Asian Journal of Information Technology 15 (8): 1275-1280, 2016
ISSN: 1682-3915

Facilitating Public Audits and Data Dynamicity with Security for Data Stored in Cloud Computing

[1]S.K. Mouleeswaran, [2]A. Grace Selvarani and [3]J. Kanya Devi
[1]RVS Technical Campus,
[2]Department of CSE (PG), Sri Ramakrishna Engineering College,
[3]Department of CSE, Sri Shakthi Institute of Engineering and Technology,
Coimbatore, Tamil Nadu,India

Abstract: The cloud computing is visualized as next generation framework for IT enterprise. The technology shifts the software and database to huge fixed central centers where the data management and services are not trustworthy. The technology gives rise to challenges in security which is of prime focus. The study focuses on ensuring security in storing data into cloud system. The third party auditor is allowed on behalf of cloud user for verifying the integrity of dynamicity of data stored into cloud. The third party auditor removes the participation of users through auditing of whether the data hoarded into cloud is certainly intact which is important in achieving the economy for cloud computing. The dynamicity in data is achieved via general forms of data like chunk alteration inclusion and removal which is a significant because the services in cloud systems are not limited for archiving the data. The conventional schemes on assuring data integrity do not support public audits or data dynamicity. The problems in identifying the complexity and security with updates in dynamic data from the earlier works and paved a way for designing a verification scheme for aggregating the above features. In order to achieve data dynamics and for supporting multiple auditing tasks a technique for combining signature are proposed which performs the task of auditing continuously. The security and performance analysis of the proposed scheme are effective and secure.

Key words: Cloud computing, dynamic data, signature, security and verification, India

INTRODUCTION

Several developments are happening in cloud computing every now and then along with the developments in internet and the utilization of computing resources. The cost reduction with SaaS framework is converting the data centers into a collection of computing resources on a large scale. Moreover, with rising network bandwidth and dependable supple network connections the users are capable of utilizing best services for data and software which exists exclusively on global data centers.

This technology even though visualized as a capable platform for the internet the fresh data storage concept in cloud computing may introduce problems in designing the system and also with security of data hoarded also the performance of the system. The great problem happens in cloud based data storage is ensuring integrity of the data hoarded at the un-trusted servers. In case the service provider may experience byzantine failures rarely which may be hidden from the user's perception for their own benefit. The service provider might delete the rarely accessed data of a normal client for saving money and space. For instance a huge sized outsourced data with limited restrictions can be accessed regularly by the user without degrading the data integrity and not holding a local copy of the data.

The solution to the problem of data integrity different techniques have been designed under various systems and security feature involving great efforts for satisfying different level of requirements like improved efficiency, integrity verification, user feedbacks and data accessibility. The verification plays a major role in the event and it provides two different facilities as private audits and public audits. The techniques in private audits attain greater efficiency but the public audits allow all sorts of people to confront the cloud server for data correctness even in the absence of private information. The users are capable to evaluate their level of performance to a unique Third Party Auditor (TPA) without considering their computing resources. It is to be noted that the users of cloud themselves are incapable in overcoming the overheads in performing regular integrity verification. It is very normal to provide a protocol for

Corresponding Author: S.K. Mouleeswaran, RVS Technical Campus, Coimbatore, Tamil Nadu, India

verification in public audits which plays a promising role in reducing the costs for cloud computing. The verification process does not make of the outsourced data to perform verification.

The biggest problem faced by the cloud computing from conventional designs is supporting dynamic data operations over cloud data storage. The globally stored data might not be accessed by the users frequently but, it will be appended by the users through the process of adding, removing or alteration. The conventional approaches focused only on the fixed data files and so the dynamic data operations are not considered as of now. The data extraction techniques supporting data movement may introduce security problems and these serve as prime importance while outsourcing of stored data. By focusing upon, the public audits and data movement in cloud storage an effective designing for combining these two components are proposed during designing a protocol. It is listed as below:

- The proposed protocol supports data movements especially during insertion which is not considered in the conventional schemes
- The scheme provides extended approach where bunch audits where different auditing tasks from different users can be performed at the same time by the TPA
- The security is enforced in the proposed scheme through implementations and based on performance comparisons

Related works: The study is performed by analyzing the drawbacks gathered from different scholars research. The drawbacks are clearly analyzed and combined solutions are proposed for attaining improvement within the system.

