Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 10, October-2016

A Survival Study on Integrity based Hashing Techniques for Secured Cloud Data Storage

M. Buvaneswari
Research Scholar
Bharathiar University
Coimbatore,Tamilnadu,India

Dr. N. Rajendran
Principal
Vivekanandha Arts and Science College for Women
Sankari,Tamilnadu,India

***Abstract*— Cloud computing is made up of many elements, namely cloud users, cloud service providers and third parity auditors. Each element has particular part in delivering functional cloud-based applications. Cloud computing security approach provides better protection in terms of filtering, risk management and deployment of standard information security policies. Integrity constraints are declared in the records to express the semantic properties that are invariably satisfied by the stored data across state changes. The high integrity processes of system are established from access by low integrity processes during runtime to present the security. Though, all risks are not reduced by moving operations to a cloud environment. In this work, integrity based hashing techniques is used for secured cloud data storage. Our research work helps to eliminate the third party auditing.**

Keywords*— *Third Parity Auditor, Integrity based hashing techniques, Cloud environment and Integrity constraints

I. INTRODUCTION

Cloud computing is computing technique used for sharing the computing resources than the local servers or personal devices for the applications. Cloud computing is type of grid computing where unused processing cycles of all computers in a network are controlled to address the issues for any stand-alone machine. Cloud computing and storage solutions present the users and endeavors with many abilities to store and process the data in third-party data centers. Cloud computing is to allocate the users from all technologies lacking the need for deep knowledge. Cloud computing is a method for allowing the suitable, on-demand network access to collective group of configurable computing resources provisioned and discharged with less administration effort or service provider communication.

Cloud computing is an internet-based growth and utilization of computer technology. Cloud computing denotes the utilization of the computing resources in both hardware and software on demand as service over Internet. It also presents a collection of services for users of network with applications, storage, many processes and remote printing. It has the Internet provision of scalable and virtualized resources. Businesses are running all apps types in cloud. Cloud computing are taken as the technology which maintains the data in many applications. It is remotely controlled lacking the requirement to download applications on computers.

This paper is organized as follows: Section II discusses Integrity based Hashing Techniques for Secured Cloud Data Storage, Section III shows the study and analysis of the existing integrity based hashing techniques on cloud computing, Section IV identifies the possible comparison between them and Section V concludes the paper, key areas of research is given as integrity based hashing techniques for secured cloud data storage.

II. LITERATURE REVIEW

Provable Data Possession (PDP) technique in [5] is to guarantee the data storage outsourcing. The design of PDP scheme for distributed cloud storage that maintains the scalability of service and data migration. A Cooperative PDP (CPDP) scheme is designed depending on the homomorphic verifiable response and hash index hierarchy to maintain the dynamic scalability on multiple storage servers. However, CPDP scheme for large files is affected through the bilinear mapping operations because of its high complexity. A public auditing protocol [2] was planned from the short signature scheme and the homomorphic hash function. Cloud service providers calculated the aggregation of the blocks and the aggregation of signatures. Network security cloud storage service is presented to users through considering public auditing system to authenticate data integrity. Though, the public auditing model for cloud storage and the model against the pollution attacks for linear network coding are not considered.

The data integrity checking algorithm was introduced in [1] to eliminate the third party auditing. A cloud computing security development lifecycle model achieve safety and enable the user to provide security and face the risks that may be exposed to data. The data integrity checking and estimation is controlled in efficient way by set of hash functions. However, all risks are not reduced by moving operations to a cloud environment. The model failed to present the suitable balance between protection and usability is discarded in cloud system. Inconsistency-Tolerant Integrity Checking (ITIC) method was designed in [4] to allow the updates to be fruitfully checked for integrity preservation even in the presence of inconsistency. The purpose of integrity checking ensures the satisfaction of each constraint preserved across updates. However, analysis of interplay between the ideas of inconsistency-tolerant repair is not included. It is not sufficient to be content with partial repairs that tolerate inconsistencies with the query.

