International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

Data Auditability and Data Dynamics for Secure Health Data Exchange Generation of Clinical Document Architecture(CDA) based on Cloud Computing

Komal R. Jadhav
Computer Department
R.C.Patel of Institute of Technology
Shirpur, India

Nitin N. Patil
Computer Department
R.C.Patel Institute of Technology
Shirpur, India

***Abstract*:- Cloud Computing is a promising service platform to access computing resources on demand over the Internet. It moves information and applications to the massive knowledge centers wherever data and services may be managed in an exceedingly far better manner than locally. In this way, users of cloud storage services do not physically maintain direct control over their data, which makes data security one of the major advantage of using cloud. Previous research work already allows data integrity to be verified without presence of the actual data file. When this verification is done by a trusted third party, the verification process is called as data auditing, and this third party is called an auditor. However, its use puts forth a lot of difficult problems associated with security, privacy and reliability of the overall system. In this paper, we focus on the problem of data-integrity verification (by a third party auditor) for the client's data residing on a cloud storage server (CSS). Here, we tend to optimize associate existing third party auditing protocol and create it immune to replace, replay and forge attacks launched by malicious insiders at cloud storage server. To firmly introduce a good third party auditor (TPA), the following two fundamental requirements have to be met: 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; The third party auditing process should bring in no new vulnerabilities towards user data privacy. We tend to utilize and unambiguously mix the general public key based mostly homo morphic authenticator with random masking to realize the privacy preserving public cloud data knowledge auditing system that meets all above requirements.**

Keywords—Health Information System (HIS), Cloud Computing, Hashing Algorithm, Auditing algorithm, Simple Object Access Protocol(SOAP).

I. INTRODUCTION

CLOUD computing is being intensively known as one of the most powerful innovation in information technology in recent age. By using reserve virtualization Cloud delivers us computing capital and services in a pay-as-you-go mode, where cloud envision to turn into as suitable to use alike to way of life utilities such as electrical energy usage, irrigate, telephone u and water in the near prospect. Today world is moving on digitization and cloud computing is best technology to handle the big data sets. Various cloud computing services are categorized into Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and last one is Software-as-a-Service (SaaS). Many global IT corporations now offer powerful public cloud services to users on a level from individual to venture all over the world various examples of this are Amazon AWS and IBM Smart Cloud. As we know the current growth and propagation of cloud compute is fast rising, debate and hesitation on the practice of cloud still there. Data security and data solitude are some of the main concern in the acceptance of cloud compute. Users lose their direct control on data when they amass data on cloud as compare to conventional systems [1].

In our future work we will address the problem of honesty confirmation for big data storage on cloud. We call this problem as data audit when the confirmation is conducted by a trusted third party i.e. TPA called as an assessor. From cloud users perspective it is named as auditing-as-a-service. In a remote confirmation scheme, the cloud storage server (CSS) cannot provide a valid honesty proof of a given amount of data to a verifier unless all this data is intact. To ensure integrity of user data store on cloud service provider, this support is of no less consequence than any data guard instrument deployed by the cloud service supplier (CSP), no matter how secure they seem to be, in that it will provide the verifier which is a piece of direct, trustworthy and real-timed cleverness of the honesty of the cloud user's information through a challenge request [2]. It is particularly not obligatory that data auditing should be conducted on. The three main contributions of our proposed work are described as follows:

1. Authorized third party auditing
2. Fine grained dynamic data updates
3. Auditability aware data scheduling

The health information that consists health of the patient, health care provided to that patient as well as the reaction of the patient to the provided healthcare can be stored as electronic health information in the form of longitudinal collection, thus forming an Electronic Health Record (EHR).Therefore, the implementation of HIE system is made to ensure successful maintenance of EHR, But there is also a problem of incompatibility between systems and also there are different characteristics involved in HIS Thus, there is a need to standardize the health information exchange between hospitals ensuring interoperability over health information. Therefore, the core of guaranteeing interoperability is to standardize the clinical document. The major commonplace for clinical documents is CDA that was established by Health Level Seven (HL7) CDA is that the core document commonplace, an XML document which holds the structure and semantics of clinical documents for health information exchange. The first version of CDA was released on 2001 and its second version was released on 2005. Many countries have done several successful projects adopting CDA. To improve interoperability, several active works are done supported open EHR [1][2].

