ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Security Enforcement with Cost Assessment for Cloud Data

A. Selvi[1], B. Arunkumar [2]

III M.E., Dept of CSE, Karpagam University, Coimbatore, India[1]

Assistant Professor, Dept of CSE, Karpagam University, Coimbatore, India[2]

ABSTRACT*:* The cloud computing has become universal, casting its outline over practically every feature of business process in every industry. Its success is due largely to customers' ability to use services on demand. The cloud user can choose with a pay-as-you go packages, which has proved convenient in many industries. Transmission cost plays an important role when trying to minimize cloud cost. The cloud have to provide a trust ability to the cloud customer. Also the performance of the cloud should not be degraded while providing a privacy over the cloud data. The proposed architecture provides a cost evaluation and privacy over cloud data stored by the data owner. A parallel encryption technique provides a privacy and secured environment over cloud database. The proposed encryption model improves the performance of process computation and cost appraisal guarantees the same level of scalability and availability of the cloud service. In this paper, we propose the parallel encryption for secured data over the cloud in customer point of view. Also we will focus on the SQL-based cloud which will dynamically change.SQL databases are difficult to scale, meaning they are not natively suited to a cloud environment, although cloud database services based on SQL are attempting to address this challenge.

KEYWORDS: cloud data, AES , ciphertext

I. INTRODUCTION

Cloud computing provides a variety of computing resources , from servers and storage to enterprise applications such as email, security, backup/DR, voice, all delivered over the Internet. A cloud database is a database that typically runs on a cloud computing platform, such as Amazon EC2, GoGrid, Salesforce, Rackspace, and Microsoft Azure. There are two common deployment models: users can run databases on the cloud independently, using a virtual machine image, or they can purchase access to a database service, maintained by a cloud database provider. Of the databases available on the cloud, some are SQL-based and some use a NoSQL data model. Cloud computing typical requirements and models are platform (PaaS), software (SaaS),infrastructure (IaaS), Services-based application programming interface (API). Infrastructure and application model dealing with sharing of compute cycles, data, storage and other resources. Cloud service provider monitor the constant performance. Each Cloud Storage object's data and metadata is encrypted with master keys, if you prefer to manage your own keys then you can still encrypt data yourself prior to writing it to Cloud Storage.

Cloud Storage, Data as a service (DaaS) and Database as a service (DBaaS) are the different terms used for data management in the Cloud. They differ on the basis of how data is stored and managed. Cloud storage is virtual storage that enables users to store documents and objects. Dropbox, iCloud etc. are popular cloud storage services

II. RELATED WORK

Cloud computing allows accessing resources across the Internet transparently, in a simple way and providing high scalability and availability. Organizations need to understand where and how security policy is defined, how access is managed, and how audit and compliance requirements are me given the distinct capabilities that providers and consumers have in a Private Database Cloud as in [1]. In this fast moving world we need something essential for fast computation [4]. So here comes the parallel architecture. Along with the popular use of computer, information security has also become one of the problems which need to be solved. Encrypting databases [3] is very important because

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

databases are one of the best targets for hackers. They prefer to get millions of confidential information all at once rather than intercepting them one at a time, and a million or more records at once is what they can get from hacking a database. Cloud Computing [8] presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. DBaas [7] that poses several research challenges in terms of security and cost evaluation from customer point of view. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management [6].As said in [10] AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information. So, it has broad applications, such as smart cards and cell phones, WWW servers and automated teller machines, and digital video recorders. Numerous architectures have been proposed for the hardware implementations of the AES algorithm.

III. PROPOSED ALGORITHM

A. *Description of the Proposed Algorithm:*

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

Parallel AES Algorithm

AES is a block cipher algorithm used to encrypt data using a 128-bit key.
Step 1: Data is divided up into 128-bit blocks and encrypted
Step 2: Each block goes through 11 rounds of encryption, with 4 steps: SubBytes, ShiftRows, MixColumns, AddRoundKey .
Step 3: The ciphertext is produced and is recovered by performing decryption with the same 128-bit key.

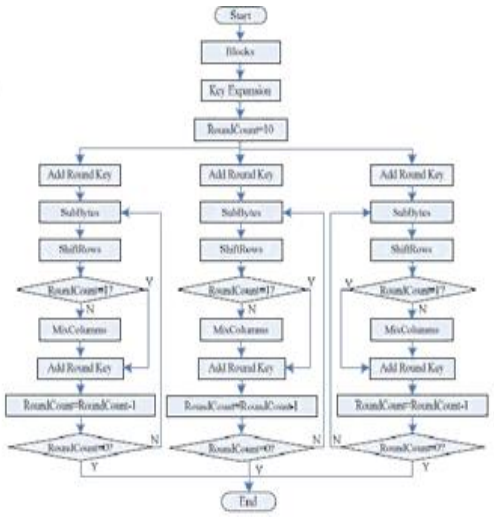

Fig. 2: Parallel AES Algorithm

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

IV. IMPLEMENTATION

In cloud database the traditional encryption algorithms are difficult to deal with large size of files and the data cost will be high while we download files. Cloud database model are major issue for buyers, in cloud the data is stored on numerous servers that required adequate encryption schemes in which we propose the parallel encryption scheme to reduce the cost and enforce the security.

