Research Journal of Applied Sciences, Engineering and Technology 10(5): 553-561, 2015
DOI:10.19026/rjaset.10.2463
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: November 19, 2014 Accepted: January 27, 2015 Published: June 15, 2015

Research Article

Dynamic Block Level Error Recovery to Trust Multimedia Data for E-learning Cloud Based Storage Services

R. Gopinath and B.G. Geetha
Department of Computer Science and Engineering, K.S. Rangasamy College of Technology, Namakkal District, Tamil Nadu, India

Abstract: The purpose of the study is to design a cloud storage service to detect the maximum probability of disrupted data blocks in a timely manner for any dynamic changes of multimedia data that does not affect the cloud environment. In the current scenario, the cloud environment must gain significant quality of service for data traversing from cloud to users. The e-learning cloud based system is always a night mare because of its security constraints as cloud application service don't give high percent of guarantee on data loss in secured layer of cloud environment. The user data stored on cloud always demands on how their private information is kept safe. This study focuses mainly on cloud data storage security for e-learning system, which has always been an important aspect of quality service. To make sure the correctness of users data within the cloud, an adaptable and effective methodology has been developed by handling dynamic data operations on the cloud data and recovery techniques are embedded by using forward error correcting algorithms applied to an e-learning web application. This extensive analysis shows that the end result which achieves blocks level data inclusion, deletion and searching dynamically along with recovery of data for malicious data modification attacks.

Keywords: Cloud computing, data integrity, data recovery, dynamic data operations, e-learning

INTRODUCTION

In today's world day by day internet usage is very high and there comes a mandate need for securing users and their data in a highly secure manner. This high level of usage also proportionally increases the data being transferred over the internet. To improve the data and network security, lot of new techniques and algorithms are emerging in parallel. Most of the application providers and vendors are increasingly moving into the path of cloud computing where it was believed that the data is being saved and maintained in a secured way. Cloud computing is an emerging industry wide accepted architecture which provides more flexibility in the form of sharing platforms, infrastructure and software applications within themselves. Depending on the mutual agreement between the cloud service provider and the companies it was vastly classified into various types based on the data availability and visibility. E-learning based applications are moving at a very faster rate into the implementation of cloud computing in the recent trend. Data security and integrity has become the primary objectives for these e-learning cloud applications moving forward.

Cloud computing is an emerging paradigm, but its security and privacy risks has been attracting significant attentions of cloud users and cloud providers. One of the important reasons is that cloud users have to trust the security mechanisms and configuration of the cloud provider. The classic intrusion detection mechanisms are not flexible enough to cope with cloud specific characteristics such as frequent infrastructure changes. Because of several attacks on cloud services like man-in-middle attack, delay attack and unauthorized access of data are major issues in cloud domain. There is no proper design for storing and retrieval of data on distributed cloud storage. So, the cloud storages that are designed using cryptographic techniques to audit multimedia data and to ensure the cloud user data on server is protected well. Thus, the challenge response protocol is design for storing and retrieval of data from cloud storage only for authenticated user (Gopinath and Geetha, 2013).

Cloud based e-learning applications demands more on the data availability in a secured fashion and in the meantime, the continuity of the business should not get affected. To improve the availability of the cloud data in a sequential manner, e-learning cloud content delivery model should be used for storing and accessing multimedia data like text, document, image, flash, audio and video. In this model, data to be transferred and stored in cloud will be considered as web objects and this model is a big change in traditional web based e-learning model to the latest cloud model. This model

Corresponding Author: R. Gopinath, Department of Computer Science and Engineering, K.S. Rangasamy College of Technology, Namakkal District, Tamil Nadu, India

may draw more attention for academia and research area and will be best suit for transferring the data in the cloud model. A content delivery model is a large distributed system of cloud server deployed in the data centers in the Internet (Guoli and Wanjun, 2010).

The goal of content delivery model is to serve content to cloud users with high availability and high performance. Content delivery model serve a large fraction of the internet content today by using web objects in developing vast applications in web, standalone, digital devices and mobile. The web objects are used in a distributed storage for content delivery. The cloud server is a single server servicing a number of users request to access content over a world wide area. The web objects transferred over the cloud environment to provide better quality of service. The public cloud services process the request of cloud user for data processing, storage and distribution. However, cloud users work with big data is a much challenging issue to move large volumes of data across cloud storage infrastructure. The data movement to cloud environment which depends on an efficient audit service for storing data and spot error checking in the distributed storage cloud computing. The protocol must be secure and supported by the public verifiability, whether the file gets corrupted and the server refuses to store in storage. As the number of cloud users request is high to store data in cloud storage, without leaving a copy in their local computer. So it should ensure that the data is not lost or corrupted. Here, the data integrity checking protocols is easy to check any modification of data block is identified and upload/download of data to be checked is secure from denial of attack (Wang *et al*., 2012; Zhu *et al*., 2013). Furthermore, the data integrity protocol challenges the cloud user about the integrity of a certain data file is uncorrupted and a cloud server generated responses proving that it has access to the complete original data file.