More HIE system has to support CDA to establish confidence in interoperable Health Information Exchange. Moreover, the structure of CDA is too complex and the correct CDA Document production is difficult without the good understanding of the CDA standard and enough experience with it. Also, the HIS development platforms for hospitals take issue therefore greatly in such the simplest way that generation of CDA documents in each hospital invariably needs a separate CDA generation system. In addition to it, a hospital refuses to adopt a replacement system unless it's necessary for delivery of care. As a result, except for only few handful countries like New Zealand or Australia, the adoption rate of EHR is too low. To promote EHR adoption among hospitals, the USA government had implemented an incentive program called the Meaningful Use Program.

A CDA document that has the record for the diagnosing is generated, once a patient is diagnosed at a clinic. These CDA documents are going to be shared with alternative hospitals if the patient agrees. A person or a patient may shift his location from one place to another hence it is common for that patient to visit a number of different hospitals for check-in or treatment. The exchange of CDA document is invoked within the following cases: once medical personnel must study a patient's medical history; once referral and reply letters are drafted for a patient cared by multiple hospitals; once a patient is in emergency and also the anamnesis must be reviewed.

It takes a large quantity of your time for the medical personnel as a result of the number of changed CDA document will increase as a result of a lot of documents means knowledge area unit distributed in several documents. This positively delays the medical personnel in creating choices. Therefore, once all the CDA documents area unit integrated into one document, the medical personnel is intended to look at the patient's medical record handily in written account order per clinical section and also the Corresponding care service is provided a lot of effectively. Sadly for currently, a solution that integrates multiple CDA documents into one don't exist nonetheless to the best of our information and there practical limitation for individual hospitals to develop and implement a CDA document integration interface.

In this paper we show a CDA document generation system that generates CDA documents on different developing platforms for the interface to be platform independent and CDA document updating system that stores CDA documents over cloud. The benefits of implementing this system are as follows. First, the system can be accessed through an Open API and developers can continue working on their developer platforms they are specialized for example Java, .NET, or C/C++. Hospital systems can simply extend their existing system instead of completely replacing it with a new system. Second, the hospitals do not have to train their personnel to generate, integrate, and view standard-compliant CDA documents. The cloud based CDA generation service produces documents in the CDA format approved by the National Institute of Standards and Technology (NIST). Third, as these services are provided free of cost at low price to hospitals, existing Electronic Health Record are more likely to consider adoption of CDA in their practices [3][4].

II. LITERATURE SURVEY

In this section, we conduct literature survey of work done till now in this domain. Our literature survey is an independent summary of published research literature relevant to the topic of our consideration.

First work is by Attendees et al who consider public audit ability in provable data control replica for ensuring possession of records on un trusted storages. Attendees present a model in which RSA based homomorphism tag are used. With the assistance of this method public audit ability idea is achieved, But the problem with this model is so as to it does not support dynamic data operation and too suffer security problems. Another research by Wang careful dynamic data storage in a distributed scenario which is a better idea, he proposed challenge reply protocol can both determine the data rightness and locate possible errors but this model only measured partial support for dynamic data operation [1].

Kaliski obtained a proof of retrievbility representation. The main disadvantage of this model as it does not support public audit ability. Extended research on this done by Shacham and Waters design an improved PoR system with full proofs of security in the security model. In this model they use publicly verifiable homomorphism authenticators built from BLS signatures base on which the proofs can be aggregated into a small authenticator value by using this public irretrievability is achieved. The main concern comes in front with this is the author only consider static data files which are not preferable since our main concern is about big data files [2].

One research was there on MAC based scheme which has the inconvenience like the number of times a particular data file can be audit is limited by the number of secret keys that must be set a priori. So the difficulty arise here is once all likely secret keys are tired after that the user then have to get back data in full to recomputed and republish new MACs to TPA. Here in this system TPA also has to keep and keep well-versed state flanked by audits that is to maintain track on the exposed MAC keys. It can only support static data and cannot professionally deal with dynamic data at all so this is a big issue to be solved when making an allowance for large data [3].

