ISSN:0975-9646

A Portable and Secure Healthcare Maintenance System

K.Sravani[#1], B.Bindusha Reddy[#2], R.R.V.N.V.Kumari[#3], G.Vijay Kumar*[4]

[#]*B.Tech, ECM Department, K L University*
Vaddeswaram, Guntur, A.P, INDIA

[*]*Assoc. Professor, ECM Department, K L University*
Vaddeswaram, Guntur, A.P, INDIA

Abstract: Portable Healthcare protection is a System that applies the current mobile communications and cloud computing technologies to provide feedback decision support that has been an essential approach to improve the excellence and to reduce the cost of healthcare services provided. Unfortunately, the system creates a serious risk on both user's privacy and intellectual property of monitoring by the service providers. It also discourages the broad acceptance of portable Health services. The portable healthcare application for the mutually involved parties in this mechanism is for the better security with extended privacy and data integrity by applying techniques. This portable health care maintenance system is to propose simple user interface which is easily understood even by the illiterates and the payment is done online. It integrated hash function algorithm technique and privacy aware security algorithm which can protect data integrity. This system provides ease in the portable healthcare applications with better efficiency and it is very useful to remote areas where hospitals are not easily accessible. Our proposed system demonstrates the portable health maintenance system with simple user interface and protection of data in cloud.

Keywords: Health maintenance, privacy, hash algorithm, Trust authority and security.

I. INTRODUCTION

Now a day the usage of telephones and mobile devices are very often. The mobile devices such as smart phones which are designed are high in quality and price, the low price sensors have a great impact on improving of health care services. Some of the developing countries are best examples for using this remote health monitoring system. MediNet [2] is a project designed by Microsoft to monitor the health status of a person such as blood sugar, cardiovascular diseases especially in rural areas. In this type of mobile health monitoring system, sensors are attached to the body of a patient and their physical data is noted by the sensors. This physiological data is sent to the central server of the cloud that performs various applications on web which are related to medical and report all the updates regarding the health condition of the patient along with the suggestions to the client frequently. All these applications have the capability to perform various processes to examine the client health. Even if the cloud assisted health monitoring could offer a great opportunity in quality of service and the lowering of prices. The clients are not ready to accept it because the patients are concerned more about the privacy of their health information. While the data of the patients regarding their health is collected there may be chance for the lack of privacy during storage, communication, diagnosis and computing. Even some of the existing privacy laws are considered as the protection for the health record of a patient is not transferable to cloud computing environments. As the physical data of a person is collected there will be chances for having the information of their biometrics, DNA profiles.

In the proposed scenario, it is the good chance for the people who advice to have a large set of medical information. The cloud [3] is made efficient when a viable solution is sought by incorporating the software as a service (SaaS) model and pay-as-you-go business model in cloud computing. The future trend can be observed by the adoption of automated decision support algorithms in the cloud-assisted mobile health monitoring. There can be both malicious and non-malicious attackers who come in to this health care system for illegal purpose. The malicious attackers are more dangerous when compared to the non-malicious. The inside attackers can easily hack these health care systems as they are generally a professionals. Outside attackers can be prohibited by cryptographic methods such as encryption and it is major to design preserving methods of the client's health details privacy. The cloud server is nothing but the cloud industry which gives health monitoring and provides health care service to the individual users based on the third party. With the help of cloud computing clients can preserve the information into the cloud remotely and utilize on-demand maximum quality applications. Major problem in addressing security and privacy in the computational work load involved in the cryptographic techniques. With the presence of cloud computing facilities it will be wise to shift intensive competitions to cloud server from resource-constrained mobile devices.

II. RELATED WORK

Vasiliki Danilatou et al. [4] combined the power of decentralized management and access control, provided by cryptographic credentials, with the ability to perform privacy-preserving set operations on data. Ashwini Jadhav et al. [5] discussed how the health details are compared with a value as per the doctors suggested. By this comparison the patient can get the details of his/her health condition. Here the Company provides a service and stores the encrypted health details of a patient. Trust Authority

only provides a key to the patient when entered the details. Sever is neither act towards company or patient.