Anjali and Sivachandiran (2015) described cloud computing as a suitable, resourceful and on demand availability to distributed collection of computing resources that are capable of easy setup and release using minimal efforts. The major focus of the authors is to throw light on the security issues in present cloud computing environment. This technology serves as a centralized database into which many users hoard their information, release those information and information modification. The users get their services done from the service providers on payment basis based on their requirements. The data retrieval and storage are not fully secure for which a trusted third party (TPA) is employed for making the client to ensure the integrity of their hoarded information. It is needed that the client can add, remove or append their information for which security must be ensured. The third party can use the data along with modification with security features.

Sukhvinder *et al.* (2015) described cloud computing as next generation IT infrastructure because it shifts the application software and databases to a huge central data centers for managing the data with a breach in security. This leads to many security issues within cloud computing. The major focus of the authors is to address the problems in data integrity in cloud computing. The usage of Third Party Auditing (TPA) retards the need for every client to verify the integrity of their data stored. This greatly reduces the burden on the server to authorize users and avoids the denial attacks. The DDOS is a kind of denial attack in a different vulnerable systems usually infected with Trojan viruses. The DDOS attacks systems of the user which is vulnerable and the system under the control of hackers. The solution was planned by combining RBAC and MAC algorithms. The TPA the roles can be created easily, altered without the need for updating the privileges of every individual user.

Mishra and Sharma (2014) focused on the influence of cloud computing in present scenario. The technology finds its application in business, education and social environments. The growth of technology was due to its on demand and pay on basis service. The utilization of this technology introduces threats to the hoarded data due to its sharing with other users of the cloud and its usage also differs. It is very important to focus on the security in cloud computing. The clients are dependent on the cloud providers which fosters data security and control over the stored data. The major focus of the authors was to provide improvement in cloud security by bridging the gaps in the conventional methods.

Shymali *et al.* (2015) described cloud computing as future computing framework providing services by combining the computing resources that are accessible via internet. The conventional methods allowed the data users to store their data into data centers with security features for providing data security against hackers. The users have only limited control over the stored data due to its global accessibility. The service providers of cloud are responsible for providing security of the data from the unprivileged users. A Third Party Auditor (TPA) assures security services over cloud and guarantee that the cloud data are free from unauthorized usages. The TPA is not meant for storing data but, it is to provide security between the cloud users and the service providers. The technique also provides integrity checks while transferring data from one to another cloud using hashing algorithms along with encryption and decryption techniques. The authors proposed a mechanism for

securing the data movement by employing a Third Party Auditor (TPA) using Secure Socket Layer (SSL) for maximizing the trust and security for the cloud users and service providers.

Santosh and Nandwalkar (2015) focused on the importance of privacy preservation between the third party auditor and the cloud data. The conventional encryption techniques were based on RSA which possessed various setbacks which was planned to overcome using advanced encryption algorithm (AES). The presently used encryption algorithms are based on AES which is composed of several substitutions, permutations and linear transformations. The AES algorithm is very difficult to break for which it serves as a powerful algorithm and preferred by many government agencies and banks around the globe. The authors employed a batch auditing protocol for improving the performance of TPA. It is to be noted that the stored data of the users are updated every time which must also be taken into considerations before planning a promising technique.

Kishor *et al*. (2015) addressed cloud computing as future generation technology for global access to the stored data. The technology allows buying storage spaces for implementing application software, etc. It is necessary to focus on the security issues in cloud computing. The authors focus was to provide security to the cloud data by maintaining privacy between the Third Party Auditor (TPA) and service providers.