HLA based scheme- There is need of system which can prove integrity of data without retrieving data blocks there. So there is another method obtainable that is HLA scheme was used for this reason. The only difference between HLA and MAC is that HLA can be aggregate. The main issue with this system is that data can be retrieve only if linear combinations of same chunk are used [4].

Ashish, presented purposeful use of electronic health records the road ahead. For active clinicians, the origins and certain effects of this rule could also be opaque. It might be useful to grasp the motivation behind the key parts of the purposeful use rules, wherever they're possible to require the U.S. health care system (and the obstacles on the way), and therefore the advantages and risks of a fast transformation from paper to electronic record systems [5].

D. F. Sittig, A. Wright, R. B. Ness et.al proposed the promise of the CCD: challenges and opportunity for quality improvement and population health. Interoperability is demand of recent Electronic Health Record (EHR) adoption incentive programs within the United Stares. One approved structure for clinical data exchange is that the continuity of care document(CCD). Whereas primarily designed to push communication between suppliers throughout care transitions, coded data at intervals the CCD square measure typically reused to combination data from utterly completely different EHR's [6].

A. Rabkin, I. Stoica, and M. Zaharia et.al presented a view of cloud computing that describes cloud computing. In this authors describes is to scale back that confusion by instructive terms, providing straightforward figures to quantify comparisons between cloud and traditional computing and distinguishing the highest technical and non-technical obstacles and opportunities of cloud computing [7].

S. Lee, J. Song, and I. Kim, projected clinical document architecture integration system to support patient referral and reply letters. Several Clinical Document Architecture (CDA) referrals and reply documents are accumulated for patients since the readying of the Health information Exchange System (HIE'S) Clinical information were scattered in several CDA documents and this took an excessive amount of time for physicians to read. Physicians in Korea pay solely restricted time per patient as insurances in Korea follow a fee for service model. Therefore, physicians weren't allowed comfortable time for creating medical decision, and follow-up care service was hindered. To handle this, authors tend to developed CDA Integration Template (CIT) and CDA Integration System (CIS) for the HIE'S. The clinical things enclosed in CIT were outlined reflective the Korean standard for CDA Referral and Reply Letters and requests by physicians [8].

S. R. Simon, R. Kaushal, P. D. Cleary et.al proposed correlates of electronic health record adoption in office practices: A wide survey within which despite rising proof that electronic health records (EHRs) will improve the potency and quality of medical aid, most physicians in office practice in the United States do not currently use an EHR. We tend to sought after to live the correlates of EHR adoption [9].

J.L ahteenmaki, J. Leppanen, and H. Kaijanranta proposed the establishment of the purposeful Use criteria has created a critical need for robust interoperability of health records. A universal definition of a Personal Health Record (PHR) has not been approved. Standardized code sets are designed for specific entities; however, integration between them has not been supported. The aim of this analysis study was to explore the hindrance and promotion of interoperability standards in relationship to PHR's to explain interoperability progress in this area. The study was conducted following the fundamental principles of a systematic review, with 61 articles used within the study. Lagging ability has stemmed from slow adoption by patients, creation of disparate systems due to speedy development to fulfill needs for the Meaningful Use stages, and speedy early development of PHR's before the mandate for integration among multiple systems. Findings of this study recommend that deadlines for implementation to capture Meaningful Use incentive payments area unit supporting the creation of PHR information, there by hindering the goal of high-level interoperability [10].

S. Kikuchi, S. Sachdeva, and S. Bhalla Proposed cloud computing model in PHR architecture. They stated that some practical and commercial Personal Health Records and some related services such as Google Health and Microsoft Health Vault have been launched. On the other hand, Cloud Computing has matured additional and become the most important streams to appreciate a simpler operational environment. However, there have been few studies in regards to applying Cloud architecture in the PHR explicitly despite generating volume data. They review on the general architecture design by applying the Cloud components for supporting healthcare record areas and clarify the required conditions to realize it [11].

M. Bellare introduced Health Information Privacy, Security, and Your EHR. If your patients lack trust in Electronic Health Records (EHR's) and Health Information Exchanges (HIE's), feeling that the confidentiality and accuracy of their electronic health information are at risk, they will not reveal health information to you. Withholding their health information could have life-threatening consequences. Digital health information is to attain higher health outcomes, smarter defrayal, and healthier folks, suppliers associated people alike should trust that an individual's health information is non-public and secure. EHR developer is responsible for taking the steps needed to protect the confidentiality, integrity, and availability of health information in your EHR system [12].

