International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 1, January 2014

A Secured Patient Healthcare Monitoring in Cloud Infrastructure

Vaishnavi B[1], Yogeshwari R[2]

[1]PG Scholar, Faculty of Information and Communication Engineering,
MNSK College of Engineering, Vallathirakottai, Pudukottai-622305, Tamilnadu, India

[2]Assistant Professor Departments of Electronics and Communication Engineering,
MNSK College of Engineering, Vallathirakottai, Pudukottai-622305, Tamilnadu, India

Abstract: ***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. The patient's report will reach the doctor in encrypted format, by using the Identity Based Encryption (IBE) 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.***

Keywords: Patient Healthcare Monitoring, Identity Based Encryption, Outsourcing Decryption, Cloud Computing, mHealth.

1. Introduction

The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloud remains a tempting trend from a financial perspective, there are several other aspects that must be taken into account by companies before they decide to do so. One of the most important aspect refers to security: while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service/data can be placed in the cloud. Aiming to give a better understanding of this complex scenario, in this article we identify and classify the main security concerns and solutions in cloud computing, and propose taxonomy of security in cloud computing, giving an overview of the current status of security in this emerging technology [1].

2. Existing System

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 is to address this important problem and design a cloud-assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. Moreover, the outsourcing decryption technique and a newly proposed key private proxy reencryption are adapted to shift the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' intellectual property. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design.

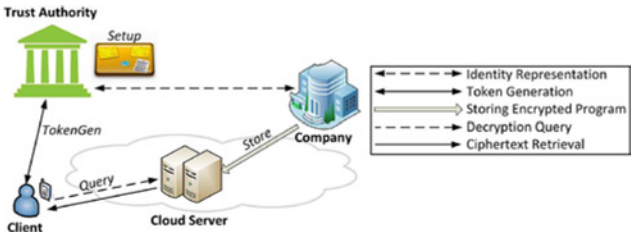

Figure 1: System architecture for Existing system

CAM consists of four parties: the cloud server (simply the cloud), the company who provides the mHealth monitoring service (i.e. the healthcare service provider), and the individual clients (simply clients), and a semi-trusted authority (TA). The company stores its encrypted monitoring data or program in the cloud server. 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 server through a mobile (or smart) device. 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 [2].

3. Proposed system

A secured patient healthcare monitoring in cloud infrastructure 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. The encryption and decryption format is the soul of this project. The patient's report will reach the doctor in encrypted format, by using the Identity Based Encryption algorithm (IBE) while a master key helps to deliver the report to the doctor in decrypted format. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as master key). Given the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for identity ID [3].

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. While the idea of database outsourcing is becoming increasingly popular, the associated security risks still prevent many potential users from deploying it. In particular, the need to give full access to one's data to a third party, the database service provider, remains a major obstacle. A seemingly obvious solution is to encrypt the data in such a way that the service provider retains the ability to perform relational operations on the encrypted database [4].

