International Journal of Latest Trends in Engineering and Technology
Vol.(10)Issue(1), pp.146-149
DOI: http://dx.doi.org/10.21172/1.101.24
e-ISSN:2278-621X

DESIGN AND IMPLEMENTATION OF SECURITY FOR MOBILE CLOUD STORAGE AS A SERVICE USING MAPREDUCE SYSTEMS

B.Venkata Naga Sai[1], Dr.M. Varaprasad Rao[2], Dr.K. Srujan Raju[3], Dr.K.Srinivas[4]

Abstract- The development of computation, storage, scale and networking technology have made processing tremendous data become real. As a result, the demand of discovering knowledge from the big data by using tools such as statistical analysis and data mining become higher. Using MapReduce a software framework introduced by Google in 2004 to implement computations on clusters of commodity computers is an economical solution. However, malicious MapReduce framework or source codes can leak the sensitive data through computation process. Giving user the least privilege on MapReduce-based system can solve the problem. Therefore, in our research, we propose a Mobile Cloud Storage using MapReduce-based computational system limiting the access to system resource by using access control mechanisms. Moreover, noise were added to the output of the Reduce to ensure the computational result can not signal the presence of a sensitive data. The cloud storage technology, for the problems of confidentiality and privacy in cloud storage framework, design the security cloud storage framework, solves the confidentiality of documents, and ensure the customer's privacy. Our prototype implementation demonstrates the efficiency of preserving privacy on several cases.

Keywords – Cloud Computing, Privacy, Integrity, Authorization, Security, Randomization, Code Analysis, Mobile Cloud Storage

1. INTRODUCTION

Cloud Computing solutions makes ease of use methodologies to store and retrieve data at cloud data centers than in a PC or an organization's server [1]. MapReduce (MR) is a service of an open source proposed by Google. The MR is used in many research areas or domains like machine learning, sentimental analysis, and scientific applications. Computation with MR has its own privacy disadvantages like malicious application of MR may exploit confidential and sensitivity data. Many researchers have proposed various methods in data mining, anonymization is one of the algorithms which is used to remove identifiable information, and also does not provide confidentiality [2][3].

Preserving privacy and security in Cloud is a big challenge with adhoc devices like mobiles, laptops and others. The cloud storage is accessed through Internetwork; therefore the concerns of this is confidentiality, unauthorized access of data even if accessed data, still it should be safe. Internet itself is very complex to understand and ISP is not also not safe. To provide safeguard of the data, one of the encryption algorithms used and this makes the users to ensure the confidentiality.

2. LITERATURE SURVEY

Indrajit Roy and others [7], introduced Security and Privacy for MapReduce formulated as Airavat, provides security and privacy for distributed networks on confidential data, where data comes from various sources. Study of secured cloud storage architecture proposed by Lin Qinying and others [4]. Query efficiency to retrieve data very quickly, proposed by Mu Fei, et al [5]. Hong Cheng et al, [6]; presents a dynamic method called attribute encryption algorithms for ciphers to reduce the complexity of Cloud server for fast response system.

3. PROPOSED SYSTEM

3.1 Design of Mobile Cloud Storage Framework

[1] Scholar, B.Tech Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India
[2] Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India
[3] Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India
[4] Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India

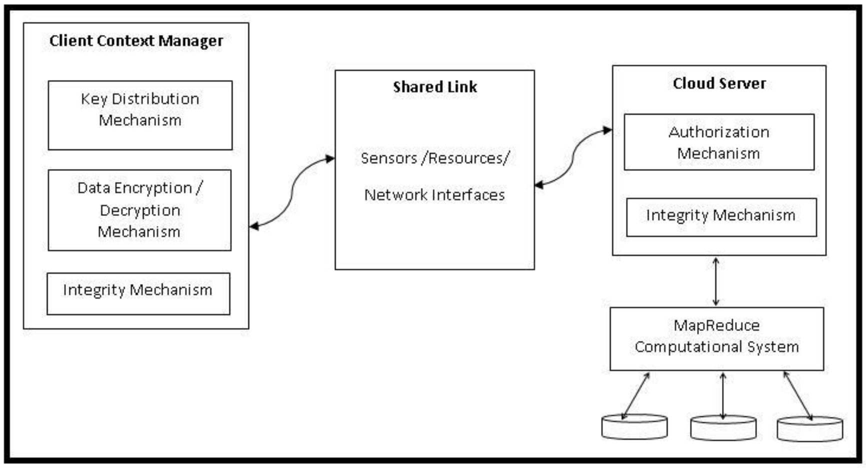

Fig1: Mobile Cloud Storage Security Architecture

The above figure depicts about privacy and secure architecture for mobile users. It consists of Client phase, Server phase and link phase, described in detail below.

- Client phase deals with three modules as key distribution mechanism, encryption and integrity mechanisms. o The key distribution mechanism prevents unauthorized access to access cloud server by verifying of authenticate and then authorize the user. Key distribution mechanism is responsible for operations like key generation, load, update, backup and destroy; in order to write or read operations on data storage.

o In order to provide confidentiality of data, the framework used a symmetrical encryption algorithm, which increases efficiency and reduces burden on server.
o To ensure the integrity of data, the system uses CRC or a hash algorithm, to not to alter data during transmission.

- Link phase mediates, establishment communication between client and server via sensors, resources or standard network interface in the form of an encrypted files.
- Cloud Server phase provides to authorize and check integrity of the users request and respond. Writing to disk and reading from storage space would be check with checksum and time stamp; if checksum and time stamp are correct then access of either read or write permission granted through MapReduce [8] computational system, then not otherwise. Here MapReduce computational system will intern verifies lookup and process the index of storage space with help of a set of pair <key, value>.