Sundararaman, K. Parthasarathi, Appa Rao et.al proposed a solution to monitor cardiovascular disease using personal digital assistant (PDA) and applying Grid Computing as a technology enabler. Medical staff can use an application in software as a service (SaaS) basis. The resulting solution provides some requirements of work; however, it focuses on a different solution thus not covering how vital data is acquired, i.e.

it should implement the ways to gather, method and distribute patient's vital data, from beside to remote accessibility [13].

Liu et al. have illustrated an EHR system developed in China to solve the challenges of preventive medicine and management of chronic diseases. The healthcare system based on a Cloud-computing architecture was developed and deployed in Xilingol county of Inner Mongolia. The system used several computing resources to deliver services over the healthcare network using the Internet. There are some challenges to the system like integrating different levels of the healthcare system which makes it difficult for obtaining the information needed to implement public health records and to manage chronic diseases [14].

Rodriguez-Martinez et al. have introduced MedBook, a platform to exchange EHR's and billing activities to assists patients, healthcare suppliers, and helthcare player's collaboration and knowledge exchange. MedBook has some benefits as it matches the US HIPAA standardization and privacy. MedBook is a SaaS platform built on top of open source cloud technologies and running atop an IaaS platform. The platform offers the full benefit of cloud computing. The server applications are implemented using different web services and web applications, Python, Django, PostgreSQL, HBase, and the Apache web server in order to benefit from each technology. MedBook uses Ubuntu Linux 10.04 for security assurance and MedBook Eucalyptus 2 for management and resource allocation which is considered one of the challenges in cloud computing. MedBook is constructed exploitation free cloud technology that grants users the liberty of customization, modification, and distribution. On the other hand, MedBook has limitations on its privacy and legislation status since it's built using open source cloud computing [15].

Hus et al. have proposed a solution for protecting personal health records in the cloud by encrypting patient data before sending them to the cloud. The solution proposes two encryption keys. The first key is owned by the user called "a right-to-decrypt code", while the second key is called "a substitute-key-half code." Thus, patient data stored in the cloud will be secure and will not be disclosed to anyone without proper authorization [16].

Fernndez-Cardeosa et al. have introduced a cloud-based solution for different scenarios of an EHR management system.The proposal lined a large hospital and a network of Primary care center. They estimated the cost of the implementation using the Amazon calculator tool. EHRs with no images have been migrated to the Cloud environment, because of the large size of the DICOM images. They said that the implementation might be dependent on the bandwidth of the center and the amount of money that health centers want to spend [17].

III. METHODOLOGY

A. *System Architecture*

Cloud is everywhere, and that we use cloud storage daily in several platforms. There are different ways through which cloud computing is intervened in our lives. We use cloud computing in several formats like storages, marketing, education, healthcare and much more. Google's Gmail is one in all the most effective examples for a cloud computing. You can access the files stored in Gmail through any device using web. There are plenty of cloud computing components we tend to use every day lik: Gmail, Dropbox, Spotify, Facebook, Google Drive, Amazon Web Service, One Drive. Cloud computing is a method wherever all the information, files and images are stored in a cloud storage. This data then is accessed from computer using net. There is no necessity for a hard drive to store the data. Also, the cloud storge allows several information when compared with the hard drive. The above-mentioned examples are stated in consumer perspective. When it involves business, it is different cloud. There are alternative ways using that we tend to implement it for business.

· Software as a Service (SaaS)

· Platform as a Service (PaaS)

· Infrastructure as a Service (IaaS)

Company or organization that value more highly to implement a software system for running the business by storing, accessing and delivering the data will use SaaS. Using internet, the business accesses the application. If a business wants the software available to all the employees in the office to access, then Platform as a Service (Paas) will be suitable. For example, Salesforce. Infrastructure as a Service (IaaS) works with a structure where the services can be rented out from a big cloud provider. For example, Netflix offers services to the Amazon customers because Netflix rented out cloud services from Amazon [3][4].