The public auditing system of data storage security in cloud computing maintains fully dynamic data operations to maintain block insertion through designing the Third Party Auditor (TPA) in [3]. TPA of the cloud client verifies the integrity of dynamic data stored in the cloud. TPA also recognizes the complexities and potential security problems as well as creates the elegant verification scheme for seamless integration. However, the technique of bilinear aggregate signature is not expanded to a multiuser setting. TPA scheme cannot perform in multiple auditing tasks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 10, October-2016

III. INTEGRITY BASED HASHING TECHNIQUES FOR SECURED CLOUD DATA STORAGE

Cloud computing need the security keys on many features of large integrated system. The application software and databases in cloud computing are shifted to the centralized large data centers where the organization of the data and services are not responsible. Cloud computing has many elements like cloud users, cloud service providers and third parity auditors. Each element has many parts in distributing functional cloud-based applications. Cloud storage service is of low-cost, scalable, position-independent platform for client's data. The high integrity processes of system are calculated and verified from accesses started through low integrity processes in runtime to present the security.

A. Public Data Integrity Verification for Secure Cloud Storage

Cloud storage presents a flexible on-demand data storage service for users in anyplace at anytime. In system model of public auditing, there are three entities, namely user, Cloud service providers (CSP) and third party auditor (TPA). User is an entity with the large data files that stored in the cloud and depends on the cloud for data maintenance and computation for individual consumers or for organizations. Cloud service providers (CSP) are the manager of cloud servers. It has an essential storage space and computation resource to preserve and calculate the user's data. Third party auditor (TPA) has capability that users are not trusted to evaluate and to depict the risk of cloud storage service for the users leading request.

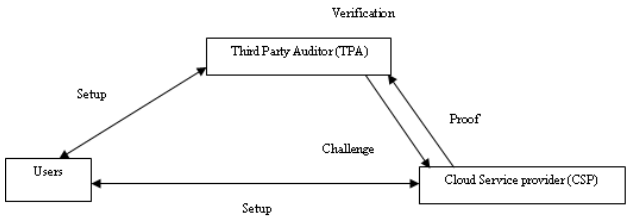

Fig. 1 System Model of Public Auditing

In cloud model, with the large data files on remote servers, users reduced the burden of storage and computation. Initially, the users calculate the signature of data then it sends the data and signature to CSP. In cloud storage system, users accumulate the data into group of cloud servers by CSP execute in cooperated and allocated way. Subsequently, users fail to have the data locally. If users verify whether the data exists certainly in cloud servers, auditing work starts. After receiving the auditing request from users, TPA generates and sends a challenge to CSP. On receiving the challenge from TPA, CSP creates a proof of data storage and sends it to TPA. In verification, TPA verifies the accuracy of the proof from CSP and revisits TRUE/FALSE.

In cloud storage system, TPA is considered to be honest and curious. It executes truthfully in whole auditing method, however it is curious concerning the received data. CSP is considered to be dishonest. Some attacks against this system exist. In the public auditing system, with the curiosity attack, loss attack and tamper attack from the adversary, the verification model consists of four algorithms. The user can run this key generation algorithm to generate the secret parameters and public parameters. Using the data and the secret parameters, the user can run this signature generation algorithm to generate the signature of the data. Using the data and signatures stored in cloud servers, and the challenge from TPA, CSP can run this proof generation algorithm to generate the proof. On receiving the proof from CSP, with public parameters, TPA executes the proof verification algorithm to check whether the data exists indeed in the cloud servers. With the system model, attack model and the verification model, the objectives of public auditing protocol are described. Public verifiability permits anyone not the users who stored the file on cloud server's capability to authenticate the integrity of stored data on demand. Data dynamics is to permit the users to execute block level operations on data files while maintaining the same level of data integrity verification. Privacy preserving without the blocks are retrieved by the verifier TPA during verification process.