The output screenshots of Administration data upload and Encrypted data are shown in Figure 1 & 2 respectively.

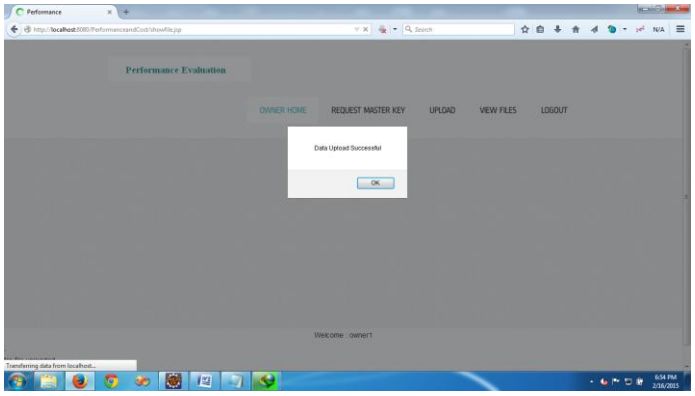

Figure 1 : Administrator Data Upload

The above figure shows how the administrator uploads data

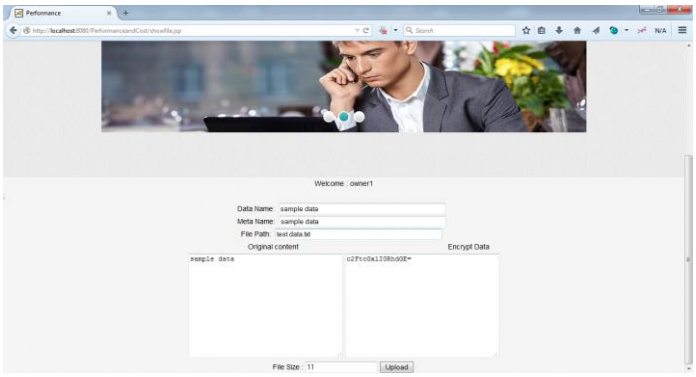

Figure 2 : Encrypted data

The above figure shows the encrypted data.

V. CONCLUSION AND FUTURE WORK

The proposed system guarantees the ability to minimize the cloud cost in any cloud database, even when the set of SQL queries dynamically changes. The proposed parallel encryption scheme, which was initially proposed for applications not referring to the cloud, encrypts the uploaded data and increases the performance of the cloud data for the cloud customer. We propose the parallelism for the cost estimation model for evaluating cloud database costs in plain and encrypted instances from a customer point of view. In which it improves the scalability and availability of the cloud service. As expected, parallel encryption influences the costs related to file size, time taken to respond from the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

database and the network usage of a database service. In future we can evaluate the cost over the different servers through various network resources.

REFERENCES

1. J. Cao, B. Carminati, E. Ferrari, and K.-L. Tan, "Parallel data processing ," IEEE Trans. Depend. Secure Comput., vol. 8, no. 3, pp. 337–352, May–Jun. 2011.
2. RC Chen, CT Bau, CJ Yeh, "Merging domain ontologies based on the Word Net system and Fuzzy Formal Concept Analysis techniques" , vol. 51, issue no. 1, pp. 229–237, Feb. 2004.
3. R. J. Bayardo and R. Agrawal ,"Parallel distributed systems" ,IEEE Trans. Depend. Secure Comput., vol. 8, no. 3, pp. 337–352, May–Jun. 2011.
4. Chris Norman , "Parallel AES Implementation" , International Journal of Scientific & Engineering Research, vol. 58, issue no. 6, pp. 3041–3052, Jul. 2009.
5. Anjana Nigam, Prof. Roopali Soni, "A Novel Approach For Enhance Security On Database Using Proposed Algorithms", International Journal of Emerging Technology and Advanced Engineering , ISSN 2250-2459, Volume 2, Issue 11, November 2012
6. Sanjanaashree, Accelerating Encryption/Decryption Using GPU's for AES Algorithm, International Journal of Scientific & Engineering Research, Volume 4, Issue 2, February-2013.
7. Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "SecurityIssues for Cloud Computing", International Journal of Information Security and Privacy,vol 59, pp 1224-1238, 2010
8. Jiyi Wu et al, "Recent Advances in Cloud Storage", in Third International Symposium on Computer Science and
9. Computational Technology(ISCSCT '10), Jiaozuo, P. R. China, 14-15,August 2010, pp. 151-154.
10. Vishal Pachori, Gunjan Ansari, Neha Chaudhary "Cloud Platform Storage with Server-side encryption " International Journal of Engineering Research and Applications , ISSN:2248-9622 , Vol. 2, Issue 1,Jan-Feb 2012, pp.967-971.