Rasal and Kahate (2015) discussed about the storage and sharing facilities in cloud for the benefit of users in sharing information between them. The cloud computing provides an environment where along with data storage it is possible to use application software and other services offered by the service providers. The cloud users hoard their data into cloud servers without holding a copy for themselves. The users of cloud hoard their data into private cloud and they migrate to public cloud for attaining storage expansions but the security aspects in public cloud must be focused. The public cloud may allow unauthorized user to gain access to the hoarded data. It is necessary that the users have to verify the integrity of their stored data on the un-trusted global servers. The public clouds may offer several security features but they may be incomplete. These problems can be addressed using Third Party Auditors (TPA) with different services for ensuring data integrity. The services may be like access, modify, append for verifying the integrity to the hoarded data in public clouds. The authors proposed an auditing model based on hash tree for availing security benefits over public, private or hybrid clouds.

Badhe and Ramtteke (2015) described cloud computing as the latest technology with different services for the benefit of users via internet. The servers of cloud allow the data users to hoard their data without focusing on data integrity and correctness. The users of cloud can gain to the stored information anywhere, anytime without involving complex facilities. The cloud providers provide maintenance and storage based on the user's demand. The problem can arise with the security in global data for their integrity and correctness. The authors proposed a secure cloud storage system with privacy preservation where the Third Party Auditor (TPA) audits different users continuously and effectively.

MATERIALS AND METHODS

Problems addressed: The framework for data storage in cloud is shown in Fig. 1 containing different units as explained.

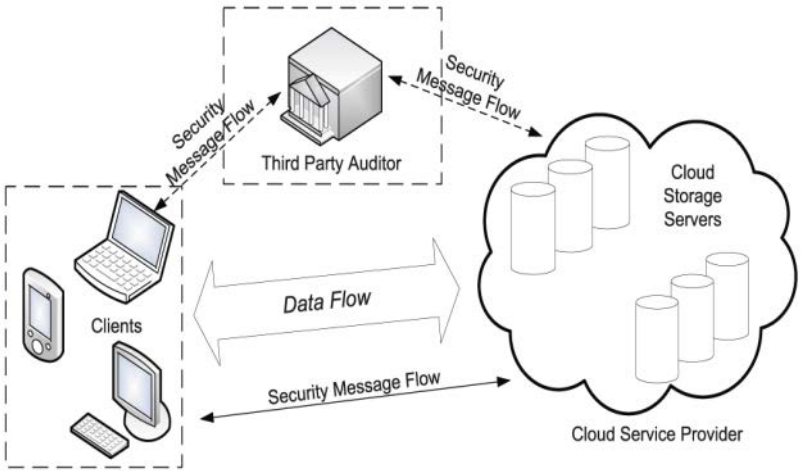

Fig. 1: Cloud data storage

User: The users hold huge data files for storing them into the cloud and they depend upon cloud for maintaining their data and its operation. The users may be single or it may be an organization.

Storage Server: The servers are maintained by the service providers containing space for storage and resources to perform computation and they maintain the user data.

Third party auditor: The auditors are capable and hold abilities that the user does not possess. The TPA can be trusted and it identifies the risks involved in storage services on behalf of the client based on the request by the user.

The cloud storage holds huge data files into global servers by freeing the users from the problem of storing the data and its computation. The users do not hold their data with them and it is important that the users must be ensured that their data is being stored correctly and it is maintained properly. The users must be aware about the security terms for verifying the correctness of their data periodically even without the local copy of their stored data. In case, if the client does not have enough time or adequate resources for monitoring their data they assign the task to a trusted Third Party Auditor (TPA). The prime focus of the paper is to perform verification in public audits, i.e., the TPA with public key can act as a observer for an un-trusted server. The client requests the cloud servers through the service providers for retrieving their already hoarded data. The users continuously perform bundle of operations onto the stored data files and more likely the operations like data alteration, adding and removal are given the prime importance. The data integrity is dealt here but, the privacy of these data still remains an unsolved problem which is planned for addressing in this paper.