In cloud computing one of the core design principles is dynamic scalability, which guarantees cloud storage service to handle growing amounts of application data in a flexible manner or to be readily enlarged. Provable Data Possession (PDP) schemes evolved around public clouds offer a publicly accessible remote interface to check and manage the furious amount of data. It refers to the ability of a client to verify that data stored with a server still possesses the data without retrieving it. Cloud service provider is used to store and maintains the users data and a publicly verifiable PDP is used to verify the integrity and availability of their stored data in distributed storage. Dependencies should be uphold to facilitate the rapid deployment of cloud data storage service with security aggravation methods that to enable on-demand data correctness verification on behalf of cloud data owners has to be designed. The users are allowed to dynamically access and update their data for e-learning cloud applications and the verification process of PDP is seamlessly performed for the clients in public cloud service provider (Wang *et al*., 2013, 2011).

The public cloud service providers assure customers that they have regular and predictable access to their data and applications. It should available to all users at a time without any delay and reliable manner. The data availability is the major concern in cloud computing. Cloud must ensure that the data is available to user on demand at any time. The correctness and availability of the data files being stored using Reed-Solomon (RS) encoding method. The RS codes are used for error correcting codes that can be employed in cloud distributed storage. They are powerful error-correcting codes whose symbols are chosen from a finite field, $GF(n)$. A Reed-Solomon code is specified as $RS(m, k)$ with n-bit symbols. The RS encoding method can takes m data vector and adds k parity vector to make an encoded data file. The RS decode method can correct up to t symbols that contain errors in a codeword, where $2t = m - k$. Furthermore, if the data file of the block errors is identified as an erasure, the forward error correction can recover from any modification of data block (Tsai *et al*., 2011). The two complexity measures are considered: the computational complexity, measured in the number of system of linear equations that need to be solved and the communication complexity, measured in the number of encoded packets that need to be downloaded when data are retrieved from the distributed storage system. The detection and recovery require only solving systems of linear equations over a finite field $GF(n)$. The analysis ensures recovery from attacks even if a large fraction of the encoded packets are modified, but it does not scale up to very large systems in terms of computational complexity (Buttyan *et al*., 2011). Thus, the cloud user can upload/download their data in the cloud storage for an e-learning application and services are shared securely.

Cloud service provider has to consider importance of data privacy, integrity and availability and reliability issues. The issues in cloud distributed storage for a multimedia data that reside for a certain amount of period which is owned and maintained by the cloud service provider. In e-learning cloud, multimedia data files are shared among different users as services to have better learning environment. Cloud users access these resources available on "E-learning Cloud" to ensuring storage correctness across distributed storage. So, the cloud users can concentrate on their core active learning processes. The aim of proposed study detects the maximum probability of disrupted data blocks in a timely manner for any dynamic changes of multimedia data that does not affect the cloud environment. Also, the each corrupted file has to be audited periodically for corrupted file replacement and low bandwidth interruption of file downloads. Our approach helps to audit users data with cloud service provider and also enforce strong back-end protection for file recovery. Moreover, the main feature of our study is to audit

original copies of multimedia data without users knowledge.

The proposed system will be responsible to cover most of the key points in this field to consider distributed data storage security in cloud computing. The main contributions of the study are listed as:

- Proposed scheme achieves the integration of storage correctness and data error localization for dynamic data operations, i.e., the identification of misbehaving server (s) by introducing erasure code algorithms for dynamic data operations are inclusion, deletion and searching.
- Introduction of layered interleaving data encoding scheme achieves the time sensitivity packet recovery in the presence of burst loss.
- Provides a file replacement method for enabling e-learning web applications to be stored within the cloud with secure data storage assurance.
- The experiment results of the proposed scheme had proven that the suggested solution is highly efficient with data integrity during burst data packet loss. The detailed security analysis shows our scheme is reliable against Byzantine server failures and malicious external modification attacks.

MATERIALS AND METHODS

An effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users data in the cloud was proposed and it rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. The auditing is performed without demanding the local copy of data and thus drastically reduces the communication and computation overhead. The homomorphic linear authenticator and random masking protocol guarantees that the auditor could not learn any knowledge about the data content stored in the cloud server during the efficient auditing process (Wang *et al*., 2012). To retrieve the encrypted content in cloud storage, the retriever makes index terms from its private key satisfying the access policy made up of keywords associated with the content, where these index terms are only used for data accessing in the cloud storage system. This construction might drastically reduce the communication and storage overhead as compared to the traditional replication-based file distribution techniques. Their scheme also achieves the storage correctness insurance as well as data error localization, that is, whenever data corruption has been detected during the storage correctness verification, their scheme can almost guarantee the simultaneous localization of data errors. Later the extension of the work allows user to audit the cloud storage with very lightweight communication and computation cost (Wang *et al*., 2013; Koo *et al*., 2013). Our proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack and even server colluding attacks.

