ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

A Survey on Two Cloud Secure Architecture

Sujata Bahadure, D.K. Chitre

M. E Students, Department of Computer Science Engineering, Terna Engineering College, Nerul, Navi Mumbai, India

Professor, Department of Computer Science Engineering, Terna Engineering College, Nerul, Navi Mumbai, India

ABSTRACT: The security challenges are still among the major obstacles when considering cloud adoption services. Industries and individuals outsource database to low-cost applications and services.in order provide enough functionality for SQL queries, many secure database schemes have been proposed. The main reason is that the database is hosted and processed in the cloud server, which is beyond the control of the data owners. For the numerical query, these schemes do not provide sufficient privacy protection against practical challenges, for example, loss of static property privacy, access patterns. In addition, the growing number of consultations will inevitably be Learn more about the cloud server. In this article we propose two cloud architecture for a secure database with that provide protection to several questions related to the numeric range. The security analysis shows that the confidentiality of numeric information is strongly protected against cloud providers in our proposed scheme.

KEYWORDS: database, range query, privacy preserving, cloud computing

I. INTRODUCTION

Cloud computing is a rising computing standard in which assets of the computing framework are given as a service over the Internet. As guaranteeing as it may be, this standard additionally delivers a lot of people new challenges for data security and access control when clients outsource sensitive data for offering on cloud servers, which are not inside the same trusted dominion as data possessors. Numerous services like email, Net banking and so forth are given on the Internet such that customers can utilize them from anyplace at any time. Indeed cloud storage is more adaptable, how the security and protection are accessible for the outsourced data turns into a genuine concern. The three points of this issue are availability, confidentiality and integrity.

A cloud User, such as an IT company, wants to outsource the database to cloud, which contains valuable and sensitive information (such as transaction logs, account information, medical information) and then access to the database. Due to the hypothesis that the cloud provider is honest, but curious, the cloud might try the best to get private information for its own benefits. Worse still, the cloud could convey such sensitive information to for-profit business competitors, which is an unacceptable operational risk.

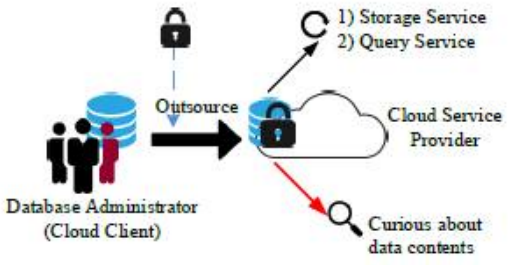


Fig. Outsource Database and Services

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

II. RELATED WORK

This Paper analyzes recent research related to single or multiple cloud security and addresses possible solutions. Research on using multicloud providers to maintain security has been found to receive less attention from the research community than using individual clouds. This work aims to promote the use of multiple clouds thanks to its ability to reduce security risks affecting the user of cloud computing [1].

We present new preprocessing techniques that allow to obtain interactive query times in large text collections (100 GB of text, served by a single machine). Consider two similarity measures, one in which the query terms coincide with similar terms in the collection (for example Algorithm of algorithm matches or vice versa) and one in which the query terms coincide with terms with a similar prefix in the collection (for example, Alori corresponds to the algorithm). The latter is important when we want to show the results instantly after each keystroke (search while writing). All the algorithms have been completely integrated into the complete search engine [2].

In this Paper, we define and solve the search for keywords classified as effective but protected on data encrypted in the cloud. We use order preserving symmetric encryption to protect data in the cloud. Although many research techniques are available, they do not offer efficient search results. For example, the search results generated 40 records and in those 30 records are relevant and the remaining 10 records generate irrelevant data. This paper focuses mainly on research methods that will improve the effectiveness of research. We use search methods based on keywords and concepts to retrieve relevant search criteria. This method will restore documents based on broader conceptual entities, which will improve the efficiency of the search [3].

Security challenges remain among the biggest obstacles when considering the adoption of cloud services. Cloud security is becoming a key element of differentiation and competitive advantage among cloud service providers. This triggered many research efforts, which led to a series of proposals aimed at various threats to cloud security. Along with these security issues, the cloud paradigm comes with a new set of unique features that open the way for new approaches, techniques and security architectures. The basic idea is to use multiple different clouds at the same time to mitigate the risks of manipulation and disclosure of malicious data. By integrating multiple clouds, trust assumption can be reduced to hiring non-collaborative cloud service providers. This configuration makes it much more difficult for an external attacker to retrieve or manipulate data hosted by a specific cloud user [4].

Cryptography is a consolidated technology for the protection of sensitive data. However, once encrypted, the data is no longer easily searchable, apart from the exact matches. We present an encryption scheme of order retention for numerical data that allows you to apply any comparison operation directly to the encrypted data. The results of the produced query are solid (without false access) and complete (without errors). Our schema correctly handles updates and new values can be added without requiring changes in the encryption of other values. It allows to build standard database indexes on encrypted tables and can be easily integrated with existing database systems. The proposed scheme is designed to be implemented in application environments where the intruder can access the encrypted database, but has no information about the previous domain, such as the distribution of values, and cannot encrypt or decode arbitrary values from his election. Cryptography is robust against the estimation of real value in such environments [5].

