ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Pervasive Cloud Based Healthcare Data Processing In Smart Cities

[1] Rajiv Kumar, [2] Chandra Suriyan, [3] Deepak Kumar, [4] Logeshwaran
[1][2][3][4] Department of computer Science and Engineering, VSB Engineering College, Karur, Tamil Nadu, India

***Abstract* – Nowadays, hospitals and clinics are using cloud computing to store the patient details. It is accessed by professional such as doctor and nurse in the hospitals. It can help the professionals to make the treatment in correct way. Access the information in remote location is necessary for the treatment to any patient. It is available in the cloud to access the information. Some security risks are involved in the m-health service. In today's world, cloud computing play a vital role in storing much information to access that in remote location. We can access the stored information from anywhere. Sometimes the information is stolen or modified by some hackers or intruders. To make a data secure in cloud we use optimal asymmetric encryption padding algorithm. Optimal Asymmetric Encryption Padding is a type of data encryption that produces a cipher text. The OAEP algorithm is used to process the original text to asymmetric encryption which uses oracle G. Treatment details stored in the cloud to reduce the patient from keeping the record safe in their daily life.**

1. INTRODUCTION

Cloud computing is an information technology that enables in all places access to shared pools of configurable system resource. It is a virtualization based technology that reduces the cost of the infrastructure. It provides a solution of storing information with pay as you go model. Top benefits of cloud are cost, speed, performance and reliability. In types of cloud, private cloud is used in the system. In medical field and health care, the patient information is stored in the cloud computing for further treatment. Moreover, the stored information is not secured in the cloud computing.It cannot prevent partial decryption of cipher texts by ensuring that an adversary of recover any portion of the plaintext. These healthcare services and applications generate copious amounts of big healthcare data in real time thus requiring computational resources. Over provisioned resource can be migrated by initiating a migration technique.

In this system we can implement the cloud that can store the patient detail to access it in a remote location. This system can store every information of patient and it will avoid the patient to keep the records safe in daily life. In the first visit the patient is assigned with separate id and password. Patient can go to hospital then the records are transferred to lab when the patients go for any test. We can use an OAEP algorithm to process the plain text with decrypting and keep the data in a secure manner. Optimal Asymmetric Encryption Padding is a network which is used with RSA algorithm. This algorithm can make the treatment details with security.

RELATED WORKS

1)Maomeng Su, Lei Zhang, Yongwei Wu, Member, Kang Chen, and Keqin Li, Fellow.

By using erasure coding, a systematic model is formally formulate data placement in multi-cloud storage. Applying non-linear programming and geometric space. Abstraction the problem of data placement optimization is addressed. Effectively balance
among different objectives in optimization by tritons.

2) J.Stanek, A. Sorniotti, E.Androulaki, and L. Kencl, "A secure data regeneration scheme for cloud storage", 2013.

This paper introduces a new cryptographic method for secure Proof of Ownership, based on the joint use of convergent encryption and the Merkle-based Tree, for improving data security in cloud storage systems, providing dynamic sharing between users and ensuring efficient data reduplication. Our idea consists in using the Merkle-based Tree over encrypted data, in order to derive a unique identifier of outsourced data. On one hand, this identifier serves to check the availability of the same data in remote cloud servers. On the other hand, it is used to ensure efficient access control in dynamic sharing scenarios.

3)J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer, "Reclaiming space from regenerate files in a server less distributed file system." in ICDCS, 2002, pp. 617–624.

It propose a solution, that provides both security and regeneration and retains benefits offered by each technique. ClouRegen makes use of convergent encryption but prevents the dictionary attacks. The

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

components involved in ClouRegen are: the basic cloud storage provider, a metadata manager and an additional server. by comparing the two cipher texts, check whether a file has already been stored or not.

4)P.Anderson and L. Zhang, "Fast and secure laptop backups with encrypted de-regeneration", 2010.

This present paper focuses on the security and efficiency of cloud storage, namely that clients outsource their data to cloud storage servers. While cloud storage offers compelling scalability and availability advantages over the current paradigm of "one storing and maintaining its own IT systems and data", it does not come without security concerns. This has led to studies on cloud storage security and efficiency.

5)M.Bellare, S.Keelveedhi, and T. Ristenpart, "Dupless Server aided encryption for deregenerated storage" 2013.