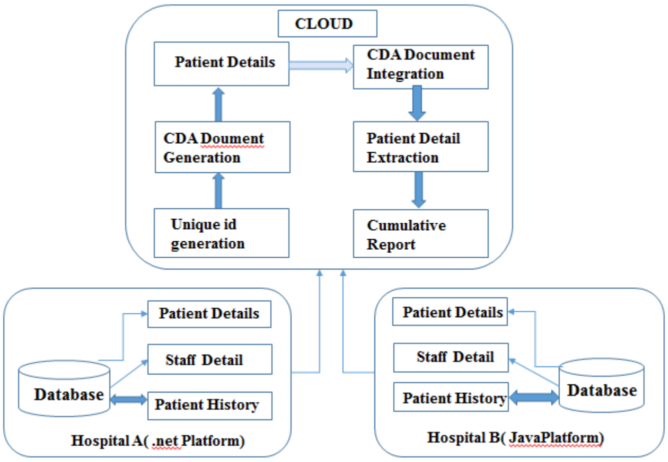


Fig. 1 System Architecture

XML is a great technology because it can deal with any data, any software system and any programing language. Due to the successes of this technology, XML start growing rapidly. SOAP protocol is XML-based that allowed applications exchange the knowledge over hypertext transfer protocol. W3C begin regarding about XML and SOAP security therefore, they implemented different solutions to secure their data which are as follow:

Encryption: Sensitive data can be encrypted using either symmetric or asymmetric cryptography. Although, the information is distributed within the clear; the encrypted part will be opaque and onerous to crack. The process and format of the encrypted XML data defines by W3C.

Authentication: SOAP services users' can be authenticated in many ways such as digest authentication and token-based authentication. Token based authentication requires users to supply credentials through a secure channel (i.e. request). SOAP servers respond with an authentication token which can be used for farther requests.

Digital signature: Signature is a technique to ensure the integrity of the data. SOAP messages either partially or the full documents are initial digestible. The digest, along with other sensitive data, is then digitally signed using the sender's certificate after that encrypted by the receiver's public key [5][6].

As the signature is encrypted using the receiver's public key, only the receiver can decrypt it then verify the signature and message digest. Signature or hash verification failure offers Associate in proof for manipulation throughout the transmission. However, several people have illustrated the weaknesses and drawbacks of SOAP. Even although, the options of SOAP-XML ar encouraging; the recent versions of SOAP aren't secure. The available security solutions are by hybrid approaches exploitation the prevailing security mechanisms like cryptography, digital signatures, tokens and etc [3][5].

B. Auditing Algorithm

Database auditing deals with observations and recordings chosen user actions. Auditing is often accustomed investigate suspicious activities and to watch and gather data regarding specific database activities. Auditing is very essential to healthcare informatics systems since it helps to maintain the integrity of a database, or, at least, to discover after the fact who had affected what values and when. Audit granularity becomes an important issue. While auditing events in operating systems are operations like "open file" or "call procedure," they are seldom as specific as "write record" or "execute instruction" For auditing to be useful, database audit trails must include accesses at the record, field, and element or table level [5][6].

A representative specification for cloud information storage is illustrated in Fig. 2. Three totally different network entities may be known as follows:

- Client: An Entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations;
- Cloud Storage Server (CSS): An entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the clients data;

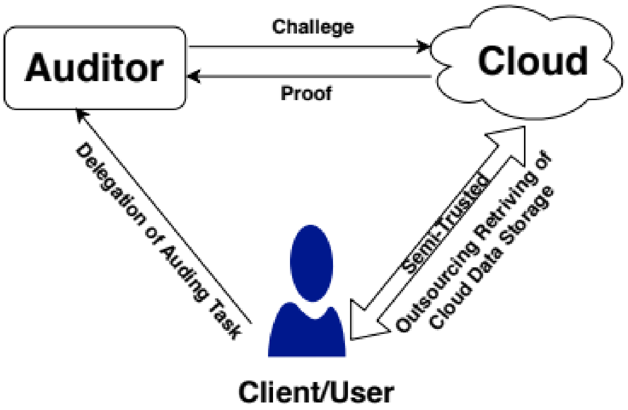

Challege
Proof
Auditor
Cloud
Delegation of Auding Task
Semi-Trusted
Outsourcing Retriving of Cloud Data Storage
Client/User