III. PROPOSED SYSTEM ARCHITECTURE

This paper focuses on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, such as employee transaction details or employee medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing surveyed.

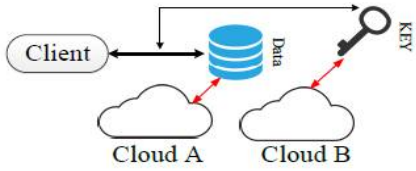
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

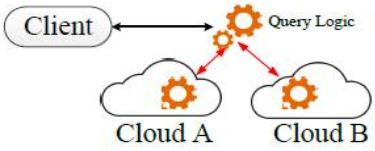
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018



(a) Knowledge Partition of Stored Data



(b) Knowledge Partition of Query Logic

2. Two-Cloud Database Architecture and Knowledge Partition Prototype

1) We propose a two non-colluding cloud architecture to conduct a secure database service, in which the data is stored in one cloud, while the knowledge of query pattern is well partitioned into two parts, and knowing only one cannot reveal any private information
2) We then present numeric-related SQL range query with privacy preservation, and especially, such protocols will not expose order-related information to any of the two non-colluding clouds.

The proposed system is based on the idea to use multiple distinct clouds at the same time to mitigate the risks of malicious data manipulation, disclosure, and process tampering. By integrating distinct clouds, the trust assumption can be lowered to an assumption of non-collaborating cloud service providers.
Further, this setting makes it much harder for an external attacker to retrieve or tamper hosted data or applications of a specific cloud user. The underlying concept is to partition the application data which is encrypted into fragments thus distributing fine-grained fragments of the data to distinct clouds. None of the involved cloud providers gains access to all the data, which safeguards the data's confidentiality.

The data is partitioned and stored in multiple clouds. So, even if a single cloud is exploited, the malicious intruder could not lay his hands on the entire data as it is only partially available in the cloud. In addition to the encryption done by the cloud provider, the proposed system also encrypts the user's data, thus providing enhanced security.

IV. METHODOLOGY

AES Algorithm

AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys.
Rijendeal was founder. In this drop we are using it to encrypt the data owner file.
Input:
128_bit /192 bit/256 bit input (0, 1)
Secret key (128_bit) +plain text (128_bit).
Process:
10/12/14-rounds for-128_bit /192 bit/256 bit input
Xor state block (I/p)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

Final round: 10, 12, 14
Each round consists: sub byte, shift byte, mix columns, add round key.
Output:
Cipher text (128 bit)

Fragmentation Algorithm
Input: File
Output: Chunks
Step1: If file is to be split go to step 2 else merge the fragments of the file and go to step
Step2: Input source path, destination path
Step3: Size = size of source file
Step4: Fs = Fragment Size
Step5:NoF = number of fragments
Step6: Fs = Size/Nof
Step7: We get fragments with merge option
Step8: End

V. CONCLUSION

In this paper, we presented a two cloud architecture with an intersection for outsourced database service, which ensures the privacy preservation of data contents and SQL range query pattern. At the
same time, with the support of range queries, it not only protects the confidentiality of static data, but also addresses potential privacy leakage in statistical properties or after large number of query processes. Security analysis shows that our scheme can meet the privacy-preservation requirements.

REFERENCES

1] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom " Cloud Computing Security: From Single to Multi-Clouds" in Proceedings of the 45th Hawaii International Conference on System Science (HICSS2012). IEEE, 2012, pp. 5490–5499
2] Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multikeyword fuzzy search over encrypted outsourced data with accuracy improvement," IEEE Transactions on Information Forensics and Security, vol. 11, no. 12, pp. 2706–2716, 2016.
3] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Proceedings of the 30th IEEE International Conference on Distributed Computing Systems (ICDCS2010). IEEE, 2010, pp. 253–262
4] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, "Security and privacy-enhancing multicloud architectures," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 212– 224, 2013.
5]R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data. ACM, 2004, pp.563–574
[6] Michael L. Brodie, "Data Integration at Scale: From Relational Data Integration to Information Ecosystems", 2010 24th IEEE International Conference on Advanced Information Networking and Applications.
[7] Zhang Jianhong, Chen Hua, "Security Storage in the Cloud Computing: A RSA-based Assumption Data Integrity Check Without Original Data, 201 International Conference on Educational and Information Technology (ICEIT 2010).
[8] Zue Jing, Zhang Jian-jun, "A Brief Survey on the Security Model of Cloud Computing, 2010, Ninth International Symposium on Distributed Computing and Spplicatino to Business, Engineering and Science.
[9] Xin Yue Yang, Zhen Liu, Yan Fu, "MapReduce as a Programming Model for Association Rules Algorithm on Hadoop".
[10] Kevin Chiew, Shaowen qin, "Analysis of Privacy- Preserving Mechanisms for Outsourcing Data Mining Tasks, 2008, IEEE.
[11] Ian Molloy, Ninghuri li, and Tiancheng Li, "On the (In) Security and (Im) Practically of Outsourcing Precise Association Data Mining, 2009 Ninth IEEE International Conference on Data Mining.
[12] Jinghan Ren, Baowen zhang, "An Improvement on a Non-deterministic One-to-n Substitution Scheme in Outsourcing Association Rule Mining", 2009 World Congress on Computer Science and Information Engineering.