ISSN Online: 2319 – 9253
Print: 2319 – 9245

Security in Cloud Based Health Monitoring Systems

#1Ramya katanguri- M.Tech Student
#2A.Ravi kumar- Assistant Professor
Dept of CSE, Ganapathi Egineering College, Warangal, Telanagana, India.

***Abstract*—Cloud based monitoring system is a boon for the patients because by sitting at their home they can check their health status without much expenditure. Unfortunately, it poses a serious risk on client's privacy because cloud services are generally considered very unreliable. This paper is to design a cloud assisted mhealth monitoring system to protect the data involved in transfer as a result provide security to the health monitoring system.RSA algorithm with digital signature is used to keep the data secure during transmission. The disadvantages of the existing system has been rectified as it covers all the aspects of a secure system such as authentication,confidentiality,integrity and non-repudiation. This system is also designed to cater to the needs of the resource constraint industries as it involves less expenditure during its setup and execution.**

***Index Terms*—Mobile health (mHealth), Healthcare, Privacy,Outsourcing decryption, Key private proxy re-encryption.**

I.INTRODUCTION

During the recent years mobile has become the part and parcel of our life. Remote mobile health monitoring is considered as a successful example of mobile health (mheath) application. Microsoft launched its "MediNet" to help patients to check their health status even in remote areas. In this system a client could deploy portable sensor network to collect various physiological data such as blood pressure, breathing rate and blood glucose. Such data are then sent to the cloud server which runs its web medical application on these data and returns back to the client with the advice.

Apart from providing health benefits to the client, small emerging companies can avail the facility of incorporating the software as a service (SaaS) model and pay-as-go business model in cloud computing. Even after deploying various secure health monitoring system there is still the problem of client's privacy being severely breached during storage, diagnosis and computing. Such companies have a greater threat from its disloyal employees who share the private data with other company in lieu of money. These data are used by research institutes, insurance companies and even government agencies. Although the existing privacy laws such as HIPAA(heath insurance portability and accountability act) provide baseline protection for personal heath record, the generally considered not applicable or transferable or applicable to cloud computing environment.

Traditional privacy protection mechanisms by simply removing clients' personal identity information (such as names or SSN) or by using anonymization technique fails to serve as an effective way in dealing with privacy of mHealth systems due to the increasing amount and diversity of personal identifiable information . It is worth noting that the collected information from an mHealth monitoring system could contain clients' personal physical data such as their heights, weights and blood types, or even their ultimate personal identifiable information such as their fingerprints and DNA profiles .

According to, personal identifiable information (PII) is any information, recorded or otherwise, relating to "an identifiable individual. Almost any information, if linked to an identifiable individual, can become personal in nature, be it biographical, biological, genealogical, historical, transactional, location, relational, computational, vocational, or reputational". In other words, the scope of PII might not necessarily be restricted to SSN, name and address, which are generally considered as PII in the traditional sense. Indeed, the state of the art reidentification techniques , have shown that any attribute could become personal identifiable information in practice . Moreover, it is also noted that although some attribute may be uniquely identifying on its own, "any attribute can be identifying in combination with others, while no single element is a (quasi)-identifier, any sufficiently large subset uniquely identifies the individual". The proposed mobile health monitoring scenario provides a good opportunity for adversaries to obtain a large set of medical information, which could potentially lead to identifying an individual user. Indeed, several recent works have already shown that even seemingly benign medical information such as blood pressure can be used to identify individual users. Furthermore, it is also observed that future mobile health monitoring and decision support systems might have to deal with other much more privacy-sensitive features such as DNA profiles , from which an adversary may be able to reidentify an individual user . Traditionally, the privacy issue is tackled with anonymization technique such as -anonymity or -diversity.

However, it has been indicated that these techniques might be insufficient to prevent reidentification attack . The threat of reidentification is so serious that legal communities have already been calling for more sophisticated protection mechanism instead of merely using anonymization. We believe that our proposed cryptographic based systems could serve as a viable solution to the privacy problems in mHealth systems, and also as an alternative choice for those privacy-aware users. 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 become a great challenge, which should be carefully investigated.

As an important remark, our design here mainly focuses on insider attacks, which could be launched by either malicious or nonmalicious insiders. For instance, the insiders could be disgruntled employees or healthcare workers who enter the healthcare business for criminal purpose .It was reported incident rate of insider attacks is rapidly increasing. The insider attacks have cost the victimized institutions much more than what outsider attacks have caused. 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 . On the other hand, while outsider attacks could be trivially 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.

