Elysium Journal
Engineering Research & Management

P-ISSN: 2347-4408
E-ISSN: 2347-4734

SECURE CLOUD ARCHITECTURE FOR HOSPITAL INFORMATION SYSTEM

Menaka.C[1], R.S.Ponmagal[2]
[1]Research Scholar
[2]Professor
[1]Bharathiyar University
[2] Dept. of Computer Science and Engineering
[2]Dr.MGR Educational and Research Institute, Chennai, Tamil Nadu, India
[1]menu_mca_03@yahoo.co.in
[2]ponmagal.rs@drmgrdu.ac.in

ABSTRACT

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. Hospital Information system such as Telemedicine is an important application which is recently gaining momentum on cloud. As telemedicine not only promises to dramatically reduce the costs, but at the same time it makes access to care easier for patients and makes more revenue attainable for practices. Despite cloud's attractiveness, it has got tremendous security concerns including accessibility issues, user authentication, confidentiality concerns, verification of data integrity, risk identification and mitigation, as well as insider threats from cloud provider staff. Precise identification of the patient/clinician during authentication process is a vital requirement for telemedicine cloud services as it involves sensitive physiological data. This paper proposes a secure cloud architecture which includes an authentication system for telemedicine cloud using a set of different unobtrusive physiological sensors (ECG) and web camera that continuously authenticate the identity of the user. This new type of authentication is called dynamic authentication. We further extend our result to enable the TPA to perform audits for multiple patients simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Keywords— Cloud computing, TPA, Telemedicine, authentication.

I. INTRODUCTION

Cloud Computing has been envisioned as the next-generation architecture of IT enterprise, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced into the Cloud. From users' perspective, including both individuals and enterprises, storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc. Although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. Thus, how to efficiently verify the correctness of outsourced cloud data without the local copy of data files becomes a big challenge for data storage security in Cloud Computing.

To avail the telemedicine services through cloud, it is necessary that the identity of the user who may be a patient or clinician need to be ensured throughout the session. This can be done using a process called as continuous authentication. In this kind of authentication static authentication is done when first accessing a cloud service and will be valid throughout a full session, until the user logs off from that session. Hence in this paper a continuous authentication scheme using ECG or keystroke along with facial recognition is used.

To fully ensure the data security and save the cloud users' computation resources, it is of critical importance to enable public auditability for cloud data storage so that the users may resort to a third party auditor (TPA), who has expertise and capabilities that the users do not, to audit the outsourced data when needed. Based on the audit result, TPA could release an audit report, which would not only help users to evaluate the risk of their subscribed cloud data services, but also be beneficial for the cloud service provider to improve their cloud based service platform. Section II discusses about the related issues, Section III details about the proposed system architectures. Section IV, explains the implementation part and Section V concludes the work.

P-ISSN: 2347-4408
E-ISSN: 2347-4734

II. RELATED WORK

Kallahalla et al. proposed [2] a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. By dividing files into filegroups and encrypting each filegroup with a unique file-block key, the data owner can share the filegroups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation.

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Considering TPA might [3] learn unauthorized information through the auditing process, especially from owners' unencrypted cloud data, new privacy-preserving storage auditing solutions are further entailed in the cloud to eliminate such new data privacy vulnerabilities. Moreover, for practical service deployment, secure cloud storage auditing should maintain the same level of data correctness assurance even under the condition that data is dynamically changing, and/or multiple auditing request are performed simultaneously for improved efficiency. Techniques we are investigating/developing for these research tasks include proof of storage, random-masking sampling, sequence-enforced Merkle Hash Tree, and their various extensions/novel combinations.

The situation that has been envisaged is where a user provides an identity and gives proof of his identity[4], in order to get access to certain medical services. To avail the telemedicine services through cloud, it is necessary that the identity of the user who may be a patient or clinician need to be ensured throughout the session. This can be done using a process called as continuous authentication

Guennoun, M et. al. [5] proposes a framework for continuous authentication of the user based on the electrocardiogram data collected from the user's heart signal. The electrocardiogram (ECG) data is used as a soft biometric to continuously authenticate the identity of the user. Continuous User Authentication Using Multimodal Biometrics for Cloud Based Telemedicine Application [6], is been discussed with two phases of algorithm.

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) the third party auditing process should bring in no new vulnerabilities towards user data privacy. We utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

Another concern is that the computation overhead of encryption linearly increases with the sharing scale. Ateniese et al.leveraged proxy reencryptions to secure[8] distributed storage. Specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key.

III. PROPOSED SYSTEM ARCHITECTURE

The cloud hospital information system called Telemedicine system is having a large amount of data to be stored in the cloud and the user is not able to check the integrity of the data which is stored in the cloud storage.