Balaganesh et al. [6] proposed abilinear map whichis a function combining elements of two itemsto get an element of a third item. Homomorphic encryption-key is generated. The paring is done using Diffe-Hellman (DBDH) algorithm. This algorithm is used for securely exchange of Cryptographic Keys over the public channel. System time is divided into time periods called slots. These slots may be 1 week/month based on the specific application. The problem identified in this is the private key can be known from cloud server by identity test MDRQ's. So to protect the Key, we use "Key Private-Encryption Schema "here Cryptographic hash functions are used. The data (disease, symptoms...) are known to some people like scientists and different doctors for research and also other purpose but the personal details are not be relieved. In [1] the author's proposed the use of integrity and showed that it is a vital aspect in health care. It also provides SMS alert for users.

Ramya et al. [7] In USA 75% people believe the security of their health records and data are very essential. In system development they used decryption and non-decryption algorithms on the cipher text developed in store algorithm. Mohammed Azhar et al. [8] this cloud assisted monitoring stores no details of the user query, so it can be more secured and therefore the user will be reliable of this cloud assisted [13] privacy preserving health monitoring system. The trusted authorities have an idea to take details of client query but nevertheless it cannot succeed their idea due to the client's privacy. The trusted authority is willing to take details of the users because when two users have the same query they might get the same suggestions regarding their health care without checking their previous health record.

Neena Jose et al. [9] proposed the remote home health care systems provide long term care to patients, to keep their physical fitness, nutrition, social activity, so that they may function independently at their homes as long as possible. It helps to deal with the social and financial burden of an aging population.

Clifford et al. [10] proposed a new paradigm for decryption of ABE that largely eliminates the overhead for users, suppose that ABE cipher texts are stored in the cloud. Here it is shown as how a user can provide the cloud with a single transformation key that allows the cloud to translate any ABE cipher text satisfied by that user's attributes into a (constant-size) ElGamal-style cipher text, without the cloud being able to read any part of the user's messages. For security issues [12] various clouds are available namely private, public and hybrid. Private cloud is set up within an organization's internal enterprise datacenter. Dimitrios et al. [11] discussed that resources and virtual applications provided are pooled together and are available for users to share their data and use when necessary. Cloud resources and applications are managed by an organization itself. This is more secure because of its specified internal exposure. Only the organization and the esignated stakeholders can access to operate specific private cloud.

Public cloud is based on the Self-service over the internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on computing basis. It is based on a pay-per-use model. Public Clouds are less secure compared to private cloud because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to any malicious attacks. Hybrid cloud is a private cloud linked to one/more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network. It provides a service by mixing both public and private clouds. It provides more secure over data and applications. So we use hybrid technology for more secure reasons. It has an open architecture which allows the clients interfacing with the other management systems.

III. PROBLEM DEFINITION

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 achieve this effectively without compromising privacy and security becomes a great challenge, which should be carefully investigated. The problem becomes especially trickier for cloud assisted mobile health systems because we need not only to guarantee the privacy of clients' input health data, but also that of the output decision results from both cloud servers and healthcare service providers.

IV. PORTABLE HEALTHCARE MAINTENANCE SYSTEM

Cloud assisted monitoring contains four parties which involves to provide security to the users data. The four parties are trust authority, client, cloud server and company. The trust authority is responsible for generation of token and to get information from the cloud. These tokens are generated as requested by user in a partially encrypted form and it is sent to the cloud. Cloud authorizes to send a unique key to the users for their respected queries and also it is responsible to collect the service fee from clients. As the hybrid cloud is more secured, it can be utilized when privacy is the main concern. The client request for a service to the service provider and a token is generated to the client to go through the service. After the service is completed, the charges will be sent by the service provider to the client. On receiving of the charges, the client can pay the amount through any one of these options like net banking, credit card, debit card and even using "pay pal" account when the client performs online payment the payment is done faster. The paper work and the time can be reduced by doing the payment online. Clients can complete their payments securely in a very short time comparativelyto the manual payment.