The problem becomes especially trickier for cloud-assisted mHealth 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 (which will be referred to as *the company* in the subsequent development). In this paper, we design a cloud based Health monitoring system . Identification of the design problems on privacy preservation and then provide the solutions. To ease the understanding, start with the basic scheme so that we can identify the possible privacy breaches. The resulting improved scheme allows the mHealth service provider (the company) to be offline after the setup stage and enables it to deliver its data or programs to the cloud securely. To reduce clients' decryption complexity, outsourcing decryption technique is used. To relieve the computational complexity on the company's side, a further improvement has been proposed, leading to our final scheme. It is based on a new variant of key private 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, further reducing the computational and communication burden on clients and the cloud.

II. SYSTEM MODEL

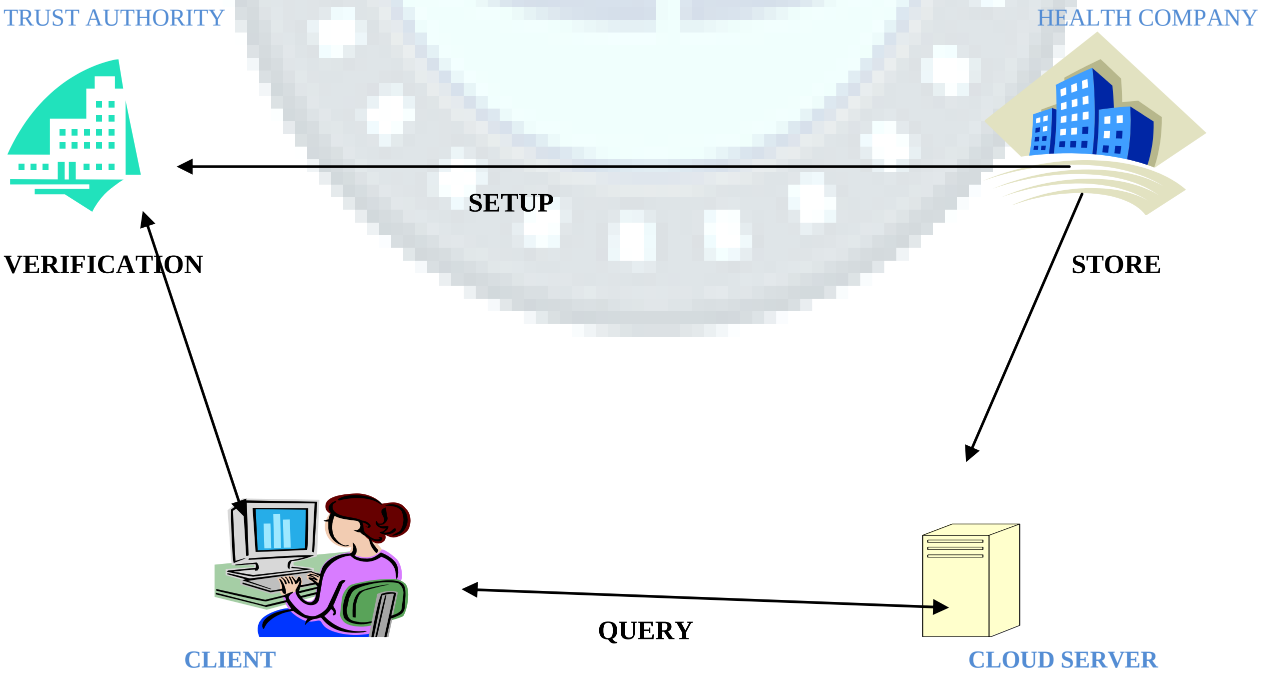
A. *Branching Program*

Since our mHealth monitoring program CAM builds upon branching programs, we first illustrate how a branching tree works. We use the monitoring program introduced in the MediNet project to construct a branching program . The MediNet aims to provide automatic personalized monitoring service for patients with diabetes or cardiovascular diseases. Clients input their related health data such as systolic blood pressure (BP), whether they missed daily medications or have an abnormal diet, and the energy consumption of physical activity to the decision support system, which will then return a recommendation on how the clients can improve their conditions. For instance, assume a hypertension patient input an attribute vector consisting of the following elements "[Systolic BP: 150,Missed one medication=0 (indicating he did miss the medication)Energy expenditure:900 kcal, salt intake:1000 milligrams]" and the respective threshold "t1=130 ,t2=0, t3=700 kcal,t4=1500.The recommendation returned from the monitoring program would be " D1,D2,D3" (by following the path through comparing each attribute element with the respective threshold, which indicates the client needs to "notify next kin, modify daily diet, and take regular medication".

