International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Privacy-Preserving Methodology in Distributed Computing using Encrypted Cloud Database

S. J. Chougule[1], C. M. Jadhav[2]

[1]Solapur University, Computer Science and Engineering, A/P ramanadnagar Kirloskarwadi

[2]Professor, Computer Science and Engineering, Solapur University, A/p Solapur

Abstract: ***Nowadays cloud computing is emerging technology in engineering which gives on-demand resources which located on internet. It is also provide storage of large amount of data to the cloud users which use cloud services and distribute data on different server for huge speed over the network. Using distributed system we cannot get security of user's confidential data. It becomes the main problem in cloud users who uses cloud computing environment. So to increase the security problem, we can propose an encryption algorithm for better and better performance. It is a new approach and it met the requirements of public key systems. By using algorithm it will increase the security in data and consumes less time and less cost. The efficacy of the proposed architecture is evaluated through theoretical analyses and extensive experimental results based on a prototype implementation subject to the TPC-Standard benchmark for different numbers of clients and network latencies.***

Keywords: Confidentiality, SecureDBaaS, Privacy, cloud storage, metadata, PLA, PBA, PLAC.

1. Introduction

Previous paper work in this area is carried out in which secure database system which is implemented and data is encrypted form and stored on server. Only authorised users only can gain access the database other clients who want to access the same data then client should be authorised. Cloud data is hidden from cloud providers, intermediaries but only accessible and visible to the user who is authorised.

This context proposes Secure DBaaS as the novel solution that allows cloud tenants to take full advantage of DBaaS qualities, such as availability, reliability, and elastic scalability, without exposing unencrypted data to the cloud provider. Independent and geographically Clients can perform simultaneous operations on encoded data in distributed system, including SQL statements that modify the database structure; to preserve data confidentiality and consistency at the client and cloud level; to eliminate any intermediate server between the cloud client and the cloud provider. Using secure DBaaS we can achieve availability, scalability and elasticity, also improving data confidentiality. Cloud Computing is a distributed architecture in which server uses resources on a scalable platform so as to provide an on-demand computing resources and services. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) both offer services. Cloud computing is the technique which provides network access to shared pool on storage, network and application which uses convenient networking uses. Generally cloud service providers provide three types of net services i.e. Software's as a Service (SaaS), Platforms as a Service (PaaS) and Infrastructures as a Service (IaaS).. The service provided by cloud provides are on payable basis, consumable user pay for particular resources which user uses. Cloud computing can meet the requirement of leading market place to ensure the leading edge for cloud users [1].

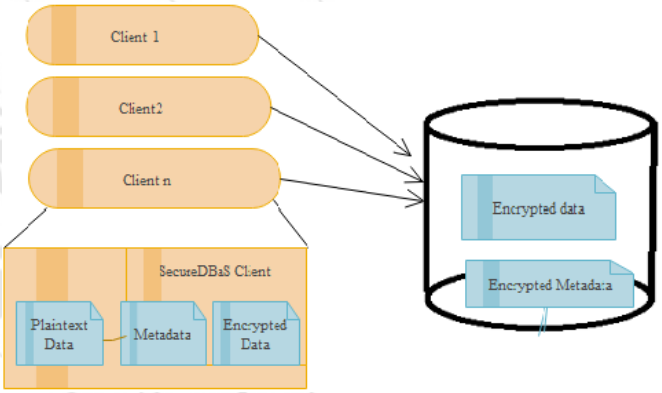

Figure 1: Cloud DBaaS

1.1 Cloud Computing Building Blocks

1.1.1. Different models of cloud computing

Cloud services are divided into four types:

- Software as a Service (SaaS),
- Platform as a Service (PaaS),
- Infrastructure as a Service (IaaS)
- Database as a Service

Software as a Service SaaS: In SaaS service Application Service Providers (ASP) deliver different software applications through the Internet. Using this service consumer does not need to install and operate the application on machine. It Also removes the load maintenance of software; continuing operating system, preservation and maintenance [3].

Platform as a Service (PaaS): PaaS provides platform to run any application without installing and downloading any software for developers, users and IT manager. Examples of

PaaS includes: Force.com, Google App Engine and Microsoft Azure.

Infrastructure as a Service (IaaS): Infrastructure as a service (IaaS) uses Virtualization technology to share hardware resources for executing services. This type of service is to allocate resources to server, network and storage devices which are accessible by application and operating system. It also offers basic on-demand infrastructure services and using Application Programming Interface (API) to interact with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In cloud computing the user does not maintain the underlying hardware in the cloud infrastructure, but user controls the storage, operating systems, Examples of IaaS include Amazon Elastic Cloud Computing (EC2), Amazon S3, and GoGrid.

Database as a Service (DaaS): In this type of service it uses DBaaS model which is fee-based subscription service in which the dataset runs on the service provider's physical infrastructure. Different service levels are usually available. In a classic DBaaS arrangement, the provider maintains the physical infrastructure. A customer can set up a managed hosting arrangement, in which the provider handles database maintenance and management. This service also provides to small business that need database to store data of employee or store any organizational data.