In our data integrity protocol the TPA needs to store only a single cryptographic key irrespective of the size of the data file F and two functions which generate a random sequence. The TPA before storing the file at the archive pre-processes the file and appends some metadata to the file and stores at the archive. To verify the truthfulness of the data at the time of verification the TPA uses this metadata. It is necessary to check the integrity of data with our proof of data integrity protocol.

6)Matthew MacDonald, "Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage".

This paper explains the integrity verification problem in regenerating-code-based cloud storage, especially with the functional repair strategy. It can allow a data owner to verify the integrity and repair the faulty servers. Considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing and reparation in the cloud can be formidable and expensive for the users.

7)Jeffrey Richter, "Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage Provable Data Possession at Untrusted Stores".

The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems.

8)Patrick Smacchia,"PORs: Proofs of Retrievability for Large Files".

To produce a concise proof that a user (verifier) can retrieve a target file F, by enable an archive or back-up service (prover) that is, that the archive retains and reliably transmits file data sufficient for the user to recover F in its entirety. POR protocol in which the verifier stores only a single cryptographic key irrespective of the size and number of the files.

9)Behrouz A Forouzan," MR-PDP: Multiple-Replica Provable Data Possession"

To increase the availability and durability of data on untrusted storage systems this systems rely on replication. It look like they are storing many copies of the data then storage system can collide.

10) James F. Kurose," HAIL: A High-Availability and Integrity Layer for Cloud Storage"

We introduce HAIL (High-Availability and Integrity Layer), a distributed cryptographic system that permits a set of servers to prove to a client that a stored file is intact and retrievable. HAIL strengthens, formally unifies, and streamlines distinct approaches from the cryptographic and distributed-systems communities.

11) Abraham Silberschatz," An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing"

In cloud computing, data owners host their data on cloud servers and users (data consumers) can access the data from cloud servers. Due to the data outsourcing, however, this new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud.

12) M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia," Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing"

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

13) H. Harney, A. Colgrove, and P. D. McDaniel," NCCloud: Applying Network Coding for the Storage Repair in a Cloud-of-Clouds"

To provide fault tolerance for cloud storage, recent studies propose to stripe data across multiple cloud vendors. However, if a cloud suffers from a permanent failure and loses all its data, then we need to repair the lost data from other surviving clouds to preserve data redundancy.

14) P. D. McDaniel and A. Prakash," Distributed data possession checking for securing multiple replicas in geographically-dispersed clouds"

It is important to ensure that each replica should have availability and data integrity features; that is, the same as the original data without any corruption and tampering. Remote data possession checking is a valid method to verify the replicas's availability and integrity.

15) T. Yu and M. Winslett," Remote Data Checking for Network Coding-based Distributed Storage Systems"

Remote Data Checking (RDC) is a technique by which clients can establish that data outsourced at untrusted servers remains intact over time. RDC is useful as a prevention tool, allowing clients to periodically check if data has been damaged, and as a repair tool whenever damage has been detected.

16) J. Li, N. Li, and W. H. Winsborough," Privacy-Preserving Public Auditing for Secure Cloud Storage"

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.

17) J. Anderson," Towards Secure and Dependable Storage Services in Cloud Computing"

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.

18) M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu," Network Coding for Distributed Storage Systems"

Application scenarios include data centers, peer-to-peer storage systems, and storage in wireless networks. Storing data using an erasure code, in fragments spread across nodes, requires less redundancy than simple replication for the same level of reliability.

19) E. Goh, H. Shacham, N. Modadugu, and D. Boneh," Signing a Linear Subspace: Signature Schemes for Network Coding"

Network coding offers increased throughput and improved robustness to random faults in completely decentralized networks. In contrast to traditional routing schemes, however, network coding requires intermediate nodes to modify data packets en route; for this reason, standard signature schemes are inapplicable and it is a challenge to provide resilience to tampering by malicious nodes.

20) G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Secure Network Coding Over the Integers"

Network coding has received significant attention in the networking community for its potential to increase throughput and improve robustness without any centralized control. Unfortunately, network coding is highly susceptible to "pollution attacks" in which malicious nodes modify packets in a way that prevents the reconstruction of information at recipients.

PROPOSED SYSTEM

This paper proposed that a security to store the patient details in cloud computing in medical field. Nowadays, hospitals and clinics are accessing a patient detail in the cloud. This will avoid the patient from keeping the detail of treatment with them. In this system, we keep the data and keep the record with secure. Optimal Asymmetric Encryption Padding is a padding scheme often used together with RSA encryption.