As we can observe, a monitoring program can be modeled as a binary decision tree based on the range of the monitored measurement. We can represent measured data as an *attribute vector* and then construct the binary branching tree with the leaf nodes as the final consultation to design the medical decision support system. Let be a client's attribute vector v=(v1,v2,v3) be a client's attribute vector. An attribute component is a concatenation of an attribute index and the respective attribute value. For instance, A||KW1 might correspond to "blood pressure: 130", which means that the client's blood pressure 130. Each attribute value is a C bit integer. In this proposal, we choose to be 32, which should provide enough precision in most practical scenarios.

B) *Proposed Model for mhealth system*

With the binary programs illustrated earlier, we now highlight our design of the proposed cloud based mHealth monitoring system. It 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*), and a semi trust authority (TA). The company stores its encrypted monitoring data or program (branching program) in the cloud. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud through a mobile (or smart) phone. 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 the four major steps: setup, store, verification and query .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. At the initial phase, TA runs the setup phase and publishes the system parameters. Then, the company first characterizes the flow chart of a mHealth monitoring program as a branching program , which is encrypted under the respective directed branching tree. Then the company will deliver the resulting cipher text and its company signature to the cloud, which corresponds to the algorithm in the context. When a client wishes to query the cloud for a certain mHealth monitoring program, the client and TA run the algorithm. The client sends the company signature and the message to TA, and then inputs its private query (which is the attribute vector representing the collected health data) and TA verifies the message which is send. The client obtains the token corresponding to its query input while TA gets no useful information on the individual query. At the last phase, the client delivers the token for its query to the cloud, which runs the phase. The cloud completes the major computationally intensive task for the client's decryption and returns the partially decrypted cipher text to the client. The client then completes the remaining decryption task after receiving the partially decrypted cipher text and obtains its decryption result, which corresponds to the decision from the monitoring program on the client's input. The cloud obtains no useful information on either the client's private query input or decryption result after running the phase. Thus the system can prevent the cloud from deducing useful information on client's query corresponding to the received information from the client.



Proposed system architecture for cloud based heath monitoring system.

C. Adversarial Model

The assumption here is that a neutral cloud server neither colludes with the company nor a client to attack the other. This is a reasonable model since it would be in the best business interest of the cloud for not being biased. Clients may collude with each other. We do not consider the possible side-channel attack due to the co- residency on shared resources either because it could be mitigated with either system level protection or leakage resilient cryptography. Thus, our design assumes an honest but curious model, which implies all parties should follow the prescribed operations and cannot behave arbitrarily malicious. Moreover, we also target at the insider attack, which could be launched by either malicious or non malicious insiders who behave normally, but intend to discover information about the others' information. For instance, the insiders could be disgruntled employees, or the healthcare workers who have entered the healthcare business with criminal purposes. It was reported that 32% of medical data breaches in medical establishments between January 2007 and June 2009 are due to insider attack, and the incident rate of insider attacks is rapidly increasing. The insider data breaches are also reported to cost the victimized institutions much more compared with the breaches due to outsider attacks. Furthermore, insider attacks are generally considered much harder to detect and trace since attackers are generally sophisticated professionals or even criminal rings who are adept at making victims incapable of detecting the crimes. On the other hand, while outsider attacks could be trivially prevented by directly adopting cryptographic mechanisms such as encryption, it is nontrivial to design a privacy-preserving mechanism against insider attacks because we have to balance the privacy requirements with normal operations of mHealth monitoring systems. The problem becomes especially tricky for cloud-assisted mHealth monitoring 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.

III. PRIVACY MECHANISM

This system addresses the important problem and designs a cloud-assisted privacy.

- This process is preserving mobile health monitoring system to protect the privacy of the involved parties and their data.
- The outsourcing decryption technique and a newly proposed key public key encryption is used.
- It shifts the computational complexity of the involved parties to the cloud without compromising clients' privacy and service provider's intellectual property.
- A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model.
- The TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual

interest with the company.However the company and TA could collude to obtain private health data from client input vectors.

The benefits of the system are:-

- Effectively protect the privacy of clients and the intellectual property of m-Health service providers.
- The proposed system reduces the workload of both the company and clients by outsourcing the majority of the computational tasks.
- Based the encryption technique, it protects the client's privacy.
- Our mechanism reduces the decryption complexity.
- It is cost and time effective process.