B. Data Possession for Integrity Verification in Multi-Cloud Storage

A verification framework is planned for multi-cloud storage along with two fundamental techniques called hash index hierarchy (HIH) and homomorphic verifiable response (HVR). The cooperative PDP (CPDP) scheme is designed without the data privacy from cryptographic methods like interactive proof system (IPS). CPDP scheme is designed by above-mentioned structure. A multi-prover zero-knowledge proof system (MP-ZKPS) is planned with unity, knowledge soundness and zero-knowledge properties. The property guarantees CPDP scheme designs the security against data leakage attack and tag forgery attack. The performances are examined of probabilistic queries for categorizing the abnormal locations. The probabilistic method has inherent advantages in minimizing the computation and communication overheads. An effective technique is designed for the choice of optimal parameter values to reduce the computation overheads of CSPs and the client's operations.

C. Data Integrity In Cloud Computing Security

A cloud computing is made up of many parts: Cloud users, cloud service providers, third parity auditors. Each part plays a significant role in distributing functional cloud-based application. Cloud users are an individual or an organization storing their data in cloud and accessing the data. CSP manages the cloud servers (CSs) and presents a storage space on its infrastructure to users. Servers are in many locations. The servers on cloud computing is from the principle of virtual servers because the user failed to identify where server has the necessary service. A collection of servers form the data center, where the application is housed. Cloud data centers are identified as cloud data storages (CDSs). The software is installed on physical server and allocating the multiple instances of virtual servers. Cloud Computing is executed on many deployment models.

The deployment model is chosen based on the user needs and market accessibility. Private Cloud is used through one organization. The cloud is executed through the organization itself or third party. If private cloud is realized and managed, it has minimized potential security concerns. Public Cloud is utilized through the public and includes an organization by cloud infrastructure shared through the Internet with additional organizations of the public like Microsoft, Google

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 10, October-2016

and Amazon. Public cloud has many inherent security risks that required to be taken. Community Cloud is shared through many organizations and setup for similar security needs. It also requires to store or process data of similar sensitivity like many agencies of similar government. Hybrid Cloud is a mixture of cloud deployment models. Each cloud is controlled while applications and data are allowed to move with hybrid cloud. A private cloud is a public cloud while it needs many resources. A particular business and technology needs are used in planning hybrids to enhance the security and privacy with minimum IT costs.

IV. COMPARISON OF INTEGRITY BASED HASHING TECHNIQUES FOR SECURED CLOUD DATA STORAGE & SUGGESTIONS

In order to compare the integrity based hashing techniques, no. of cloud users is taken to perform the experiment. Various parameters are used for integrity based hashing techniques for secured cloud data storage.

A. Cloud Data Security Level

Cloud data security level is defined as the secured rate at which the cloud data is sent to the destination without any third party auditors. It is measured in terms of percentage (%).

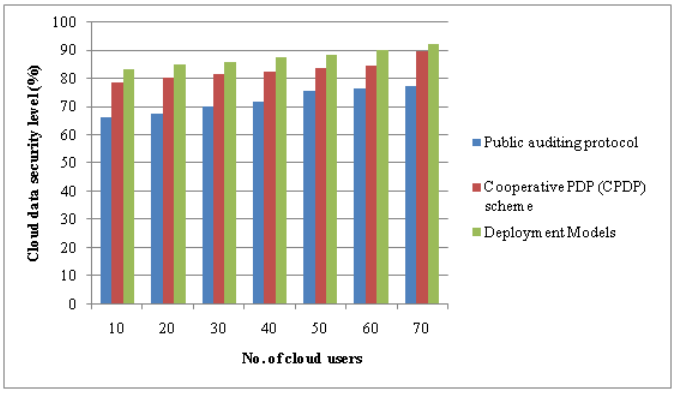

Fig. 4.1 Cloud Data Security Level of Integrity Based Hashing Techniques

Fig. 4.1 reveals the comparison between the three methods namely, public auditing protocol, Cooperative PDP (CPDP) scheme and Deployment Models. From the figure, the Deployment Models provides better performance in terms of cloud data storage security level as compared to other methods. When the number of cloud user gets increased, the cloud data security also gets increased correspondingly. The percentage of Deployment Models improves the cloud data security level by 17% compared to public auditing protocol. In addition, the cloud data storage security level is increased by 5% compared to Cooperative PDP (CPDP) scheme.