Fig. 2 Auditing Procedure

- Third Party Auditor (TPA): An entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request. In the cloud paradigm, by putting the large data files on the remote servers, the clients can be relieved of the burden of storage and computation. As purchasers not possess their information regionally, it is of critical importance for the client to ensure that their data are being correctly stored and maintained. That is, purchasers ought to be equipped with bound security means that so they'll sporadically verify the correctness of the remote information even while not the existence of native copies. In case those purchasers don't essentially have the time, feasibility or resources to monitor their data, they can delegate the monitoring task to a trusted TPA [7].

In this paper, we only consider verification schemes with public auditability: any TPA in possession of the public key can act as a verifier. We assume that TPA is unbiased whereas the server is untrusted. For application functions, the purchasers could move with the cloud servers via CSP to access or retrieve their pre-stored information. More significantly, in sensible situations, the client may frequently perform block-level operations on the data files. The most general forms of these operations we have a tendency to take into account during this paper area unit modification, insertion, and deletion. Note that we have a tendency to don't address the problem of information privacy during this paper, because the topic of information privacy in Cloud Computing is orthogonal to the matter we have a tendency to study here.

In past there have been lot of work has been done on cloud information security totally different techniques were accustomed offer security to cloud information however there are some disadvantages of such systems. Existing ways for safe guarding user information embrace encryption before storage and user authentication procedures before storage or retrieval of knowledge subsequently building secure channels for data transmission over the cloud. In this existing system the algorithms used are crypto logical and digital signature primarily based [7][8].

C. Problem Defination:

In preceding research it is shown that the cloud environment gives various advantages by providing infrastructure as a service and maintenance as a service. It relieves the load of user's task but security became a major concern in all time. User hires a TPA to check the integrity of the data store in a cloud server. But once more the matter arises whether or not the TPA is allowed or not. Another concern is connected to the utilization of resources in cloud surroundings. There are a number of resources as well as needs. There is no better way to serve the requests inside a particular time and with available reserve. Previously programing algorithm were performed during a grid however cut back the performance by requiring advance reservation of resources. In a cloud environment due to the scalability of capital, manually allocate resources to a task is not likely [9].

D. Work Flow of the System:

The new user first registers with application. After his/ her registration the user can access the account if and only if the user is authenticated by the Cloud Service Provider. The System has three dedicated logins for Data Owner, Third party Auditors and Cloud Service Provider. Cloud Service Provider Manages the users of applications. Users are like DO and TPA. This both users are authenticated by the CSP. If User is not authenticated by the CSP then user is not able to visit the account dashboard. After Successful login of the DO, DO can perform Several operations like, File upload, file Preview , File part Update, File Delete, Accept request proposal of the TPA, Grant access to file to the TPA, Hire TPA , Fire TPA. Views Notification form TPA about file updates. Here The User will upload the file, that file will be divided in to three parts, and three parts will get encrypted. Each time to Preview, Updating this respected parts are getting decrypted and previewed. Each time on any operation on file these multiple parts of file will get operated. The TPA can check the integrity of the file system only if that TPA is hired by the User. The TPA can Check the integrity of the file and sent the notification to the user account and email to the email Id provided by user at the time of Registration. The integrity check is performing by without revealing the contents" or file to the TPA. While updating the file the TPA cannot access the file integrity check. If the integrity of the file will be checked at the of file updating by DO that time the TPA will not be able to check the integrity of file, ass he will get any different result. This is done by the Priority Scheduling. The TPA will see the waiting screen for the same. To check the integrity of file we have created the SHA1 algorithm with our code. The SHA1 will give the 62 bit hash key which will be used for the cross verification of file safety. The encryption can be performed by the developing the AES algorithm to encrypt and decrypt the files and file parts of the File. Various phases of our proposed work using below Algorithm [10][11].