IV. ALGORITHMS

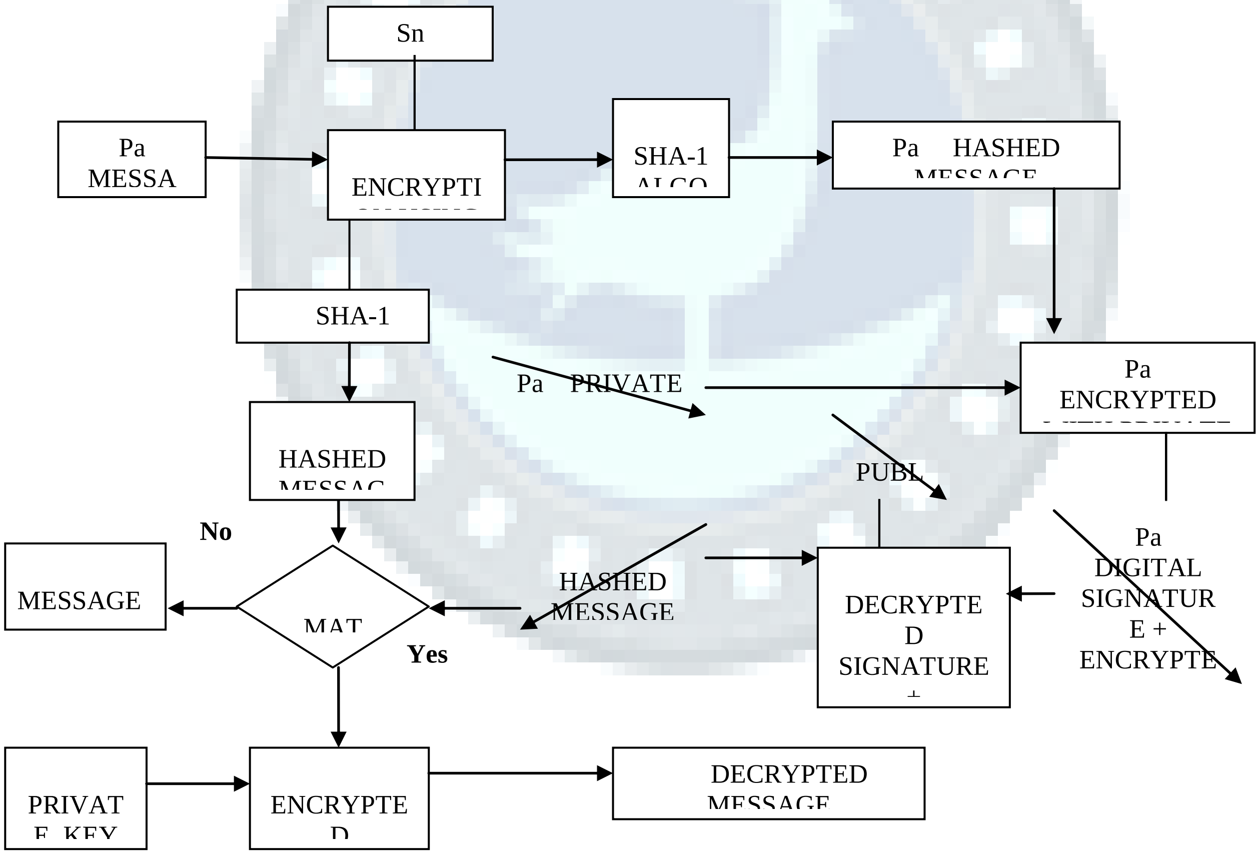
- Digital signature with RSA algorithm.
- Digital signature helps to check the integrity of the transmitted data.
- Using digital signatures helps to authenticate the message sender.

- The whole transaction is confidential as no other party can decrypt the data.

- Trusted Authority checks for non –repudiation.

ALGORITHM DESCRIPTION

RSA algorithm is a public key encryption technique. RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard,Adleman.The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. The encryption system is owned by RSA Security. The company licenses the algorithm technologies and also sells development kits. The technologies are part of existing or proposed Web, Internet, and computing standards.



BLOCK DIAGRAM

KEY GENERATION ALGORITHM

- Generate two random prime numbers P & q.
- Compute n=pq and ω(n)=(p-1)(q-1).
- Choose an integer e,where 1<e<ω and gcd(e,ω) is 1.
- Compute the secret exponent d, where 1<d<ω, ed mod ω=1 mod ω.
- The public key(n,e) and private key(n,d) .
- All value d,p,q,ω are secret.

ENCRYPTION

- Obtain the recipient B's public key(n,e).
- Compute cipher text (C)

$C=m^{e} \bmod n$ where m is the plaintext

DECRYPTION

- Done using the private key (n,d) of the recipient.
- Compute the Plaintext (m).