The trusted authority is considered as an associate for a company to share their joint business. Clients clear their queries. The cloud server is itself a cloud where the company gives mobile health monitoring nothing but the providers of health care service, the individual users and the third party known as semi trusted authority. With the help of the cloud computing, users can preserve their information in to the cloud remotely and utilize on-demand maximum quality applications. 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. The company stores it encrypted monitoring data or program in the cloud. Cloud generate a bill to the user whenever they access their service. The bills have their id and the service fee provided by the company. The payment is done from their account. Software as a service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, [15] typically the Internet. SaaS is also associated with a pay-as-you-go subscription licensing model. With the low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, support, licensing, and high initial cost.

These applications are accessed using web browsers over the Internet; therefore web browser security is important. Web Service (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) is some methods to provide security for the information. The information retrieval is effective when compared to the existing system. For the efficiency in this paper we are using MD5 algorithm and privacy aware security.

SYSTEM ARCHITECTURE

Privacy-Aware Security Algorithm for Cloud Computing: Security is one of the most demanding current research areas in cloud computing because data vendor stores their data to remote servers and clients also access required data from remote cloud servers which is not restricted and managed by data vendors. This paper proposed a new algorithm (Privacy-Aware Security Algorithm) for cloud environment which includes the three different security schemes to achieve the objective of maximizing the data owners control in managing the privacy mechanisms or aspects that are followed during storage, processing and accessing of different Privacy categorized data. The performance analysis shows that the proposed algorithm is highly efficient, Secure and Privacy aware for cloud environment we discuss three critical challenges: regulatory, security and privacy issues in cloud computing. Some solutions to ease these challenges are also proposed along with a brief description on the future trends in cloud computing operation.

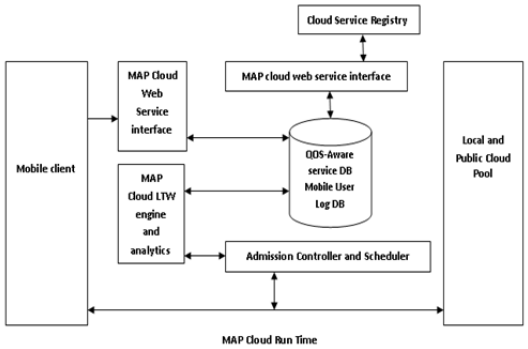


Fig. 1 Architecture

Step1: Framework to Preserve Privacy of Healthcare Data in the Cloud

With the increase of IT infrastructures, the requirement and knowledge sharing, integration has become very fundamental. Cloud computing is one among the leading standard IT infrastructures for facilitating electronic health record sharing and integration. Several expect that managing applications with clouds can create innovative. To access to present condition not exclusively can make possible. To improve present conditions we can forever be accessible from anyplace at any time, however additionally it helps scaling down the prices severely. We have a tendency to present a generic framework named "PriGen" that preserves the privacy of sensitive aid knowledge within the cloud. PriGen permit the users to preserve privacy whereas accessing cloud mainly based on service while not the assistance of a trusted third party. With creating use of homomorphic encoding operate on personal information; the planned framework maintains confidentiality of personal information sent by the cloud users to untrusted cloud mainly based on service. In this paper we have a tendency to additionally present a quick discussion of various parts of PriGen framework.

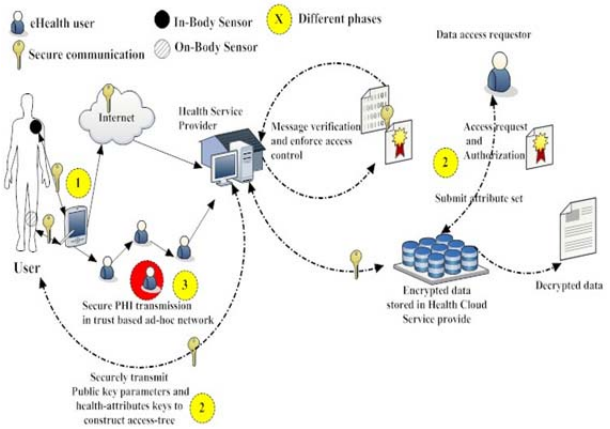


Fig. 2 Privacy of health care data in the cloud

Step2: Efficient Private Information Retrieval for Map Reduce (QOS)

