service provider .To allow TPA securely, TPA audit data from cloud and not ask for a copy and will not read data content.It will not disclose any clients information not create new vulnerability to user data privacy.

VII. CONCLUSION

Cloud Computing technology provides many advantages such as cost reduction, effective resource management and high quality service. But if security accidents occur, damages are imminent. Here a cloud-assisted privacy perpetuating mobile health observation system is designed which can effectively protect the privacy of involved parties and their data. To protect the clients' privacy, the anonymous Boneh–Franklin identity-based encryption (IBE) is applied in branching programs. To reduce the decryption complexity due to the use of IBE, decryption outsourcing with privacy protection is used. Auditing schemes proposed here helps to ensure more security. We use simple graphical user interface for health related applications which is easily learnable. The system can be used by a range of organizations including hospitals, universities, private clinics and healthcare groups.

REFERENCES

[1] Huang Lin, Jun Shao, Chi Zhang, and Yuguang Fang, Fellow, IEEE "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL.8, NO. 6, JUNE 2013.

[2] Dr.P.RajaRajeswari, J.Jameson, V. Premalatha" SPHM: A Secured Patient Healthcare Mobile Monitoring using Cloud Computing," in International Journal of Scientific Engineering and Technology, pp : 834-837 1 July 2014

[3] S.kousalya,"Privacy and Efficiency On Health Care DataUsing Private Proxy Reencryption Scheme", in International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014

[4] A.Koteswaramma, S. Lakshmi Soujanya, "A MediNet for staying connected in a Mobile Healthcare System," in International Journal of P2P Network Trends and Technology (IJPTT) -Volume3Issue7-August 2013.

[5] Carmelo Pino ,Roberto Di Salvo," A Survey of Cloud Computing Architecture and Applications in Health," in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)

[6] Imran Ahmad , Prof. Hitesh Gupta , "Privacy-Preserving Public Auditing & Data Integrity for Secure Cloud Storage," in International Conference on Cloud, Big Data and Trust 2013, Nov 13-15, RGPV.

[7] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Stephen S. Yau, "Efficient audit service outsourcing for data integrity in clouds ," in IEEE 2012 Transactions on Cloud Computing.

[8] Mohana R.S, Dr.P.Thangaraj , S. Kalaiselvi, B.Krishnakumar," Cloud Computing for Biomedical Information Management," in International Journal of Scientific Engineering and Technology Volume 2 Issue 4, PP : 239-244 April 2013

[9] Osama salameh "A Mobile Phone SMS-Based System For Diabetes Self management" in International journal of e-health technology, vol 2, NO 3,jan 2012

[10] T. Kim, M. Peinado, and G. Mainar-Ruiz, "Stealthmem: System-level protection against cache-based side channel attacks in the cloud," in Proc. 21st USENIX Conf. Security Symp., 2012.

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

[12] T .Parameswaran, S.Vanitha, K.S.Arvind," An Efficient Sharing of Personal Health Records Using DABE in Secure Cloud Environment" in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013

[13] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. CRYPTO*, 2001, pp. 213–229.