- Patient Members/Clinician: cloud user has a large amount of data files to be stored in the cloud
- Hospital Manager: cloud server which is managed by the CSP and has significant data storage and computing power.
- TPA: third party auditor has expertise and capabilities that Patient and Manager don't have. TPA is trusted to assess the CSP's storage security upon request from Patient/Clinician.

P-ISSN: 2347-4408
E-ISSN: 2347-4734

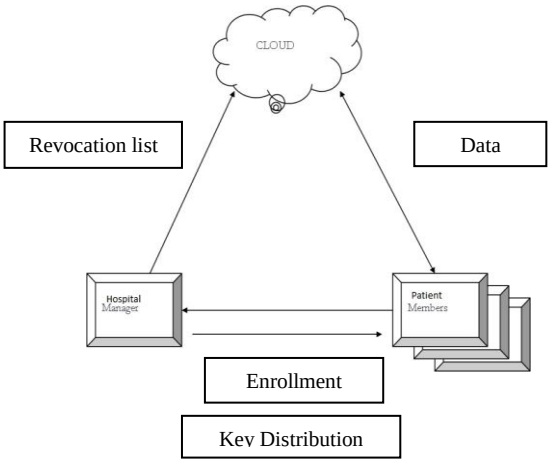

Fig 1. Secure Cloud Architecture

Each user has to compute revocation parameters to protect the confidentiality from the revoked users from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the ciphertext increase with the number of revoked users. To tackle this challenging issue, it is proposed that the manager compute the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the ciphertext size.

There are two phases in this proposed method. The registration and login process. Continuous Authentication (CA) systems represent a new generation of security mechanisms that continuously monitor the patient behavior/ physiological signal and use this as basis to re-authenticate periodically throughout a login session. Different technologies can be used to develop a CA system. In this paper a face recognition camera on a computer that can detect when a user has changed is the first biometric and ECG/keystroke can be used as the second biometric. These two can be combined to provide a robust and efficient authentication for the user.

3.1 Registration Phase:

Step 1: During Registration the user has to render the face and ECG/Keystroke Biometric and the features are extracted and stored into the biometric database of the server.

3.2 Login Phase:

Step 1: Acquire a frame containing face using web camera and imagegrab.
Step 2: Extract the facial features into a vector facial features[] using MATLAB from the acquired frame.
Step 3: Acquire ECG signal periodically through the ECG sensor and extract RR interval RR or extract key stroke characteristics from the key stroke biometrics.
Step 4: E_{ks}(RR, Facial_feature[], Request))
Step 5: Repeat steps 1,2 ,3 and 4 periodically within a session.
Step 6: During authentication the facial feature template extracted is verified against the template stored and the ECG/Keystroke features are compared with the previously acquired feature into the biometric database.

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

1. Periodic Sampling Batch Audit

The Batch TPA (or other applications) issues a "Random Sampling" challenge to audit the integrity and availability of outsourced data in terms of the verification information stored in TPA.

2. Audit for Dynamic Operations:

An authorized application, which holds data owner's secret key (sk), can manipulate the outsourced data and update the associated index hash table stored in TPA. The privacy of (sk) and the checking algorithm ensure that the storage server cannot cheat the authorized applications and forge the valid audit records.

3. Third Party Auditor

In this module, Auditor views the all user data and verifying data .Auditor directly views all user data without key. Admin provided the permission to Auditor. After auditing data, store to the cloud.

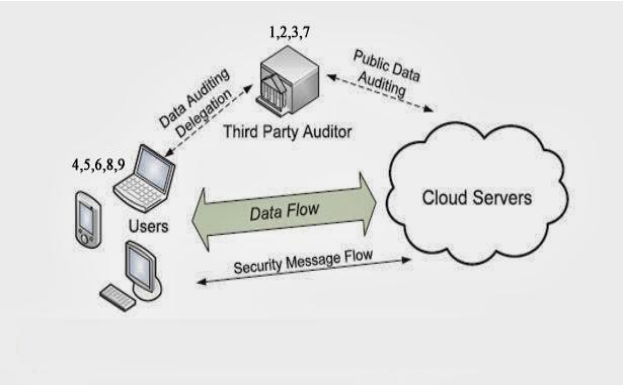

Fig 2. Third Party Auditing System Architecture.

P-ISSN: 2347-4408
E-ISSN: 2347-4734

4. User Registration and Control:

In this module, the user registration process is done by the admin. Here every user's give their personal details for registration process. After registration every user will get an ID for accessing the cloud space. If any of the user wants to edit their information they have submit the details to the admin after that the admin will do the edit and update information process. This process is controlled by the Admin.