The OAEP algorithm is a network which can uses oracle G to process the original text to asymmetric encryption. this processing is proved in the random oracle model to result in a combined scheme when combined with any secure trapdoor one-way permutation f, this processing is proved and is semantically secure under chosen plaintext attack. OAEP is also proved secure against chosen cipher text attack when it is implemented with certain trapdoor permutation. OAEP can be used to build an all-or-nothing transform.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

OAEP satisfies the following two goals:

To convert a deterministic encryption scheme into a probabilistic scheme we can add an element of randomness. Prevent partial decryption of cipher texts (or other information leakage) by ensuring that an adversary cannot recover any portion of the plain text without being able to invert the trapdoor one-way permutation f.

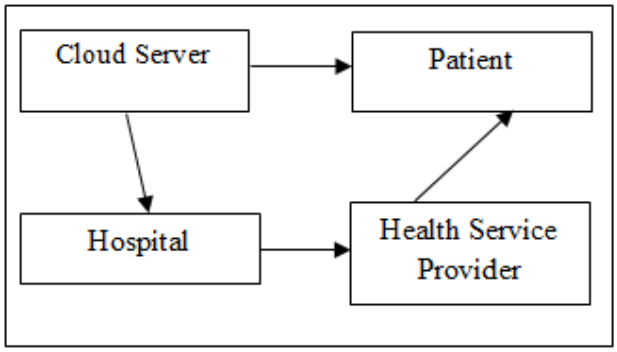
The "plaintext awareness" is showed by the original version of OAEP in the random oracle model when OAEP is used with any trapdoor permutation. Subsequent results contradicted this claim, showing that OAEP was only IND-CCA1 secure. When OAEP is used with the RSA permutation using standard encryption exponents, the original scheme was proved in the random oracle model as in the case of RSA-OAEP. An improved scheme that works with any trapdoor one-way permutation was offered to solve this problem. It is impossible to prove the IND-CCA2 security of RSA-OAEP under the assumed hardness of the RSA problem in the more recent work shown in the standard model.

BLOCK DIAGRAM

Level 0

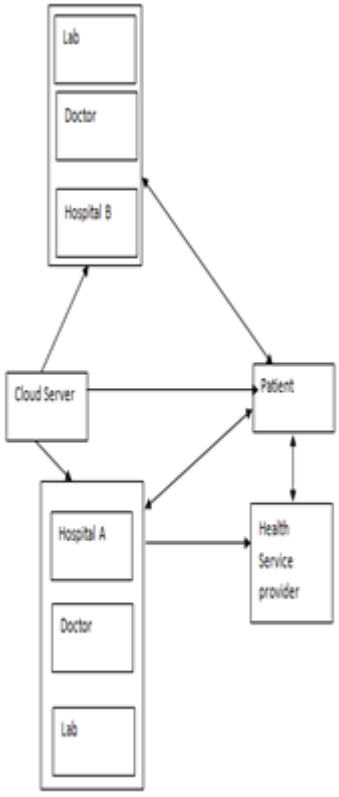
In this above diagram represents that patient information can be stored in cloud server. The data stored in the cloud will be accessed by the patient to see their treatment details and also hospital can access the information.

Level 1



All the patient details are stored in the cloud server. Patient and hospital professionals are access that stored information from anywhere at any time. Health service providers are professionals who are licensed to practice health care. Every details of patient are sending to concern labs or medicals to make the treatment and provide the necessary medicines. It will make the patient to free from taking the papers to every lab and medicals.

Level 2



This system can store the patient information by using their id and a password that is provide when their first visit. This system can be used in the particular hospital and it cannot share to the other hospital because sharing of hospital detail to other will cause security problem.

EXPERIMENTAL ANALYSIS

Cloud computing provides the application as services through the Internet and the systems software in the data centers that offer that services. The payment can be depend on the resources that the user used, such as network, server, storage, applications and services.

In this paper we present a CDA document generation system that generates CDA documents on different users and a CDA document integration system that integrates multiple CDA documents scattered in different hospitals

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

for each patient. The benefits of adopting this system are as follows. First, the system is accessible through an application and users can continue working on their location they are comfortable. Hospital systems can simply extend their existing system rather than completely replacing it with a new system. Second, it becomes unnecessary for hospitals to train their personnel to generate, integrate, and view standard-compliant CDA documents.