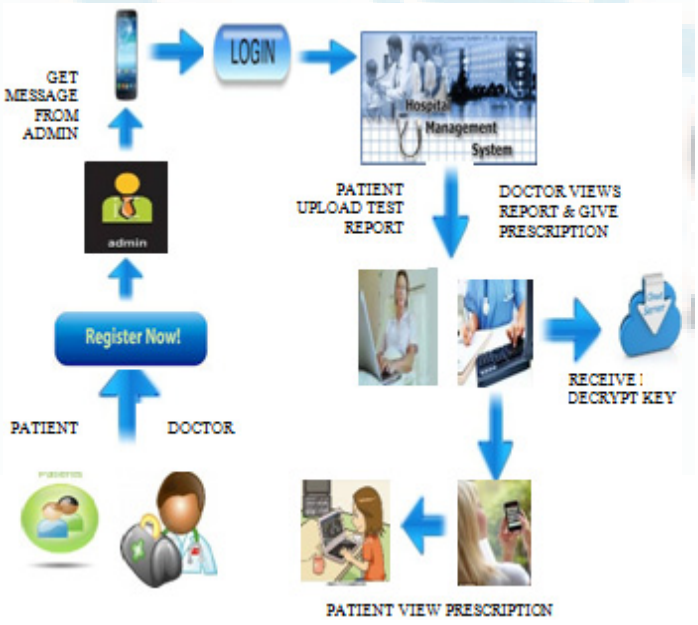

Figure 2: System architecture for proposed system

Registration is a mandatory process to get into a hospital management system for any doctor and Patient. A doctor and Patient have to provide their personal information to the patient healthcare monitoring to create their account. Admin will assess the given detail of a user and activates their account to view the patient healthcare monitoring. After activation the user get message from admin by their mobile. An existing user can directly login to the system with their valid user name and password. Activated User can enter into patient healthcare monitoring with their valid username and password. User should have all their test reports whatever related to their disease which was advised by the doctor earlier. Cloud area serves as a storage medium where all user records are being stored. When doctor login to the patient healthcare monitoring by providing their valid user name and password, they can view the history of a patient. When doctor wants to view the files of any patient, he will be finding all their reports in encryption format. To decrypt this test report doctor have to get the patient ID from the appropriate column. This ID, which is used as Doctor's key. This helps him to view the patient test report in decrypted format. Then doctor will decide the medicine to be prescribed, which will be entered by the doctor manually. This prescription to the user will be saved in cloud server in encrypted format. If the patient wants to view the doctor's prescription, user has to login into the patient healthcare monitoring.

4. Algorithms Used

4.1 Identity Based Encryption

Identity (ID)-based encryption, or IBE for short, is an exciting alternative to public-key encryption, which eliminates the need for a Public Key Infrastructure (PKI) that makes publicly available the mapping between identities, public keys, and validity of the latter. The senders using an IBE do not need to look up the public keys and the corresponding certificates of the receivers, because the identities (e.g. emails or IP addresses) together with common public parameters are sufficient for encryption. The private keys of the users are issued by a trusted third party called the private key generator (PKG) [5].

ID-based encryption (or identity-based encryption (IBE)) is an important primitive of ID-based cryptography. As such it is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). This can use the text-value of the name or domain name as a key or the physical IP address it translates to. Identity-based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as *master key*). Given the master public key, any party can compute a public key corresponding to the identity *ID* by combining the master public key with the identity

value. To obtain a corresponding private key, the party authorized to use the identity *ID* contacts the PKG, which uses the master private key to generate the private key for identity *ID*. As a result, parties may encrypt messages (or verify signatures) with no prior distribution of keys between individual participants. This is extremely useful in cases where pre-distribution of authenticated keys is inconvenient or infeasible due to technical restraints. However, to decrypt or sign messages, the authorized user must obtain the appropriate private key from the PKG. A caveat of this approach is that the PKG must be highly trusted, as it is capable of generating any user's private key and may therefore decrypt (or sign) messages without authorization. Because any user's private key can be generated through the use of the third party's secret, this system has inherent key escrow. A number of variant systems have been proposed which remove the escrow including certificate-based encryption, secure key issuing cryptography and certificate less cryptography.

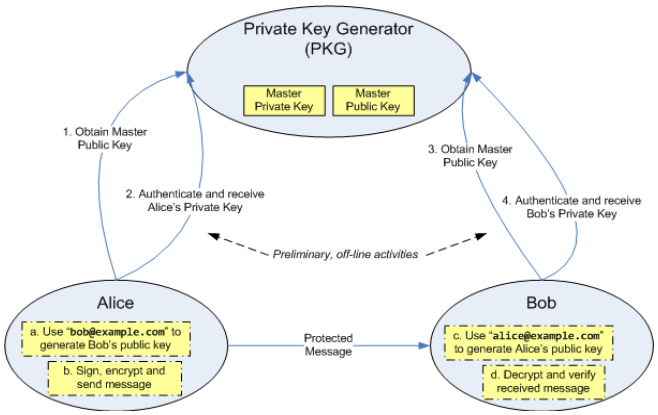

Figure 3: Steps for IBE

The IBE algorithm consists of four operations:

1. **Setup**, which initializes a key server. This algorithm is run by the PKG one time for creating the whole IBE environment. The master key is kept secret and used to derive users' private keys, while the system parameters are made public. It accepts a security parameter (i.e. binary length of key material) and outputs. A set of system parameter, including the message space and cipher text space and a master key.
2. **Key Generation**, which generates a private key for a given user. This algorithm is run by the PKG when a user requests his private key. Note that the verification of the authenticity of the requestor and the secure transport of are problems with which IBE protocols do not try to deal. It takes as input and an identifier and returns the private key for user.
3. **Encrypt**, which encrypts a message for a given user.
4. **Decrypt**, which given a private key, decrypts a message [3].