$M=c^{d} \bmod n$

V.DIGITAL SIGNATURE

A **digital signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

SECURE HASHING ALGORITHM

In cryptography,SHA-1 is a cryptography hash function designed by the United States National security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST.

SHA-1 produces a 160-bit (20-byte) hash value. A SHA-1 hash value typically forms a hexadecimal number, 40 digits long.

SHA stands for "secure hash algorithm". The four SHA algorithms are structured differently and are named *SHA-0*, *SHA-1*, *SHA-2*, and *SHA-3*. SHA-0 is the the original version of the 160-bit hash function published in 1993 under the name "SHA": it was not adopted by many applications. Published in 1995, SHA-1 is very similar to SHA-0, but alters the original SHA hash specification to correct alleged weaknesses. SHA-2, published in 2001, is significantly different from the SHA-1 hash function.

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols.

Digital signature with RSA algorithm

With public key encryption technique each user has two different keys one made available to the public and other is kept secret. One of the keys is used to encrypt a message and other is to decrypt a message. If Alice wants to send a secret message to Bob, for example she looks up Bob‛s public key and uses it to encrypt the message. Because Bob's public cannot undo the encryption process, no one who intercepts the message can read it.Only Bob who processes the secret key corresponding to his public key can read the message. Alice never has to meet Bob out of the hearing of others to exchange keys or passwords; this is a substantial improvement over older encryption method in which an exchange of private keys where necessary. This system can also be used as a means for Bob to be sure that the message comes from Alice. If Alice wants to sign a message she can encrypt it with her private key.When Bob receives an encrypted message which purports to be from Alice he can obtain Alice's public key and decrypt the message. If a readable message emerges Bob can have confidence that the message came from Alice because Alice 's public key would only properly unlock a message which was locked with her private key(Known only to Alice).Of course digitally signing the message does not make the content of the message private because anyone with Alice's public key can read a message she encrypted with her private key.

Alice can send a private, signed message to Bob however, by first encrypting the message with Bob's public key(so only Bob can read it with his private key) and then encrypting the message second time with her private key forming her signature. Anyone who receives the message can use Alice's public key to undo the second encryption, but only Bob(or someone with Bob's private key) can undo the first encryption step and actually read the message. All these complex sounding manipulations can be made manageable with well written software.

VI. CONCLUSION

A cloud based health monitoring system which can effectively protect the privacy of the clients and intellectual property of mhealth service providers has been designed. Clients privacy during message transmission is given the topmost priority. All the security aspects such as authentication (The user is trusted and registered), confidentiality (no other party can decrypt the data), integrity(message is not tampered during the transmission) and non-repudiation(none of the party can deny the participation

) has been incorporated..The proposed system so simple to implement that even small scale companies can also effectively use the system.

REFERENCES:

1)P Mohan,D Marin,S Sultan and A deen,"Medinet:Personalizing the self care process for patients with diabetes and cardiovasculat disease using mobile telephony.
2)A Tsanas,M Little,P Mcsharry and L Ramig ,"accurate telemonitoring of Parkinson's disease progression by noninvasive speech tests.
3)G Clifford and D Clifton "Wireless technology in disesase mamagement and medicine".
4)L Ponemon institute ,Americans opinion on health care privacy,2010[online].
5) A Narayanan and V Shmatikov, "Miths ans fallacies of personally identifiable information".
6)P Baldi, R Baronio ,"Countering gattaca :efficient and secure testing of fully sequenced human genome.
7)A Narayanan, V Shmatikov,"Robust De-anonimization of large sparse datasets".
8) A Narayanan, V Shmatikov ,"De-anonimizing social network".
9)J Domingo –Ferrer,"A three dimensional conceptual framework for database privacy".
10) T Lin ,"Nano sensors :Theory and applications in industry healthcare and defence".
11)K E Emam and M King, data breach analyzer 2009 (online).
12)E Shaw , K Ruby and J Post,"the insider threat to information systems :the psychology of the dangerous
13)J Brickell ,D Porter,"privacy preserving remote diagonostics".
14)A Farmer,O Gipson ,"A realtime mobile phone based telemedicine system to support young adults with type-1 diabeties.
15)A Sahai and B Waters,"Fuzzy Identity based Encryption".

AUTHORS PROFILE:

[1]. Ramya katanguri pursuing m.tech, Dept of CSE,From Ganapathi Egineering College.

[2].A.Ravi Kumar,working as Asst.Professor,Dept of CSE, Ganapathi Egineering College.