5. Sharing Information's:

In this module, every user's share their information and data's in their own cloud space provided by the admin. That information may be sensitive or important data's. For providing security for their information every user's storing the information in their specific cloud. Registered users only can store the data in cloud.

6. Proxy Re-Encryption:

Proxy re-encryption schemes are crypto systems which allow third parties (proxies) to alter a cipher text which has been encrypted for one user, so that it may be decrypted by another user. By using proxy re-encryption technique the encrypted data (cipher text) in the cloud is again altered by the user. It provides highly secured information stored in the cloud. Every user will have a public key and private key. Public key of every user is known to everyone but private key is known only the particular user.

7. Integrity Checking:

Integrity checking is the process of comparing the encrypted information with altered cipher text. If there is any change in detection a message will send to the user that the encryption process is not done properly. If there is no change in detection means then it will allow doing the next process. Integrity checking is mainly used for anti-malware controls.

8. Data Forwarding:

In this module, the encrypted data or information stored in the cloud is forwarded to another user account by using that user's public key. If any user wants to share their information with their friends or someone they can directly forward the encrypted data to them. Without downloading the data the user can forward the information to another user.

IV. IMPLEMENTATION

A private cloud with minimum number of systems was developed by using a LAN connectivity. The cloud infrastructure is implemented successfully by using the Ultidev, a cloud deployment tool. The cloud user, auditor, cloud admin are using different systems. The file is uploaded by the user from a system and the auditor is able to check the integrity of the data from another system.

We also extended the work by performing batch auditing. Batch auditing is doing multiple auditing at the same time for different users. With computer networks spreading into a variety of new environments, the need to authenticate and secure communication grows. Many of these new environments have particular requirements on the applicable cryptographic primitives. For instance, several applications require that communication overhead be small and that many messages be processed at the same time. In this paper we consider the suitability of public key signatures in the latter scenario. That is, we consider signatures that are 1) short and 2) where many signatures from (possibly) different signers on (possibly) different messages can be verified quickly.We propose the first batch verifier for messages from many (certified) signers without random oracles and with a verification time where the dominant operation is independent of the number of signatures to verify. We further propose a new signature scheme with very short signatures, for which batch verification for many signers is also highly efficient. Prior work focused almost exclusively on batching signatures from the same signer. Combining our new signatures with the best known techniques for batching certificates from the same authority, we get a fast batch verifier for certificates and messages combined. Although our new signature scheme has some restrictions, it is the only solution, to our knowledge, that is a candidate for some pervasive communication applications.

We designed the work in ASP.Net and code is written in VB.net for front end designed. The reports in Crystal Reports is built in Micro Soft Visual Studio 2008. Vb.Net is very flexible and easy to understand any application developer. Microsoft SQL Server is a Structured Query Language (SQL) based, client/server relational database. Each of these terms describes a fundamental part of the architecture of SQL Server.

V. CONCLUSION

In this paper, we propose a secure cloud architecture system which has a number of applications including the health service for defense services wherein the health condition of the soldier can be continuously monitored with strong authentication. The defense personnel need not carry their health record along with them as the clinician or the defense personnel can access the health record from the cloud.

Privacy-preserving public auditing system for data storage security in Cloud Computing is also proposed where TPA can perform the storage auditing without demanding the local copy of data. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner, i.e., simultaneously. Extensive security and performance analysis shows that the proposed schemes are provably secure and highly efficient. We believe all these

P-ISSN: 2347-4408
E-ISSN: 2347-4734

advantages of the proposed schemes will shed light on economies of scale for Cloud Computing.

REFERENCES

[1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index. html, 2009.

[2] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[3] Justin J Sam ,V.Cyril Raj,"SystemPrivacy Preserving Third Party Auditing for Ensuring Data Integrity in Cloud Computing ", Proceedings of the National Conference NCICT2014.

[4] Zheng Hua Ten "Biometrics and the cloud",CWI-CTiF workshop on Cloud Communication and applications,2011, Copenhagen.

[5] M. Guennoun, N. Abbad, J. Talom, Sk. Md. M. Rahman, and K. El-Khatib, "Continuous Authentication by Electrocardiogram Data", 2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH 2009), ISBN: 978-1-4244-3877-8, 26-27 September, Toronto, ON, Canada, pp. 40 – 42, 2009.

[6] Rajeswari Mukesh, Continuous User Authentication Using Multimodal Biometrics for Cloud Based Telemedicine Application, Proceedings of the National Conference NCICT2014.

[7] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy- preserving audit and extraction of digital contents," Cryptol- ogy ePrint Archive, Report 2008/186, 2008.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at un- trusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.