a. Key Generation Algorithm:

```
1. Start
2. Read Data owner id (udoid)
3. If(doid==udoid) (Execute step 4 to 10)
4. Read secret key (ssk)
5. Choose random number α from Zp(α <- Zp)
6. Choose random group generator (g) from Zp
7. Calculate v=gα
8. Display secrete key pair spk=(v, ssk)
   And Public key pair spk=(v,spk)
9. Update α value on alpha xml in sky drive.
10. Stop
11. Else
12. Stop.
```

b. Signature Generation Algorithm:

```
1. Start
2. Read data owner id (udoid)
3. If (doid ≠ udoid)
4. Stop
5. Else
6. Read file path (Fp)
7. Read No. of levels (n) for the construction of MHT
8. Calculate the block size of MHT =size of file/n.
9. Divide the file into NOB Bloks
10. For i=0;
11. For (i<=0) && (i>=NOB)
12. Calculate Hc[i] = enceyptsha1[block[i]]
13. Display hc[i]
  14. Choose random number u from set of group generators
      'G'
15. if (i<=0 &&i>=NOB)
16. Calculate Sig[i] = (hc[i]*)α
17. Display sig [i]
18. Construct MHT and generate Root node(R)
19. Generate signature for root node rootsign = (H(R))α
20. Upload file to web server
21. Update hash values & signature on TPA xml on Sky
Drive.
```

c. Data Integrity Verification by TPA Algorithm:

```
1. Start
2. Read data owner id(udoid)
3. If (doid ≠ udoid)
4. Stop
5. Read file name from AWS
6. Retrieve No. of blokes from TPA xml
7. Select the blocks number the user want to verify.
```

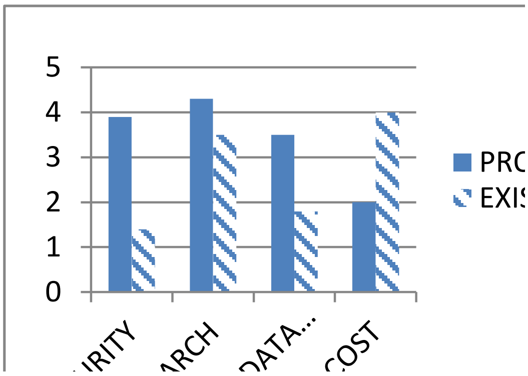
```
8. Get the auxiliary information for block chal from TPA xml
    9. Based on Auxiliary information generate new root for MHT
10. If (new root ≠ root) file modified
11. Else File not modified
12. Stop.
```

E. *Table and Graph*

Security monitoring on the cloud is important because computers sharing data are most readily available to an attacker. Without mechanisms in place to detect attacks as they occur, a system may not realize its security. Therefore it is vitally important that computers residing in the cloud are carefully monitored for a wide range of audit events. The auditing in a system consists of three steps. The first step is the attack has attempted on any node in a system , secondly, the attack is detected by the system by hashing algorithm after detection of attack the notifications are sent to the data owner. Due to this security is improved [18][19].

TABLE 1.

Sr.No.	ATTRIBUTES	PROPOSED SYSTEM	EXISTING SYSTEM
1	SECURITY	3.9	1.4
2	SEARCH	4.3	3.5
3	DATA CLUSTERING	3.5	1.8
4	COST	2	4



Graph 1.

CONCLUSIONS AND FUTURE WORK

The CDA document format for clinical information in traditional style to vow ability between hospitals this cloud computing. In this paper, we have a tendency to propose a privacy-preserving public auditing system for data storage security in Cloud Computing. Numerous of project works developed previously which can merely store data and share data between large numbers of user in a group. In our proposed work we have presented an third party auditing scheme to construct a secure data organization mechanism with high privacy protection method plus also working on audit ability conscious data preparation system which is based on priority. In this paper the main qualities are: (1) data security (2) privacy protection (3) audit details to the data owner (4) Auditability aware data preparation. For security and integrity of data cloud user ensure only the trust third party. How to guarantee trusting a third party we present an overview in this paper. TPA cannot derive user's knowledge throughout the method of public knowledge auditing as a result of it targeted on privacy-preserving for datasets. In future we have to improve more on security issues of data storage on cloud storage service. On cloud computing this topic is not negotiable to improve. For implementing that process we increase the layers of authentications to TPA.

REFERENCES

[1] Chang Liu, Jinjun Chen, Senior Member, IEEE, Laurence T. Yang, Member, IEEE, Xuyun Zhang,Chi Yang, Rajiv Ranjan, and Ramamohanarao Kotagiri , "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates." VOL. 25, NO. 9, SEPTEMBER 2014.