The role of third party auditor to verify the data integrity of the dynamic data stored in the cloud. The role of the verifier in this scheme presents two categories: private audit-ability and public audit-ability. The schemes with private audit-ability can achieve higher scheme efficiency but public audit-ability allows anyone to challenge the cloud server for correctness of data storage while keeping no private information. The verification protocol with public audit-ability is much important to achieve economies of scale for cloud computing. The third party auditor can periodically challenge the storage server to ensure the correctness of the cloud data and the original files can be recovered by interacting with the server. To achieve efficient data dynamics, the existing proof of storage models by manipulating the classic Merkle Hash Tree construction is used for block tag authentication. To support efficient handling of multiple auditing tasks, the bilinear aggregate signature technique is used in multi-user setting, where third party auditor can perform multiple auditing tasks simultaneously. This scheme is highly efficient and provably secures cloud data (Wang *et al*., 2011).

The cloud storage infrastructure provides users with easy interfaces and high performance services. Today, most of the enterprises will outsource their sensitive data for sharing in a cloud. To keep the shared data legal against un-trusted cloud service providers, a natural way is to store only the encrypted data in a cloud. The approach addresses to establish access control for the encrypted data and revoking the access rights from users when they are no longer authorized to access the encrypted data. Application of storage technology can significantly reduce the amount of cloud storage servers, thereby reducing system development costs, reduce the system caused by the server a single point of failure and performance bottlenecks, reduce data transmission link, to provide system performance and efficiency and ensure the overall system efficiency stable operation. The data management for cloud storage services have to meet user demands by providing transparent and reliable storage solutions (Wang, 2011).

In order to provide strong confidentiality for messages in storage servers, a user can encrypt messages by a cryptographic method before applying an erasure code method to encode and store messages. When user wants to use a message, user needs to retrieve the codeword symbols from storage servers, decode them and then decrypt them by using cryptographic keys. The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages. The tight integration of encoding, encryption and forwarding makes the storage system to meet the requirements of data robustness, data confidentiality and

data forwarding efficiently. The use of distributed key server increases the level of key protection, to decrypt a message of *m* blocks that are encrypted and encoded to n codeword symbols, each key server only has to partially decrypt two codeword symbols (Lin and Tzeng, 2012).

Earlier versions of model based algorithms mostly concentrates more on spot checking and error correcting code by means of introducing homomorphic tokens. To ensure possession of data in the cloud by an external attack was previously achieved by using various model based approaches like Proof of Reliability model and Provable Data Possession Model (Zhu *et al*., 2013). But later due to the advancement in the various approaches of security analysis, these model based approaches has became deprecated. The major disadvantages faced over this model based approaches are listed as computation overhead for an entire multimedia file and the unsecure data storages. Model based algorithms are usually fast to query but relatively slow to update. To overcome this, there has been recent work in privacy-preserving collaborative filtering that can enable Collaborative Filtering (CF) without leaking private information. In CF, achieving accuracy and preserving privacy are orthogonal problems. The two main directions of research in privacy-preserving collaborative filtering are: encryption based and randomization based techniques (Basu *et al*., 2012). In encryption based techniques, prior to sharing individual user data are encrypted using cryptographic systems that support homomorphic properties. In randomization based privacy preserving techniques, the ratings data is randomized either through random data swapping or data perturbation or anonymization. The introduction of security token during the file upload and download as per the proposed approach in this study greatly helps in avoiding all these problems. In the application of cloud computing and cloud storage, users are concerned more and more about security and privacy issues involved in the latest techniques. From industrial and academic viewpoints currently, cryptography is considered as a key technology to solve security and privacy problems.

In our previous work, the main idea proposed was to give review on research results of secure cloud storage in which error correcting algorithms and challenge response techniques have been used in their design. This methodology starts from reviewing the definition of cloud storage and subsequently review the existing secure cloud storage based on cryptographic techniques. Moreover, the system indicates what type of cryptographic techniques is mainly adopted in existing cloud storages and what role the cryptographic techniques play. Through this study, system can better catch what the relationship between secure cloud storage and cryptographic techniques and how about the application mechanism of cryptographic techniques in cloud storage. Hope this review can give some help for future research and more secure cloud storages by using cryptographic techniques can be proposed in the future. This concept of future work is actually implemented in the proposed work for ensuring data integrity in cloud (Gopinath and Geetha, 2013).