B. Verification Time

The verification time is defined as the difference between the starting and ending time of verification. It is measured in terms of milliseconds (ms).

Verification time = starting time – ending tie of verification

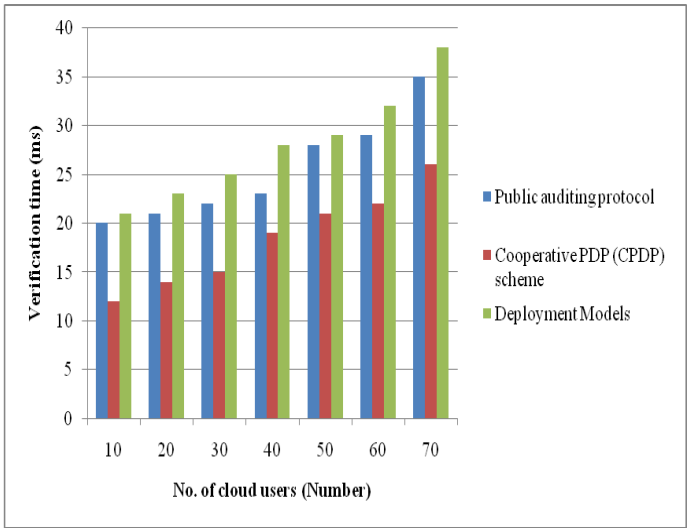

Fig. 4.2 Verification Time of Integrity Based Hashing Techniques

The fig. 4.2 compares the verification time measurement based on the number of cloud users. The Cooperative PDP (CPDP) scheme takes less amount of verification time compared to other public auditing protocol and Deployment Models. The verification time and the number of cloud users are directly proportional to each other. Cooperative PDP (CPDP) scheme consumes 40.59% lesser verification time compared to public auditing protocol and 54.71% lesser verification time when compared to the Deployment Models.

C. Storage Size

The storage size is defined as the amount of memory space required for sending the cloud data without showing to the third party auditors. It is measured in terms of megabytes (MB).

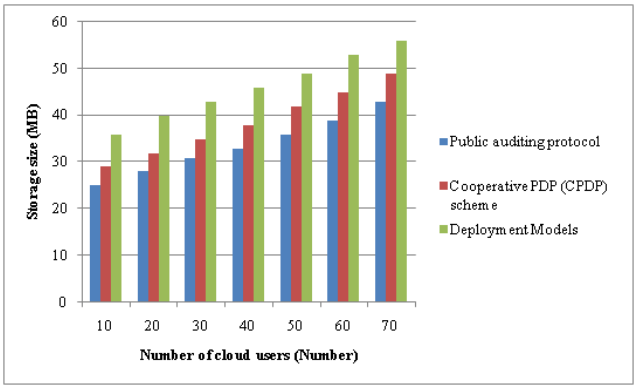

Fig. 4.3 Storage Size of Integrity Based Hashing Techniques

In fig. 4.3, the storage size comparison of public auditing protocol, Cooperative PDP (CPDP) scheme and Deployment Models are explained. The public auditing protocol consumes lesser amount of space when compared to Cooperative PDP (CPDP) scheme and Deployment Models. Public auditing protocol consumes 14.90 % lesser storage size when compared to Cooperative PDP (CPDP) scheme and 38.17% lesser storage size when compared to Deployment Models.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 10, October-2016

V. DISCUSSION ON LIMITATION OF INTEGRITY BASED HASHING TECHNIQUES FOR SECURED CLOUD DATA STORAGE

A cloud computing security development lifecycle model attains the safety and allow the user to present the security and address the problems that exposed to data. The data integrity checking algorithm removes all the third party auditing. However, all risks are not minimized through moving operations to a cloud environment. In addition, they failed to present the suitable balance between protection and usability that are discarded in cloud system. The public auditing protocol is designed based on the BLS short signature scheme and the homomorphic hash function. Cloud service providers are evaluated the aggregation of blocks and the aggregation of signatures. Network security cloud storage service is presented to users through taking the public auditing system to authenticate the data integrity. However, the public auditing model for cloud storage and the model against the pollution attacks for linear network coding are failed to taken.