Private Information Retrieval (PIR) allows a user to retrieve bits from a database while hiding the user's access pattern. However a PIR in a real-world cloud computing setting has recently been questioned. In such a setting, PIR's huge computation and communication overhead is expected to be more important than the cost saving advantages of cloud computing. In this paper, we first examine existing PIR protocols, analyzing their efficiency and practicality in realistic cloud settings. We identify shortcomings and, subsequently, present an efficient protocol (PIRMAP) that is particularly suited to Map Reducea widely used cloud computing model. PIRMAP focus especially on the retrieval of large files from the cloud, where it achieves good communication complexity with query times considerably faster than previous schemes. To achieve this, PIRMAP enhance related work to allow for optimal parallel computation during the "Map" phase of Map Reduceand homomorphism aggregation in the "Reduce" phase. To improve computational cost, we

also employ a new, faster "some what homomorphism" encryption, making our scheme practical for databases of useful size while still keeping communication costs low. PIRMAP has been implemented and tested in Amazon's public cloud with database sizes of up to 1TByte. Our evaluation shows that non-trivial PIR such as PIRMAP can be more than one order of level, cheaper and faster than trivial PIR in the real-world.

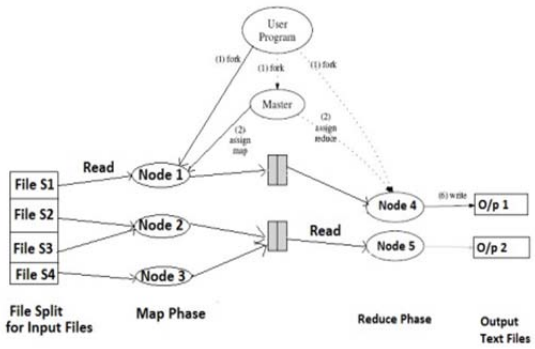
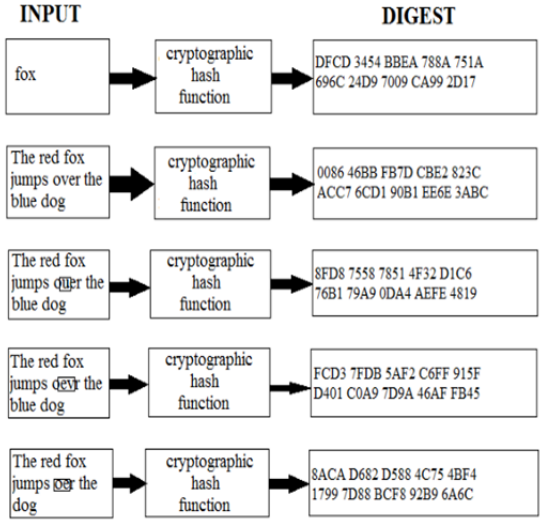


Fig.3 Map Reduce Process

MD5 algorithm (hash Function)

The MD5 function is a cryptographic algorithm that takes an input of arbitrary length and produces a **message digest** that is 128 bits long. The digest is sometimes also called the "hash" or "fingerprint" of the input. MD5 is used in many situations where a potentially long message needs to be processed and compared quickly. The most common application is the creation and verification MD5 was designed by well-known cryptographer Ronald Rivest in 1991. In 2004, some serious flaws were found in MD5. The complete implications of these flaws has yet to be determined



MD5 algorithm (hash function) can be used Message of arbitrary length and produces as output a 128 bit "message digest" of the input. It is assumed that it is computationally infeasible to produce two messages having the same message digest. Intended where a large file must be "compressed" in a secure manner before being encrypted with a private key under a public-key cryptosystem.

MD-5 Algorithm

Step1 – Append padded bits:

The message is padded so that its length is congruent to 448, modulo 512. Means extended to just 64 bits shy of being of 512 bits long. A single "1" bit is appended to the message, and then "0" bits are appended so that the length in bits equals 448 modulo 512.

Step 2 – Append length:

A 64 bit representation of b is appended to the result of the previous step. The resulting message has a length that is an exact multiple of 512 bits.

Step 3 – Initialize MD Buffer

Step 4 – Process message in 16-word blocks

Step 5– output

3-Tier Architecture: The three-tier software architecture emerged to overcome the limitations of the two-tier architecture. The third tier (middle tier server) is between the user interface (client) and the data management (server) components.[14]This middle tier provides process management where business logic and rules are executed and can accommodate hundreds by providing functions such as queuing, application execution, and database staging. The three tier architecture is used when an effective distributed client/server design is needed that provides increased performance, flexibility, maintainability reusability and scalability while hiding the complexity of distributed processing from the user. These characteristics have made three layer architectures a popular choice for Internet applications and net-centric information systems.