The security of the verification technique is safe if there no polynomial time algorithm which might cheat the observer using a non-avoidable probability and also there exists an extractor for this polynomial which extracts the original data by multiple attempts. The third party auditor occasionally confronts the storage servers for assuring the correctness of the data stored over cloud. The stored original data can be extracted by communicating with the server. The focus is upon ensuring correctness of the data stored and the scheme proves right if the algorithm used for verification works correctly while communicating to the observer. It resembles cheating if it compromises the user hoarding their data into the server.

The above security measures are not suitable for data movement and adding bunch of data is not allowed due to the involvement of cryptographic signature generation within the file directory. It creates complex file procedures and involves complex computational procedures. This might differ from conventional data verification and appending schemes which must resemble authenticated on every data update.

Goal of the proposed plan:

- Ensuring correctness of the stored data by anyone not only the users who hoard their data into cloud servers can assure correctness in the stored data for their needs
- Supporting data movement and assuring integrity to the stored data
- The users should not gain access to the restricted data during verification process in order to enhance the efficiency of the system

Proposed plan: Security schemes are proposed for storing data into cloud by considering the above mentioned problems. The ultimate goal is to achieve data integrity to the cloud data for which the proposed security scheme supports public audits and data movement. The technique also allows TPA to perform audits in bundles based on the allocation by multiple users.

The outsourced data is collection of ordered groups where the data integrity can be straightly ensured by pre-computing the MAC of the entire data. This is performed with the fact that the owner of the data computes the MAC for the data with a set of secret keys before performing outsourcing and stores them locally. For performing audits the data owner gives its secret key each and every time to the cloud server and obtains a new MAC along with the key for performing verification. This scheme determines the integrity of stored data in a straight forward technique since the verification is performed for all the data into the cloud. The verification process is restricted based on the secret keys and once if the secret key gets exhausted the owner of the data has to obtain the entire data file from the server for computing a fresh MAC which tends to create overheads in communication. The scheme is suitable for public audits because private keys are required for the verification process.

The scheme can be extended for supporting public audits without obtaining entire data file from the server using non-varied authentication technique. This authenticator technique generates genuine metadata from every unique data chunk which can be combined safely in a way that the observer verifies its correctness. The scheme supports data movement which is a major problem to be focused in cloud storage systems.

The user or the TPA verify the integrity of outsourced data by confronting the server before which it makes use of the secret key for verifying the signature. In case, if the verification fails the entire data chunk must be obtained from the cloud storage. Here, the data chunks and the signature are combined into a bundle along with some needed information. Based on the responses received the observer performs verification with the data stored into cloud.

The scheme can handle dynamic operations with the data like data alteration, data inclusion and data removal within the cloud storage. It is to be noted that the data file and the signature are already been created and stored properly in the server. The metadata are been signed by the user and it is hoarded into the cloud server with which any user of cloud storage with the public key can confront the data correctness within the server.

The data alteration is more frequently used operations in data stored into the cloud storage. The data alteration refers substitution of particular chunks with a fresh one. For altering a chunk of data the user generates equivalent signatures and builds a request for update and sends it to the server for performing data alteration. Here, the particular data chunk will be replaced at the server and outputs the results. The data alteration does not change the internal logical structure of the user's data but the data inclusion allows insertion of fresh chunks after particular positions into the data bundles. For inserting a data chunk after a position 'p' the similar of data alteration is employed. The user generates a signature and builds an update request and sends that to the server for performing insertion operation. After receiving the request the server runs and adds the chunk into the desired positions thus producing an updated data block. The data removal is opposite of data inclusion operation. Removal of single data chunk refers removing a particular chunk and shifting all the later chunks one step forward. After receiving an update message for data removal that particular chunk will be removed and the space will freed for accepting new chunks. This operation is same as data alteration and data inclusion.