2. Literature Survey

Gartner in [8] recognized security risks that are essential to be considered before enterprises make decisions regarding the conversion into a cloud computing model [9]. These problems are as follows:

1) **Authorized user access:** the potential risk of exposing sensitive organizational data over a network platform, due to the limited physical, logical and personal controls outside the organizational boundaries.
2) **Conformance to regulations:** in case of auditing an external third-party space processing data outside the organizational boundaries is still subject to problem measures.
3) **Storage space:** cloud customer has no hint about the exact location of their data that requires service provider commitment to comply with privacy restrictions.
4) **Data separation:** clouds hold the customers' data over a shared place where data segments are not stored in sequential manner, for that a reliable and well-tested encryption schemes are needed.
5) **Recovery:** This system should have to provide recovery of data by service providers.
6) **Investigation:** due to the scattering of the data and resources interruption attempts are hard to be tracked and spotted over the cloud network. The high complexity level investigation is impossible because.
7) **Long-term viability:** There should be guarantee of data availability if in case of service provider impoverishment occurs.

Cloud computing introduces risks, effects and magnifies. Total threats and their consequence on security risks and vulnerabilities were explained in [10]. Due to the increased on-demand and rank of cloud service there need to regulate the cloud services security. [12]. For instance, standardized Security Level Agreement (SLA) guarantees translucent assurance and increases the faith among cloud adopters. This research presents an abstract study of the data security issues and challenges in cloud computing.

3. Algorithms

Cryptosystems can be of two types:

- Asymmetric Cryptosystems
- Symmetric Cryptosystems

3.1 Asymmetric Cryptosystems

In an asymmetric key cryptosystem two different keys are used for the encryption and decryption of data. The key used for encryption is kept public and so as called public key, and the decryption key is kept secret and called private key. The keys are generated in such a way that it is difficult to derive the private key from the public key.

The source and the destination both have two keys in an asymmetric cryptography system. However, the private key is kept in private and not sent over with the message to the receiver, although the public key is sent through network.

Advantages of Asymmetric Cryptosystem

- In asymmetric, cryptography there is no need to exchanging keys, thus eliminating the key distribution problem.
- The primary advantage of asymmetric key cryptography is improved security because the private keys always need not to be transmitted or revealed to anyone.
- This Can provide digital signatures that can be rejected

Disadvantages of Asymmetric Cryptosystem

A disadvantage of using asymmetric cryptography for encryption is speedy because there are popular secret key encryption methods which is faster than any currently available asymmetric encryption method.

3.2 Symmetric Cryptosystems

A symmetric cryptosystem (or private key cryptosystem) uses only one key for both encryption and decryption of the data. The key used for encryption and decryption is called the private key and only people who are authorized for the encryption/decryption

Advantages of Symmetric Cryptosystems

- A symmetric cryptosystem is faster.
- In Symmetric Cryptosystems, encrypted data can be transferred on the link even if there is a possibility that the data will be intercepted. Since there is no key transferred with the data, the chances of data being decrypted are null.
- A symmetric cryptosystem uses password authentication to prove the receiver's identity.

- A system only which possesses the secret key can decrypt a message.

Disadvantages Symmetric Cryptosystems

- Symmetric cryptosystems have a problem of key transportation. The secret key is to be transferred to the receipt system before the actual message is to be transferred. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only safe way of exchanging keys would be exchanging them personally.
- Cannot provide digital signatures that cannot be repudiated

Table 1: Symmetric/Asymmetric

Characteristic	Symmetric Cryptography	Asymmetric Cryptography
Key user For Encryption/ Decryption	Same key used for encryption and decryption	One key user for encryption and another or different key user for decryption
Speed Of Encryption/ Decryption	Very fast	Slow
Size of resulting encrypted text	Usually same of less than original data	More than the original clear text size
Key agreement /exchange	Big Problem	No problem at all
Number of key required	Equal the about the square of the number of participants so scalability is an issue	Same as the number of participants, so scale up is quite well
Usages	Mainly for encryption and decryption (confidentiality), Not used for digital signature	Can be used for encryption and decryption as well as digital signature

General-purpose ciphers used for encryption tend to have different design goals. For example, the symmetric-key block cipher AES can be used for generating hash values, but its key and block sizes make it nontrivial and inefficient.

Table 2: List of Common encryption standard

Encryption Standard			
Acronym	Name	Type	Use
DES	Data Encryption Standard	Block Cipher	General
3DES	Triple DES	Block Cipher	General
AES	Advanced Encryption Standard	Block Cipher	General
RC4	Rivet Cipher 4	Stream Cipher	SSL, WEP
MD5	Message Digest %	Hash Function	SASL, Kerberos
SHA-1	Secure Hash Algorithm	Hash Function	TLS, SSL
RSA	RSA	Public Key	General
PGP	Pretty Good Privacy	Public Key	General

Secure cryptographic hash a function has following key properties:

- Output length is small compared to input
- Computation is fast and efficient for any input
- Any change to input affects lots of output bits
- One-way value: The input cannot be determined from the output
- Strong collision resistance: Two different inputs can't create the same output

4. Cloud Security Issues and Challenges

4.1 Privacy Issue

Lack of user control

In SAAS environment controlling user's data is the responsibility of service provider. How customer can maintain control on data when information is processed or stored? It should not be prescribed in cloud computing environment. It is legal requirement user to make trust between customer and vendor [8].