Cloud storage enables users to access their data anywhere and at any time. It can also comply with a growing number of regulations. However, it brings about many new security challenges. When users store their data in cloud storage, they are mostly concerned about whether the data is intact. This is the goal of remote data possession checking schemes. This methodology proposes, an algebraic signature based remote data possession checking scheme (Yang and Jia, 2012). Algebraic signature can improve efficiency and the running of algebraic signature can achieve tens to hundreds of megabytes per second. It allows verification without the need for the challenger to compare against the original data (Chen, 2012). The challenge/response protocol transmits a small, constant amount of data. The user needs to store only two secret keys and several random numbers. The algebraic property of algebraic signatures makes it possible to propose an efficient challenge updating method. Finally, experimental results reveal that the performance is bound by disk I/O and not by the algebraic signature or cryptographic computation, which enables it to be ideally suited for use in cloud storage.

The proposed system is a combination of homomorphic token generation along with the challenges received from the server stored in various locations to ensure data integrity in the cloud storage. The identification of misbehaving server will be an easy task to find the corrupted data in the cloud server by using the proposed scheme in our previous work (Gopinath and Geetha, 2013). As an extension of the previous study, the dynamic data operation for cloud data is applied in the recent work to check its data integrity. Recovery of data loss for various malicious attacks has been handled by introducing layer interleaving techniques.

Problem statement: The modern education systems grow much faster with the new advanced techniques to compete with today's user need. E-learning system also has become a major necessity nowadays for the users to update their knowledge up to date with the new advancements. Digital library, latest updates in the internet, e-books, Wikipedia are used by the end user in a vast manner to upgrade their knowledge. These upcoming advancements and the end users need have paved the way for the e-learning system to be deployed over the cloud servers. Cloud computing has gained a big boom in the information technology market to resolve lot of real world problems. The cloud system can be an infrastructure or software or else a platform where the users application are deployed and configured to access external systems. These external systems interact with users application by getting connected with a public web service to draw the graphs, mathematical

calculations, simulation, data migration and computation (Ivanova and Ivanov, 2010).

The cloud servers are usually maintained by private vendors to satisfy the application providers need. Big data and data virtualization are the best samples to illustrate the need for a cloud based system. The cloud based system can be major classified into various types depending on the permissions designed by the vendors. Public clouds are freely available and completely open to the outside world. Private cloud and hybrid cloud has their own permissions assigned to certain groups for accessing the application resources. Basically the service oriented architecture has opened the way for these modern trends for accessing external applications from the users application after some security checks. Today end user spends more time to browse and surf the internet to gather lot of future events and past proven concepts (Guoli and Wanjun, 2010).

The data to be stored in the cloud as multimedia files for e-learning purpose has to be placed in a secure manner. Cloud vendors are providing the access to their infrastructure, software and the platforms in an encapsulated manner but there comes a necessity to check how secure the user data is being stored. The data integrity has become a major factor to be taken care while designing an e-learning application on cloud. External intruders can be prevented by providing the application level security but the data in cloud has no guarantee that it is stored in a secure manner. Data security in cloud for an e-learning application can be applied by introducing homomorphic tokens for each and every user request (Peng *et al*., 2012). In parallel, the addition of various security algorithms can do the favor for us to prevent the data storage failures. But in real time applications, users cannot be restricted not to post many requests at an instance for data inclusion and deletion in the existing data stored in cloud. The dynamic changes in the existing stored data by the user have to get modified according to their actions performed in the application during the runtime.

Dynamic data operations like insertion, deletion, modification of the existing data stored in cloud has to adapt to these rapid changes. An adaptable and efficient methodology for handling dynamic data operations on cloud data has been designed by introducing the homomorphic tokens and by having the challenge response protocol for handling security constraints in cloud data. Additionally recovery techniques are also embedded by using the Forward Error Correcting algorithms to recover the corrupted data both internally and externally by the intruders. The recovery of data for malicious data modification attacks and byzantine attacks has been prevented by introducing layer interleaving data encoding scheme. This achieves time sensitivity packet recovery in the presence of burst data loss (Zhang *et al*., 2010). Zhang *et al*. (2010) by introducing all the above said techniques are used to avoid data loss even during the block level data inclusion and deletion dynamically. The file retrieval and recovery techniques has been explained in the below given system model portion to deep dive into those topics. The applied methodology largely helps to identify the data corruption and even the misbehavior of the servers due to server colluding attacks. The procedure for dynamic data operations and error recovery based on erasure correcting code technique was also given. Finally, the security analysis and performance evaluation results are shown to close of the study.

System models: The proposed system comprises of various system models including challenge token authentication, adversary model, dynamic data operations and layer interleaving encoding algorithm.