RESULTS AND DISCUSSION

Performance analysis: The proposed scheme aims to support dynamicity among the data without compromising the security features. The system were implemented with an Intel Core 2 Processor executing at 2.4GHz, 800 MB Ram and 7000 RPM Digital 275 GB serial ATA drive with 16 MB buffer. The authentication algorithm was implemented for attaining 80 bit security parameter which resulted at the averages of 9 trials. This experimental study measures the added cost initiated for supporting dynamicity with the data in the proposed scheme for server based computation, observer computation and the overhead also. The performance of the overall schemes are compared and verified with each other. The smaller chunk size compared to the authentication algorithm performs faster than the conventional techniques in terms of server computation time. The communication overhead time of the authentication scheme for different data chunks are illustrated in Fig. 2. The communication cost increases quickly along with the increase in chunk size which is results with the increase in size of the observer chunk. The performance analysis for block size of 14 KB achieves reduced cost in communication.

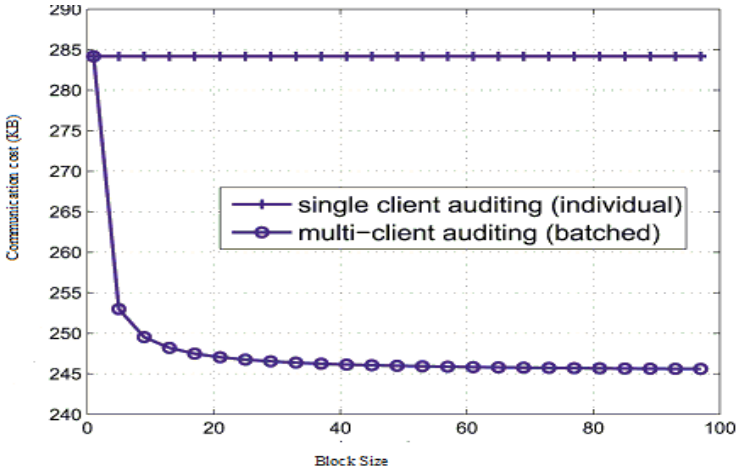

Fig. 2: Performance analysis for communication cost

CONCLUSION

For assuring security for data stored in cloud system it is important to use a third party auditor for measuring the quality of service. The public audits allow the users to assign data integrity by TPA employing verification tasks but this scheme is not quite reliable. The major focus is upon designing protocols for verification which holds the dynamicity of data. The paper addressed the problem in providing continuous integrity for data in cloud computing for which the conventional schemes are improved for assuring authentication. The multiple auditing tasks are investigated using signature based techniques allowing the TPA to perform different auditing tasks continuously. The performance analysis of the proposed scheme proves to be highly effective and secure.

REFERENCES

Anjali, R. and S. Sivachandiran, 2015. A data security for cloud computing using third party auditor. Int. J. Sci. Res. Dev., 3: 1351-1355.

Badhe, M.V. and P.L. Ramteke, 2015. A survey on privacy-preserving public aditing for scure coud sorage uing third party auditor. Int. J. Comput. Sci. Mob. Comput., 4: 168-174.

Kishor, K., M. Hegade and M. Patil, 2015. Providing security and privacy to cloud data storage using TPA. Int. J. Multidiscip. Res. Dev., 2: 667-670.

Mishra, L. and A.K. Sharma, 2014. Secure cloud computing with third party auditing: A survey. Int. J. Comput. Appl., 103: 19-24.

Rasal, K.J. and S.A. Kahate, 2015. Third party auditing for cloud storage. Int. J. Eng. Res. Sci. Technol., 4: 246-251.

Santosh P.J. and B.R. Nandwalkar, 2015. Efficient cloud computing with secure data storage using des. Int. J. Adv. Res. Comput. Communi. Eng., 4: 377-381.

Shyamli, D., D. Kumar and S. Gonnade, 2015. Secure data migration across cloud system using third party auditor. Int. J. Innovative Res. Sci. Eng. Technol., 4: 4053-4059.

Sukhvinder K., M.K. Kashyap and K.J. Jagdeep, 2015. Implementation of effective third party auditing for data security in cloud. Int. J. Adv. Res. Comput. Sci. Software Eng., 5: 214-218.