Identity-Based Encryption (IBE) dramatically simplifies the process of securing sensitive communications. For example, the following diagram illustrates how Alice would send a secure email to Bob using IBE:

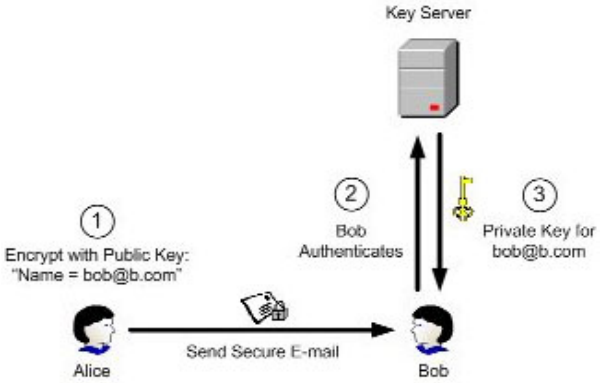

Figure 4: Example for IBE

Step 1: Alice encrypts the email using Bob's e-mail address, "bob@b.com", as the public key.
Step 2: When Bob receives the message, he contacts the key server. The key server contacts a directory or other external authentication source to authenticate Bob's identity and establish any other policy elements.
Step 3: After authenticating Bob, the key server then returns his private key, with which Bob can decrypt the message. This private key can be used to decrypt all future messages received by Bob [6].

4.2 Outsourcing Decryption

The idea of database outsourcing is becoming increasingly popular; the associated security risks still prevent many potential users from deploying it [4]. Attribute-based encryption (ABE) is a new vision for public key encryption that allows users to encrypt and decrypt messages based on user attributes. For example, a user can create a cipher text that can be decrypted only by other users with attributes satisfying ("Faculty" OR ("PhD Student" AND "Quals Completed")). Given its expressiveness, ABE is currently being considered for many cloud storage and computing applications [7]. As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). They develop a new cryptosystem for ne-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. They demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Their construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE) [8].

5. Experimental Result

Registration is a mandatory process to get into a hospital management system for any doctor and Patient.

Figure 5: User Registration

A doctor and Patient have to provide their personal information to the patient healthcare monitoring to create their account.

Figure 6: Admin updating

Admin will assess the given detail of a user and activates their account to view the patient healthcare monitoring. After activation the user get message from admin by their mobile. An existing user can directly login to the system with their valid user name and password. Activated User can enter into patient healthcare monitoring with their valid username and password.

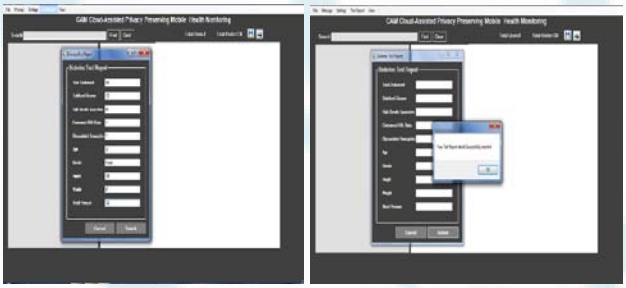

Figure 7: Patient upload test report

User should have all their test reports whatever related to their disease which was advised by the doctor earlier. Cloud area serves as a storage medium where all user records are being stored. When doctor login to the patient healthcare monitoring by providing their valid user name and password, they can view the history of a patient.

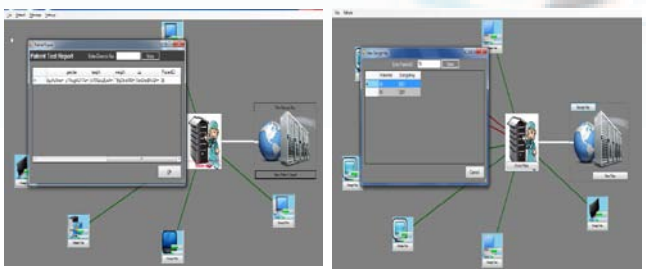

Figure 8: Doctor receives the ID & Private Master Key

When doctor wants to view the files of any patient, he will be finding all their reports in encryption format. To decrypt this test report doctor have to get the patient ID from the appropriate column.

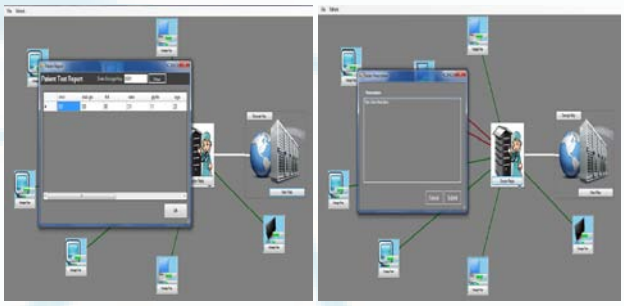

Figure 9: Doctor View the test report & gives prescription

This ID, which is used as Doctor's key. This helps him to view the patient test report in decrypted format. Then doctor will decide the medicine to be prescribed, which will be entered by the doctor manually. This prescription to the user will be saved in cloud server in encrypted format. If the patient wants to view the doctor's prescription, user has to login into the patient healthcare monitoring.