The cloud CDA generation service produces document in the CDA format has been approved. Third, if this service is provided for free at low price to hospitals, existing EHR are more likely to consider adoption of CDA in their practices. The integrated clinical document analysis is examined for mistake in the CDA validate, and the result is returned as string to the hospital that requested CDA document integration. This is because the CDA Integration System and the CDA Generation System are separate entities, and a new CDA document is made after document integration, hence it is necessary to determine whether the new document complies with the CDA document integration, especially whether there is any missing element, or the format is wrong. Mistake messages are returned if found. Then the received string is converted to a CDA document file and saved.

The outcome of the first module will be patient registration which will have the details about the patients on their name, mobile number, mail id, his last visit and his medical illness and all. Also we will generate the unique key using OAEP algorithm in this module which will be generated by the server which will be used for patient and hospital to access the details of the patients.

CONCLUSION AND FUTURE WORK

The approach employed in this paper is applicable in adopting other standards. If a hospital sends the content, admin archetype, and demographic archetype to the cloud server, then the server extracts necessary information from each case study. Next, it generates a structure that fits with a designated template and returns the structure to the requested hospital. In addition, patients are enabled to use the CDA document integration service to obtain Personal Health Record (PHR) which contains not only clinical documents but also Personal Health Monitoring Record and Patient Generated Document. Patients can effectively generate and manage their PHR by using our cloud-based CDA document integration service. The following problems were encountered while developing our CDA document generation and integration system. The format of a hospital can be converted to native format so that the other hospitals can easily see the details of other hospitals too. We are generating a medication automatically so that when the report of a user is given as input, it will be analyzed to recommend their disease and their medication.

First, we will make a concrete estimation of the reduction in cost when the patient details maintenance system becomes cloud-based. Establishing a reasonable fee system is an important issue for cloud computing. There is ample evidence that cloud computing is effective and efficient in cost reduction, and the medical field seems to be no exception. Security and stability is top priority for cloud computing resources as it is used by many users. Future work will attempt to enhance security while ensuring reasonable quality of service even with multiple users logged on the system at the same time.

REFERENCE

1)Maomeng Su, Lei Zhang, Yongwei Wu, Member, Kang Chen, and Keqin Li, Fellow.

2)J.Stanek, A. Sorniotti, E.Androulaki, and L. Kencl, “A secure data regeneration scheme for cloud storage”, 2013.

3)J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer, “Reclaiming space from regenerate files in a server less distributed file system.” in ICDCS, 2002.

4)P. Anderson and L. Zhang, “Fast and secure laptop backups with encrypted de-regeneration”, 2010.

5)M.Bellare, S.Keelveedhi, and T. Ristenpart, “Dupless Server aided encryption for deregenerated storage” 2013.

6)Matthew MacDonald, “Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage”.

7)Jeffrey Richter, ”Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage Provable Data Possession at Untrusted Stores”.

8)Patrick Smacchia,”PORs: Proofs of Retrievability for Large Files”.

9)Behrouz A Forouzan,” MR-PDP: Multiple-Replica Provable Data Possession”.

10)James F. Kurose," HAIL: A High-Availability and Integrity Layer for Cloud Storage".

11)Abraham Silberschatz," An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing".

12)M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia," Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing".

13)H. Harney, A. Colgrove, and P. D. McDaniel," NCCloud: Applying Network Coding for the Storage Repair in Cloud-of-Clouds".

14)P. D. McDaniel and A. Prakash," Distributed data possession checking for securing multiple replicas in geographically-dispersed clouds".

15)T. Yu and M. Winslett," Remote Data Checking for Network Coding-based Distributed Storage Systems".

16)J. Li, N. Li, and W. H.Winsborough," Privacy-Preserving Public Auditing for Secure Cloud Storage".

17)J. Anderson," Towards Secure and Dependable Storage Services in Cloud Computing".

18)M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu," Network Coding for Distributed Storage Systems".

19)E. Goh, H. Shacham, N. Modadugu, and D. Boneh," Signing a Linear Subspace: Signature Schemes for Network Coding".

20)G. Ateniese, K. Fu, M. Green, and S. Hohenberger,"Secure Network Coding Over the Integers".