Write operation

The following steps shows how a disk information is shared between client and server

Client (Mobileuser)	**Link**	**Cloud Server**
1. Name+Pwd+Captcha	2. Name+Pwd+Captcha	3. Name+Pwd+Captcha
6. Receive the disk information	5. Encrypted file + disk index name+ checksum + timestamp	4. Authorization, disk information returned
7. Encrypted file + disk index name+ checksum + timestamp	8. Encrpted file + disk index name+ checksum + timestamp	9. Calculate disk resource and storage
12. Receives Ack	11. Send Ack	10. Send Ack

Read operation

The following steps shows how a disk information is shared between client and server

Client (Mobileuser)	**Link**	**Cloud Server**
1. Name+Pwd+Captcha	2. Name+Pwd+Captcha	3. Name+Pwd+Captcha
6. Authorize & Receive the disk information	5. disk index name+ timestamp	4. Authorization, disk information returned
7. disk index name+ timestamp	8. disk index name+ timestamp	9. Calculate checksum
12. Receives encrypted file and calculates checksum	11. Return encrypted file	10. Return encrypted file

3.2 Privacy & Access Control

The computational system uses Secured MapReduce framework (SMR) and Distributed File Systems (DFS) to store and retrieve data at Data Center [8]. This system executes for trusted users, processes read and write operations on data and connect to the shared link; and there will be limited privileges to untrusted users.

Privacy preserving from calculated result is a big challenge. Therefore, it can be used to calculate the practical computations; which are made to preserve privacy by adding noise to the calculated output. Here the noise may be small value, Δ. This gives the difference of accuracy of the output and the probability of sensitive information that has leaked. If there is maximum change occurred in function's output when a value is added to or removed from input data, then it is called functional sensitivity.

4. IMPLEMENTATION

MapReduce framework, Hadoop DFS, JVM and MongoDB were used to implement the proposed work [9] [10] [11]. And it is verified that, the mobile user does not know which systems resource is used to leak information, by executing malicious mappers.

5. EXPERIMENTAL RESULTS

The experiment is conducted on a image_flower_photos dataset, consists of 5 types of flowers. The following table resultants, accessed the link and found the number of flowers.

Table1: Experimental Results

Link	**Type of Flower**	**Real**	**Output**	**Desired**	**Output**
Articleflowerimags/dataset/img_flower_photos_all_data.csv/		3670	3669.9	3669	3669.7
S3://projectbtech/img/flower_photos/daisy/10172636503_21bededa75_n.jpg	Daisy	633	633.3	632	632.9
S3://projectbtech/img/flower_photos/dandelion/10043234166_e6dd915111_n.jpg	Dandelion	898	897.9	897	898.2
S3://projectbtech/img/flower_photos/roses/16258946661_f9739cdc0a.jpg	Rose	641	640.8	640	640.8
S3://projectbtech/img/flower_photos/sunflowers/10862313945_e8ed9202d9_m.jpg	Sunflower	699	699.2	698	699.3
S3://projectbtech/img/flower_photos/tulips/13888320717_d2919a879b_m.jpg	Tulips	799	798.9	798	798.3

6. CONCLUSION

Cloud storage is current trend storage system, with the development of networking management technologies all the problems now can be solved. The proposed work ensures design and implement of cloud storage transmission through mobile can be done safely and securely. Here this model uses privacy preserving through MapReduce Computation System. There is a flexibility to write or extend the code of mapper class and reducer class.

7. REFERENCES

[1] Chief Information Officer's Coucil (CIO). Cloud Computing: Benefits and risks of moving federal it into the cloud, 2010.

[2] S. Hansel. AOL removes search data on vast group of web users. New York Times, Aug 8 2006.

[3] Nrayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In S&P, 2008.

[4] Lin Qinying, GuiXiaolin, ShiDeqin et al, Study of the secure AccessStrategy of Cloud Storages. Journal of Computer Research anddevelopment, 2011,48 (z1) 240-243.

[5] Mu Fei, Xue Wei, Shu Jiwu et al, An analytical Model for Large –Scale Storage System with Replicated Data. Journal of ComputerResearch and development, 2009, 46(5) 492-497.

[6] Hong Cheng, Zhang Min, Feng Dengguo, Achieving efficientdynamic cryptographic access control in cloud storage. Journal onCommunications, 2011, 32(7): 125-132

[7] Indrajit Roy , Srinath T. V. Setty , Ann Kilzer , VitalyShmatikov , Emmett Witchel, Airavat: security and privacy forMapReduce, Proceedings of the 7th USENIX conference onNetworked systems design and implementation, p.20-20, April28-30, 2010, San Jose, California

[8] Quang Tran and Hiroyuki Sato; A Solution For Privacy Protection In MapReduce; 2012 IEEE 36th International Conference on Computer Software and Applications.

[9] Yang Wei, Zhao Jianpeng, Zhu Junmao, Zhong Wei and Yao Xinlei; Design of Security and Implementation Cloud Storage Framework; 2012 Second International Conference on Instrumentation & Measurement, Computer, Communication and Control.

[10] HuseyinUlusoy, Murat Kantarcioglu, ErmanPattuk, Kevin Hamlen; Vigiles: Fine-grained Access Control for MapReduce Systems; The University of Texas at Dallas, Richardson, Texas, USA; 2014 IEEE International Congress on Big Data.

[11] Security concept and implementation for a cloud based e-Science infrastructure; Thomas Ludescher, Thomas Feilhauer, Peter Brezany; 2012 Seventh International Conference on Availability, Reliability and Security.