Challenge token authentication: The challenge-response authentication uses a cryptographic protocol that allows proving that the user knows the password without revealing the password. Using this method, the application first obtains a random challenge from the server. It then computes the response by applying a cryptographic hash function to the server challenge combined with the users password. Finally, the application sends the response along with the original challenge back to the server. Because of the "one-way" properties of the hash function, it is impossible to recover the password from the response sent by the application. Upon receiving the response, the server applies the same hash function to the challenge combined with its own copy of the users password. If the resulting value matches the response sent by the application, this will indicates with a very high degree of probability that the user has submitted the correct password. Since the server has no access to clear-text passwords, the challenge-response protocol described above is modified to use password hashes instead of the actual passwords. The exact authentication protocol works as follows:

- The application invokes the Get Challenge method with the user login name. The method returns an Auth Challenge object that contains a random challenge generated by the server and the password salt that should be used to obtain the hash of the users password.
- The application transforms the plain-text password entered by the user into a series of bytes by applying UTF-8 encoding. The application then appends the password bytes to the salt received from the server and computes the SHA-256 hash of the combined series of bytes. The resulting value is the password hash as in (1):

PasswordHash : = SHA-256 (PasswordSalt, UTF-8 (password)) (1)

- The application then appends the bytes of the password hash to the challenge bytes obtained from the server and computes the SHA-256 hash of the combined series of bytes. The resulting value is the response as in (2):

  Response : = SHA-256 (Challenge, PasswordHash) (2)
- The application invokes the Authenticate method with the original server challenge and response computed in the previous step. If authentication succeeds, Authenticate returns the authentication token to be included with subsequent requests to the server.

Adversary model: The cloud stored data can be corrupted by a third party external user simply by penetrating into the application through the security loop holes. There is no guarantee that the data inside the cloud storage is well secured as the cloud server vendors have that much secured infra structure implemented for the cloud servers. The foreign system as well as cloud server vendors may get into the data layer and can corrupt the stored cloud data either by modifying or deleting users data. A special ethical model is built by the customer to check whether the users data is secured or not in the cloud space. This adversary or antagonist model is responsible for corrupting the users data inside cloud storage (Gopinath and Geetha, 2013).

Initially this model gets into the system through various loop holes as an external user does and then will try to access the user data layer. After getting access into the data storage region, it starts corrupting the data continuously in the files stored in the various individual servers. This ethical adversary will be mainly used for checking the data integrity and correctness of data. The disruption of data will lead to take control over the application inside the cloud server. The continuous interruption may lead to damaging the cloud server database, space, business rules and network security layers by using the loop holes in each layer. This ethical model is just used only for testing and not to complaint on any cloud vendors vulnerabilities.

Dynamic data operations: The dynamic data operations model is mainly used for specific applications like digital libraries and scientific data repository. But in real world scenario, lot of potential dynamic application need are there like electronic documents, storing pictures, sharing mails, chats, online conversations and log files. To satisfy all these dynamic need, data stored in the cloud must be able to handle users dynamic data operations like inclusion, deletion and searching of data in a much secured manner. The data does not live in a local environment and it's being stored in cloud, so dynamic data operation handling will be big challenging task.

Since data do not reside at users local site but at cloud service provider's address domain, supporting dynamic data operation can be quite challenging. On the one hand, cloud service provider needs to process the data dynamics request without knowing the secret keying material. On the other hand, users need to ensure that the entire dynamic data operation request has been faithfully processed by cloud service provider. To address this problem, we briefly explain our approach methodology about layered interleaved encoding technique to ensure block level storage correctness to recover exact multimedia file. For any data dynamic operation, the user must first generate the corresponding resulted file blocks and parities. This part of operation has to be carried out by the user, since only he knows the secret matrix P. Besides, to ensure the changes of data blocks correctly reflected in the cloud address domain, the user also needs to modify the corresponding storage verification tokens to accommodate the changes on data blocks. Only with the accordingly changed storage verification tokens, the previously discussed challenge-response protocol can be carried on successfully even after data dynamics. The secured verification of homomorphic tokens help to ensure that cloud service provider would correctly execute the processing of any dynamic data operation without affecting cloud infrastructure. The secured layer of cloud infrastructure uses verification protocol to audit dynamic changes in the existing stored data by the user have to get modified according to their actions performed in the application during the runtime, it not only enhances the quality of resources but also reduces the overhead of communication, computation and storage cost. The idea of cryptographic technique and layered interleaved encoding protocol is applied in the design of cloud storage and it believes more secure cloud storage of encrypted multimedia files (Koo *et al*., 2013; Gopinath and Geetha, 2013). In this section, we will show how our scheme can explicitly and efficiently handle dynamic data operations for cloud data storage, by utilizing the linear property of Reed-Solomon code and homomorphic token verification.