The Provable Data Possession (PDP) technique guarantees the integrity of data in storage outsourcing. The design of PDP scheme for distributed cloud storages maintains the scalability of service and data migration. A Cooperative PDP (CPDP) scheme is designed depending on the homomorphic verifiable response and hash index hierarchy. However, CPDP scheme for large files is not secured through the bilinear mapping operations because of its high complexity.

A. Related works

Dynamic Integrity Checker (DIC) module [7] was designed to observe the dynamic execution traces of the program. The integrity checker module is combined with superscalar pipeline using a cycle-accurate simulator. Therefore, checking for integrity at the instruction level is not feasible choice. However, verification mechanism is complex and does not scale well with performance when it is designed on superscalar processors. A dynamic remote attestation framework [6] was developed to measure a target system based on an information flow-based integrity model. The high integrity processes of a system is determined and established from accesses started through low integrity processes. However, dynamic risk evaluation does not explain the tolerable risk level and relevant system property.

B. Future Work

The future direction of the integrity based hashing techniques is to eliminate the third party auditing for secured cloud data storage.

VI. CONCLUSION

A comparison of different techniques for secured cloud data storage is carried out. In the present environment, there are many risks that are not reduced by moving operations to a cloud environment. From the survey, they failed to present the suitable balance between protection and usability that are discarded in cloud system. The public auditing model for cloud storage and the model against the pollution attacks for linear network coding are failed to taken. CPDP scheme for large files is not secured through the bilinear mapping operations because of its high complexity. The wide range of experiments on existing techniques calculates the comparative results of the various secured cloud data storage techniques and its limitations. Finally from the result, the research work can be carried out with integrity based hashing techniques to eliminate the third party auditing for secured cloud data storage.

REFERENCES

[1] Dr. Nedhal A. Al-Saiyd and Nada Sail, “Data Integrity in Cloud Computing Security” Journal of Theoretical and Applied Information Technology, 31st December 2013, Volume: 58, Issue: 3, Pages 1-12.

[2] Hongwei Liu, Peng Zhang and Jun Liu, “Public Data Integrity Verification for Secure Cloud Storage”, Journal of Networks, Volume: 8, Issue: 2, February: 2013, Pages: 373-380.

[3] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou and Jin Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing”, IEEE Transactions on Parallel and Distributed Systems, Volume: 22, Issue: 5, May 2011, Pages: 847-859.

[4] Hendrik Decker and Davide Martinenghi, “Inconsistency-Tolerant Integrity Checking”, IEEE Transactions on Knowledge and Data Engineering, Volume: 23, Issue: 2, February 2011, Pages: 218-234.

[5] Yan Zhu, Hongxin Hu, Gail-Joon Ahn and Mengyang Yu, “Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems, Volume: 23, Issue: 12, February 2012, Pages: 2231 – 2244.

[6] Wenjuan Xu, Xinwen Zhang, Hongxin Hu, Gail-Joon Ahn and Jean-Pierre Seifert, “Remote Attestation with Domain-Based Integrity Model and Policy Analysis”, IEEE Transactions on Dependable And Secure Computing, Volume: 9, Issue. 3, May/June 2012, Pages 429-442.

[7] Arun K. Kanuparthi, Mohamed Zahran and Ramesh Karri, “Architecture Support for Dynamic Integrity Checking”, IEEE Transactions on Information Forensics and Security, Volume: 7, Issue: 1, February: 2012, Pages: 321-332.