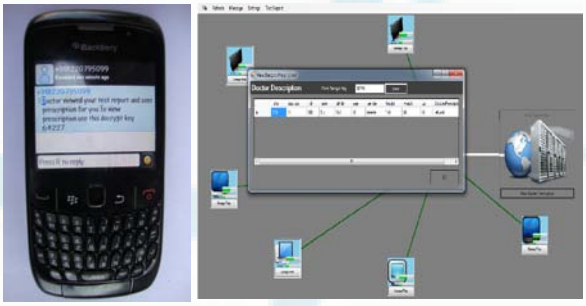

Figure 10: Patient get decrypt key & view prescription

Now the prescription will be in encrypted format. To decrypt they need a patient key. That will be sent to the given mobile number of the patient. Using patient key user can view the doctor's prescription.

6. Advantages

The identity-based encryption scheme is that if there are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed. The authenticity of the public keys is guaranteed implicitly as long as the transport of the private keys to the corresponding user is kept secure (Authenticity, Integrity, Confidentiality). When the receiver contacts the PKG to retrieve the private key for this public key, the PKG can evaluate the identifier and decline the extraction if the expiration date has passed. Generally, embedding data in the ID corresponds to opening an additional channel between sender and PKG with authenticity guaranteed through the dependency of the private key on the identifier.

7. Conclusion

Cloud Computing technology provides human advantages such as economical cost reduction and effective resource management. However, if security accidents occur, economic damages are inevitable. Our paper proposed "A secured patient healthcare monitoring in cloud infrastructure" for effective resource. Proposed method consists of Identity Based Encryption (IBE) in which a master key helps to deliver the report and Outsourcing Decryption Technique in which a master key helps to viewing the prescription.

8. Future Enhancements

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. We have proposed secure cloud architecture to address the user privacy problem in a cloud. By using OTP and WTP in cloud computing system, our proposed architecture achieves better goal of preserving the privacy of a user [9].

References

[1] Nelson Gonzalez, Charles Miers, Fernando Red´ıgolo, Marcos Simpl´ıcio, Tereza Carvalho, Mats Naslund and Makan Pourzandi "A quantitative analysis of current security concerns and solutions for cloud computing" Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012, 1:11.http://www.journalofcloudcomputing.com/content/1/1/11.

[2] 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.

[3] Wikipedia, "ID-based encryption", http://en.wikipedia.org/wiki/ID-based_encryption

[4] Sergei Evdokimov, Oliver G¨unther," Encryption Techniques for Secure Database Outsourcing", Humboldt-Universit¨at zu Berlin Spandauer str. 1, 10178 Berlin, Germany {evdokim,guenther}@wiwi.hu-berlin.de.

[5] Alexandra Boldyreva, Vipul Goyal,Virendra Kumar," Identity-based Encryption with Efficient Revocation", A preliminary version of this paper appears in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2008, ACM Press, 2008. This is the full version.

[6] Identity-based Encryption (IBE), Boneh-Franklin Algorithm.https://www.voltage.com/technology/identity-based-encryption/

[7] Matthew Green, Susan Hohenberger, Brent Waters, "Outsourcing the Decryption of ABE Ciphertexts".

[8] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data".

[9] Dr. Sandeep Sharma & Navdeep Kaur Khiva," Secure Cloud Architecture for Preserving Privacy in Cloud Computing using OTP/WTP", Global Journal of Computer Science and Technology Cloud and Distributed. Volume 13 Issue 3 Version 1.0 Year 2013.

Author Profile

B. Vaishnavi received her BE Computer Science and Engineering in 2012 from Anna University Chennai, Tamilnadu and pursuing ME Computer and Communication Engineering from Anna University, Chennai, Tamilnadu. Her area of interest includes Computer Network, Network Security and Cloud Computing.

R. Yogeshwari received her BE Electronics and Communication Engineering in 1998 from Periyaar Maniyammai college of Technology for women,Barathithasan university, Tamilnadu and ME Communication Systems 2009 from Barathithasan College of Engineering and Technology, Anna University, Trichy, Tamilnadu. She is working as a professor in Department of Electronics and Communication Engineering,MNSK college of Engineering,Pudukottai. She has more than 10 years of teaching and programming experience. Her area of interest include Wireless communication, Digital Communication and Signal Processing.