Unauthorized Secondary Usage

One of the threats can occur if information is placed for illegal uses. In Cloud computing standard business model service provider can make profits from legal secondary uses of users' data, mostly the targeting of commercials [10].

Trans border Data Flow and Data Proliferation

One of the attribute of cloud is Data explosion in which it involves no controlling and managing of data by the data owners. Vendor guarantee to the ease of use by copy data in several datacenters. This is very difficult to ensure that replica of the data or its backups are not stored or processed in a certain authority, all these copies of data are deleted if such a request is made. Due to movement of data, CP make worse the trans-border data flow matter because it can be tremendously difficult to determine which specific server or storage device will be used [8].

Dynamic provision

Cloud has effervescent nature so there is no clear aspect that which one is legally responsible to ensure privacy of sensitive data put by customer on cloud [10].

4.2 Security

Access of data

It has the threat of access of sensitive information. The risk of data theft from machine has more chances in cloud computing environment data stored in cloud in long time duration any hacker can access this data [9].

Control over data lifecycle

To ensure the customer has resistor over data, if it remove or delete by data vendor then it cannot regain this data. In cloud IAAS and PAAS models virtual machine are used that process and then media wiped but there is no guarantee that user can get that data [3].

Availability and backup of important data

There is no any guarantee of availability and backup of data in this environment. In business backup is one of the important consideration [7].

Multi-tenancy
The feature of SAAS is that one program can run on multiple machines. CSP use multi-tenant application of cloud to decrease cost by using virtual machine but it increase more exposure [17].

Audit
To implement internal monitoring control CSP need external audit mechanism. But cloud computing get rid to provide auditing of the operation without effecting integrity [4].

	Description
Data Handling Mechanism	Classify the confidential Data. Define the geographical region of data. Define policies for data destruction.
Data Security Mitigation	Encrypting personal data. Avoid putting sensitive data in cloud.
Design for Policy	Fair information principles are applicable.
Standardization	CSP should follow standardization in data tracking and handling.
Accountability	For businesses having data lost, leakage or privacy violation is catastrophic Accountability needs in legal and technical. Audit is need in every step to increase trust All CSP make contractual agreements.
Mechanism for rising trust	Social and technological method to raise trust. Joining individual personal rights, preferences and conditions straightforwardly to uniqueness of data. Devices connected should be under control by CSP. Use intelligent software.

References

[1] Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy"Cloud Computing: Security Issues and Research Challenges" IRACST -(JCSITS) Vol. 1, No. 2, December 2011.
[2] M. Armbrust, A. Fox, R. Grith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A View of Cloud Computing," *Communications of the ACM*, Vol. 53, No. 4, 2010, pp. 50-58. http://dx.doi.org/10.1145/1721654.1721672
[3] D. Jamil and H. Zaki, "Cloud Computing Security," *International Journal of Engineering Science and Technology*, Vol. 3, No. 4, 2011, pp. 3478-3483.
[4] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," *Proceedings IEEE in INFOCOM*, San Diego, 14-19 March 2010, pp. 1-9.
[5] S. Dhar, "From Outsourcing to Cloud Computing: Evolution of It Services," *Management Research Review*, Vol. 5, No. 8, 2012, pp. 664-675. http://dx.doi.org/10.1108/01409171211247677
[6] A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.
[7] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0.
[8] Osama Harfoushi[1], Bader Alfawwaz[2], Nazeeh A. Ghatasheh[3], "Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review" Vol.6 No.1(2014), Article ID:42813,7 pages DOI:10.4236/cn.2014.61003
J. Brodkin, "Gartner: Seven Cloud-Computing Security Risks," InfoWorld, 2008.
http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
[9] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," International Conference on Computer Science and Electronics Engineering, Vol. 1, Hangzhou, 23-25 March 2012, pp. 647-651.
[10] B. Grobauer, T. Walloschek and E. Stocker, "Understanding Cloud Computing Vulnerabilities," IEEE Security Privacy, Vol. 9, No. 2, 2011, pp. 50-57. http://dx.doi.org/10.1109/MSP.2010.115
[11] A. Lenk, M. Klems, J. Nimis, S. Tai and T. Sandholm, "What's Inside the Cloud? An Architectural Map of the Cloud Landscape," Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, Washington DC, 23 May 2009, pp. 23-31. http://dx.doi.org/10.1109/CLOUD.2009.5071529
[12] S. Ramgovind, M. Elo and E. Smith, "The Management of Security in Cloud Computing," Information Security for South Africa, Sandton, 2-4 August 2010, pp. 1-7