V. EXPERIMENT ANALYSIS

First the registration is compulsory to get into health maintenance system either for the doctor or the patient. For the ease of understanding since a private query protocol based on a general decision tree can be easily derived. Clearly, component is concatenation of index and the respective value. For example, patient query gives BP-130, then it shows BP lower than 130 is considered normal, and those above this are considered as high BP. After the patient is registered a query can be given on their health. The third party access the information given by the client and generate a token. A semi-trusted authority is responsible for distributing private tokens to individual clients and receiving the service fees from the clients. As per the token the client gets the status of their health condition. If there is a problem in their health status the service provider advise the client to consult doctor and inform him tha availability of the doctor prescribed. Later, when the service is finished the client pays the amount online.

VI. CONCLUSION

This paper addresses a portable health maintenance system, known as cloud assisted monitoring, which can efficiently protect the privacy of users and the cerebral property of portable health service providers. Cloud computing technology provides human advantages such as reasonable charge fall and effective resource management.To secure the users privacy we used privacy aware security algorithm. For the effective resource consists of hash function (MD-5) in which a master key helps to deliver the report.

REFERENCES

[1] Shantanu Shankar Pawar and R. N. Phursule, "Protect Integrity of Data in Cloud Assisted Privacy Preserving Mobile Health Monitoring", International Journal of Information & Computation Technology. Volume 4, Number 13 (2014), pp. 1329-1334.

[2] P. Mohan, D. Marin, S. Sultan, and A. Deen, "MediNet: Personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony," in Proc. 30th Ann. Int. Conf. IEEE Engineeringin Medicine and Biology Society, 2008 , pp. 755–758.

[3] Huang Lin, Jun Shao, Chi Zhang and Yuguang Fang, Fellow, IEEE, CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring VOL.8, NO.6, JUNE 2013.

[4] VasilikiDanilatou and Sotiris Ioannidis Security and privacy architectures for biomedical cloud computing.

[5] Ashwini Jadhav, V. Bhiksham, P. Vishwapathi Mobile Health Monitoring Technique using Cloud Computing, International Journal of Recent Technology and Engineering , Volume-3 Issue-4, September 2014.

[6] M.Balaganesh, J.Venkateshan, A Research Two Aggregate Algorithm Techniques for Third Party Auditor (TPA) Supports to Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4, April 2014.

[7] Mrs. Ramya.R, Mrs.Shruthi.G, Privacy Preserving Of Health Monitoring Services In Cloud, International Journal of Advance Research In Science And Engineering IJARSE, Vol. No.3, Issue No.6, June 2014.

[8] Mohammed Azhar, Maddikunta Laxman, Secured Health Monitoring System in Mobile Cloud Computing, International Journal of Computer Trends and Technology (IJCTT) – volume 13 no. 3 – Jul 2014.

[9] Neena Jose, Jini KM2, An efficient approach for mobile health monitoring, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 63-67.

[10] G. Clifford and D. Clifton, "Wireless technology in disease management and medicine," Ann. Rev. Medicine, vol. 63, pp. 479–492, 2012.

[11] DimitriosZissis, DimitriosLekkas," Addressing cloud computing security issues" Department of Product and Systems Design Engineering, University of the Aegean, Greece.

[12] Kuyoro S. O. ,Ibikunle F. AwodeleO, Cloud Computing Security Issues and Challenges, International Journal of Computer Networks, Volume (3) : Issue (5) : 2011.

[13] Dr.P.RajaRajeswari, .Jameson, .Premalatha,"A secured patient health care mobile monitoring using cloud computing'' International Journal of scientific engineering and technology, vol-3, issue 7, pp: 834-837.

[14] George Danezis, Benjamin livshits,"Towards ensuring client-side computational integrity".

[15] J.Benaloh, M.Chase, E.Horvitz and K.lauter,"Patient control encryption: ensuring privacy on electronic medical records", in ccws 09, 2009, pp, 103-114.