Layer interleaving encoding-island algorithm: The island algorithm is an algorithm for performing inference on Hidden Markov Models. It calculates the marginal distribution for each unobserved node, conditional on any observed nodes. The island algorithm is a modification of belief propagation. The Belief propagation is also known as sum-product message passing. From Fig. 1 it illustrate that the smaller memory usage for longer running time, while belief propagation takes $O(n)$ time and $O(n)$ memory, the island algorithm takes $O(n \log n)$ time and $O(\log n)$ memory space. The algorithm computation facility with an unlimited number of processors can be reduced to $O(n)$ total time, while still taking only $O(\log n)$ memory.

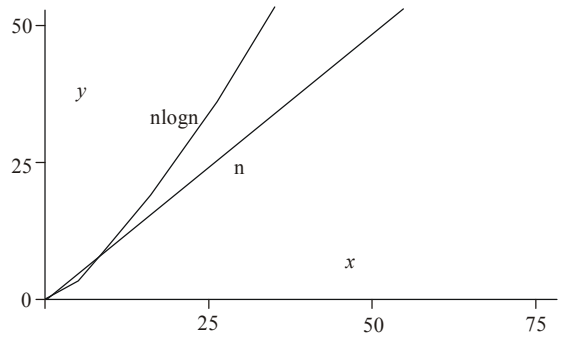

Fig. 1: A graphical demonstration of island algorithm

Algorithm: Island Algorithm

Input: Set of data files from e-learning application W_s
Output: Set of key terms T_s
Step 1: Read the data file given for training W_s
Step 2: Read stop word list S_w
Step 3: For the data file W_i from W_s
C = Read content of the data file W_i
C = Apply html parser to remove html tags from C
T_S = Split C with pattern single space
For each term T_i in the term set T_s
If T_i present in stop word list S_w then
Remove T_i from T_s
End
If (T_i contains "ing'')
T_i = Remove "ing'' from T_i
End
If (T_i contains "ed'')
T_i = Remove "ed'' from T_i
End
End
End
Step 4: For each T_i from T_s
Identify presence of bigram B_i
If B_i Presents
Update T_s
Else
Continue
End
End
Step 5: Return set of textual term set
Step 6: Stop

The idea of the island algorithm is to discard most of the forward messages α_t, storing them only at regularly-spaced intervals. The method is to store forward messages α_t at b-1 intermediate "checkpoints" or "islands", there by dividing the original sequence into b segments. Then the algorithm is recursively applied to each of the b segments between the stored vectors until it bottoms out in standard forward recursion over much shorter sequences after $d = log_b T$ files, where T is observation time. After producing the islands from left to right, the intervals are processed recursively from right to left, so that the first contiguous section to have all forward messages completed is at the end of the sequence. As each completed section is produced, the backward recursion can be applied and the posteriors computed. When the posteriors have been computed, the memory used to store the section can be overwritten to store the forward messages of the next section to the left. As the posteriors are produced from the end to the beginning of the sequence so backward probabilities need never be stored. The time and space complexity of island algorithm depends on the choice of d and b. Since for each forward messages α_t, it performs d times as much work in the forward pass. However, it requires storing only bd forward messages α_t at a time. On choosing a fixed b and set $d = log_b T$, then island algorithm requires O (n log n) time and O (log n) memory space. The Island algorithm manages to reduce the memory requirements dramatically while increasing the time slightly.

RESULTS AND DISCUSSION

The experiment is conducted for the multimedia files using Jelastic cloud server with better computing facility and it is much feasible for any cloud application as service.

Analysis on island algorithm file recovery: The interleaving is a technique for forward error correction use Reed Solomon erasure codes to control data loss for any multimedia data files over cloud storage. The layered interleaving process is an effective solution for the multimedia data for cloud storage environment. Thus, the island layer interleaving encoding algorithm carefully guess that the placement of data block to be treated differently from the legacy multimedia contents. When the file is recovered in scalable fashion and the dynamically changes does not affect the cloud environment with sequential access on the multimedia file data blocks (Dong *et al*., 2012). In the experiment, we measure the computation costs for file recovery at the cloud server varies when the block size are changed for different file type. The data size of small, medium and high in bytes is chosen. From Table 1, it shows the reconstruction of original file size in seconds. From the result of island algorithm, the reconstruction of original file size i.e., computation cost for the file size of 2-DM1 and 2-DH1, 2-DM3 and 2-DH3, 2-DM5 and 2-DH5 differs only by 115.2, 391.5 and 482.8 in sec respectively. Thus, the proposed study is possible to support scalable multimedia data in more efficient fashion from file systems point of view.