[2] A. Juels and B.S. Kaliski Jr., „„„PORs: Proofs of Retrievability for Large Files,"“ in Proc. 14th ACM Conf. on Comput. andCommun. Security (CCS), 2007, pp. 584-597.

[3] H. Shacham and B. Waters, „„„Compact Proofs of Retrievability,"“ in Proc. 14th Int‟l Conf. on Theory and Appl. of Cryptol. and Inf. Security (ASIACRYPT), 2008, pp. 90-107

[4] Q. Wang, C.Wang, K. Ren,W. Lou, and J. Li, „„„Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,"“ IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5,pp. 847-859, May 2011.

[5] K. Ashish, "Meaningful use of electronic health records the road ahead,"JAMA, vol. 304, no. 10, pp. 1709–1710, 2010.

[6] J. D. D'Amore, D. F. Sittig, A. Wright, M. S. Iyengar, and R. B. Ness, "The promise of the CCD: Challenges and opportunity for quality improvement and population health," in Proc. AMIA Annu. Symp. Proc., pp. 285–294, 2011.

[7] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[8] S. Lee, J. Song, and I. Kim, "Clinical document architecture integration system to support patient referral and reply letters," Health Informat. J., Published online before print Jun. 2014.

[9] S. R. Simon, R. Kaushal, P. D. Cleary, C. A. Jenter, L. A. Volk, E. G. Poon, E. J. Orav, H. G. Lo, D. H. Williams, and D. W. Bates, "Correlates of electronic health record adoption in office practices: A statewide survey," J. Am. Med. Inform. Assoc., vol. 14, pp. 110–117, 200.

[10] J. L€ahteenm€aki, J. Lepp€anen, and H. Kaijanranta, "Interoperability of personal health records," in Proc. IEEE 31st Annu. Int. Conf. Eng. Med. Biol. Soc., pp. 1726–1729, 2009.

[11] S. Kikuchi, S. Sachdeva, and S. Bhalla, "Applying cloud computing model in PHR architecture," in Proc. Joint Int. Conf. Human-Centered Comput. Environments, pp. 236–237, 2012.

[12] M. Eichelberg, T. Aden, J. Riesmeier, A. Dogac, and Laleci, "A survey and analysis of electronic healthcare record standards," ACM Comput. Surv., vol. 37, no. 4, pp. 277–315, 2005.

[13] C. Martınez-Costa, M. Menarguez-Tortosa, and J. Tomas Fernan-dez-Breis, "An approach for the semantic interoperability of ISO EN 13606 and OpenEHR archetypes," J. Biomed. Inform., vol. 43, no. 5, pp. 736–746, Oct. 2010.

[14] M. L. Muller,€ F. Ŭckert, and T. Burkle,€ "Cross-institutional data exchange using the clinical document architecture (CDA)," Int. J. Med. Inform., vol. 74, pp. 245–256, 2005.

[15] R. H. Dolin, L. Alschuler, C. Beebe, P. V. Biron, S. L. Boyer, D. Essin, E. Kimber, T. Lincoln, and J. E. Mattison, "The HL7 Clinical Document Architecture," J. Am. Med. Inform. Assoc., vol. 8,pp. 552–569, 2001.

[16] K. Huang, S. Hsieh, Y. Chang, F. Lai, S. Hsieh, and H. Lee, "Application of portable cda for secure clinical-document exchange," J. Med. Syst., vol. 34, no. 4, pp. 531–539, 2010.

[17] S. Lee, J. Song, and I. Kim, "Clinical document architecture integration system to support patient referral and reply letters," Health Informat. J., Published online before print Jun. 2014.

[18] Y. Kwak, "International standards for building electronic health record (ehr)," in Proc. Enterprise Netw. Comput. Healthcare Ind., 18–23, Jun. 2005.

[19] G.Ateniese, R.B. Johns,R. Curtmola, J.Herring, L. Kissner,Z. Peterson, and D. Song, „„„Provable Data Possession at Untrusted Stores,‟‟‟ in Proc. 14th ACM Conf. on Comput. andCommun. Security (CCS), 2007, pp. 598-609.