The audit service achieves the detection of cloud service provider server misbehaviors in a random sampling mode. The detection probability of disrupted data blocks is an important parameter to guarantee that

Table 1: Reconstruction of original file size in seconds

File type	Original file size (in bytes)	Modified file size (in bytes)	Proposed algorithm for recovery (in sec)
Text	2-DM1	0-36	230.4
Document	2-DM3	0-245	782.9
PDF	2-DM5	0-453	965.7
Image	2-DH1	0-54	345.6
Flash	2-DH3	0-367	1174.4
Audio	2-DH5	0-679	1448.5
Video	3-DM1	0-55	354.1

Table 2: Multimedia data corrupted server locations

File type	Corrupted server IP
Text	File name …/opt/tomcat/webapps/ELearnpart/upload/Final_Detailed_Links.txt Parity has been Removed address …..tomcat7.7.0.33.21627.env-2096869/10.10.125.98 Server address …..tomcat7.7.0.33.21627.env-2096869/10.10.125.98
PDF	File name …/opt/tomcat/webapps/ELearnPart/upload/PCD_ND07.pdf Parity has been Removed address …..tomcat7.7.0.33.21627.env-2096869/10.10.125.50 server address …..tomcat7.7.0.33.21627.env-2096869/10.10.125.50
Image	File name …/opt/tomcat/webapps/ELearnPart/upload/flowdiagram1.jpg Parity has been Removed address …..tomcat7.7.0.33.21627.env-2096869/10.10.125.98 server address …..tomcat7.7.0.33.21627.env-2096869/10.10.125.98

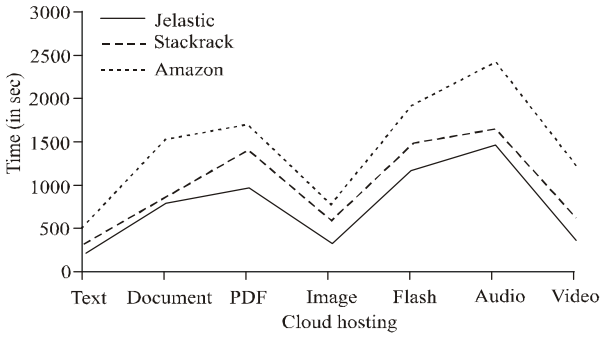

Fig. 2: Multimedia files recovery time

these blocks can be detected in a timely manner. The sampling-based audit has the potential to significantly reduce the workload on the servers and increase the audit service efficiency comparing to interactive proof system with the zero-knowledge property (Zhu *et al*., 2013). Also, the each corrupted file has to be audited periodically for corrupted file replacement and low bandwidth interruption of file downloads. This auditing mechanism is not feasible for the Hadoop distributed file system because it is much efficient for storing and accessing small files only (Dong *et al*., 2012). Jelastic service provider built its cloud IaaS powered by Jelastic on a scale-out, all solid-state disk storage system from solid fire, specifically designed to allow guaranteed service quality to a large number of applications at cloud scale. Instead of simply boosting average or maximum I/O performance like standard solid-state disk solutions, Solid fire produced an end-to-end storage architecture specifically for multitenant public cloud environments. This allows to produce guaranteed performance and enables I/O-sensitive e-learning application to realize extreme levels of performance. The e-learning cloud application is implemented and deployed in cloud service providers and the result is shown in Fig. 2. The result shows the multimedia files recover time (in seconds) is compared with different cloud hosting service providers are Jelastic, Stackrack and Amazon. On comparing these three cloud hosting service providers the computation cost for recovering multimedia files is much minimum for Jelastic cloud service. From result, we assume that each multimedia files of different block sizes. The layer interleaving encoding model guarantee that, assuming the client is honest, if and only if the server has access to the complete and uncorrupted data, it can pass the verification process successfully (Buttyan *et al*., 2011). Table 2 illustrate about the multimedia data corrupted file type and their server location. From analysis the proposed method clearly shows the locations of cloud server where corrupted multimedia data file type exist. Besides, The binary shuffle and belief propagation algorithms computation running time of $O(n)$. The binary shuffle algorithm uses the encoding of the data elements and parameterization to avoid any direct coupling to a random number generation algorithm. The belief propagation is a message passing algorithm used to draw inference on graphical models. The sum-product version of belief propagation computes the marginal distribution of each variable in the model and the max-product version computes the MAP-configuration. However, the island algorithm is dynamic to compute the modified block of any multimedia files and it achieves computation running time of $O(n \log n)$. Thus, the proposed e-learning cloud ensures a way to protect the data, check the data integrity and user authentication in cloud server.

Security analysis on challenge token authentication: The challenge response protocol computes the response by applying a cryptographic hash function to the server challenge combined with the user password and generates random challenge from the server to authenticate the $<User_i>$. The execution of challenge-response protocol, the method split the challenge key into many parts of partial keys and maintains those keys in a cloud server to guarantee security and data integrity. The user will obtain different unique challenge key while the cloud server is authenticated

for resource sharing. We can spot from the cloud users unique partial keys generated for the attributes are <$User_i$> = <generatedSaltKey, hashedPassword and securityChallengeToken>. This implies our challenge-response protocol method communication cost is more suitable and strong for distributed data storage (Gopinath and Geetha, 2013). The storage cost for identification of servers adds much effectiveness for data corrupted can be recovered back to the system. This layered interleaving error correcting code is normally a byte-error correcting code, like a Reed-Solomon code. The depth of interleaving determines the burst correcting power of the interleaved scheme.

CONCLUSION

An increasing number of cloud users to store their important data in cloud storage have become a trend. Sometimes the data stored in the cloud is so important that the users must ensure it is not lost or corrupted. The proposed methodology is used to check data integrity after completely downloading multimedia data and to ensure the cloud storage is secure. In this study, we propose a new remote data integrity checking protocol for cloud storage is suitable for providing integrity protection of cloud users important data and it ensures correctness of data error localization. Whenever a piece of data is modified, the corresponding blocks can be recovered by layer interleaving encoding technique. Thus, the proposed protocol supports reconstruction of modified file blocks are public verifiability. In the current construction, dynamic data operations can be supported by using block level and to ensure there is no attack to compromise the security of verification protocol. The performance evaluation results show that the proposed protocol has very good auditing efficiency in the aspects of communication, computation and storage costs.

REFERENCES

Basu, A., J. Vaidya, H. Kikuchi, T. Dimitrakos and S.K. Nair, 2012. Privacy preserving collaborative filtering for saas enabling paas clouds. J. Cloud Comput. Adv. Syst. Appl., pp: 1-14.

Buttyan, L., L. Czap and I. Vajda, 2011. Detection and recovery from pollution attacks in coding-based distributed storage schemes. IEEE T. Depend. Secure, 8(6): 824-838.

Chen, L., 2012. Using algebraic signatures to check data possession in cloud storage. Future Gener. Comp. Sy., 29(7): 1709-1715.

Dong, B., Q. Zheng, F. Tian, K.M. Chao, R. Ma and R. Anane, 2012. An optimized approach for storing and accessing small files on cloud storage. J. Netw. Comput. Appl., 35(6): 1847-1862.

Gopinath, R. and B.G. Geetha, 2013. An e-learning system based on secure data storage services in cloud computing. Int. J. Inform. Technol. Web Eng., 8(2): 1-17.

Guoli, Z. and L. Wanjun, 2010. The applied research of cloud computing platform architecture in the e-learning area. Proceeding of IEEE 2nd International Conference on Computer and Automation Engineering, 3: 356-359.

Ivanova, M. and G. Ivanov, 2010. Cloud computing for authoring process automation. Proc. So. Behav. Sci., 2(2): 3646-3651.

Koo, D., J. Hur and H. Yoon, 2013. Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage. Comput. Electron. Eng., 39(1): 34-46.

Lin, H.Y. and W.G. Tzeng, 2012. A secure erasure code-based cloud storage system with secure data forwarding. IEEE T. Parall. Distr., 23(6): 995-1003.

Peng, Y., W. Zhao, F. Xie, Z.H. Dai, Y. Gao and D.Q. Chen, 2012. Secure cloud storage based on cryptographic techniques. J. China Univ., Posts Telecommun., 19(2): 182-189.

Tsai, M.F., N. Chilamkurti, C.K. Shieh and A. Vinel, 2011. MAC-level forward error correction mechanism for minimum error recovery overhead and retransmission. Math. Comput. Model., 53(11-12): 2067-2077.

Wang, D., 2011. An efficient cloud storage model for heterogeneous cloud infrastructures. Proc. Eng., 23: 510-515.

Wang, Q., C. Wang, K. Ren, W. Lou and J. Li, 2011. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE T. Parall. Distr., 22(5): 847-859.

Wang, C., Q. Wang, K. Ren and W. Lou, 2012. Towards secure and dependable storage services in cloud computing. IEEE T. Serv. Comput., 5(2): 220-232.

Wang, C., S.S.M. Chow, Q. Wang, K. Ren and W. Lou, 2013. Privacy-preserving public auditing for secure cloud storage. IEEE T. Comput., 62(2): 362-375.

Yang, K. and X. Jia, 2012. Data storage auditing service in cloud computing: Challenges, methods and opportunities. World Wide Web, 15(4): 409-428.

Zhang, H., J. Zhou and J. Li, 2010. M2FEC: An effective FEC based multi-path transmission scheme for interactive multimedia communication. J. Vis. Commun. Image R., 21(2): 120-128.

Zhu, Y., G.J. Ahn, H. Hu, S.S. Yau, H.G. An and C.J. Hu, 2013. Dynamic audit services for outsourced storages in clouds. IEEE T. Serv. Comput., 6(2): 227-238.