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 4, April 2018

A Survey on Two Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving

Amit Deore [1], Surajsingh Malas [2], Vaibhav Pawde [3], Prof. Ila Savant [4]

B.E Student, Dept. of Computer Engineering, Marathwada Mitra mandal's college of Engineering karvenagar, Pune, Savitribai Phule Pune University, Maharashtra, India[1, 2, 3]

Assistant Professor, Dept. of Computer Engineering, Marathwada Mitra mandal's college of Engineering karvenagar, Pune, Savitribai Phule Pune University, Maharashtra, India[4]

ABSTRACT: In most of the organization, database management is the key component in the case of information infrastructure. A two- cloud architecture with a series of interaction protocols for outsourced database service, which ensures the privacy preservation of data contents, statistical properties and query pattern. In place of database management in-house, the computer industries have moved on the latest trend of outsourcing the database. The principle reason is that database is facilitated and handled in cloud server, which is outside the ability to control of data proprietors. In the database management, one of the necessary requirements is to provide security to the database by holding the confidential information, but when the database is encrypted there exist the problem of processing queries. Furthermore enhance the security while ensuring practicality and the logical and mathematical queries those plans can't give adequate security assurance against possible difficulties. We have studied some of these research works and analyzed the best possible ways to come to the desired level of privacy preservation for cloud computing. The security analysis shows that the confidentiality of numeric information is strongly protected against cloud providers in our proposed architecture.

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.

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 4, April 2018

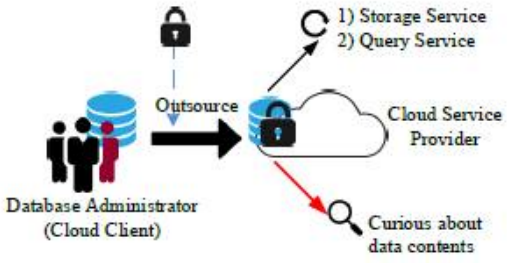

Fig1. Outsource Database and Services

II. RELATED WORK

This Paper analyzes recent research related to single or multiple cloud security and addresses possible solutions. Research on using multi-cloud 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][4]

We present new preprocessing techniques that allow obtaining 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][5].

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].

III.EXISTING SOLUTIONS

Due to the privacy concerns that the cloud service provider is assumed semi-trust. It becomes a critical issue to put sensitive service into the cloud, so encryption is needed before outsourcing sensitive data. The cloud could forward such sensitive information to the business competitors for profit, which is an unacceptable operating risk. Client's frequent queries will inevitably and gradually reveal some private information on data statistic properties.

Motivation:

In existing system only use the access control techniques to block friend in list. Don't text based preference are support and therefore it is not probable to avoid un-desired content is does not matter user who propose them Provided that this service is does not a matter of expending beforehand defined web message mining techniques for a unlike usage, moderately it require to developed ad-hoc classic strategies.

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 4, April 2018

IV. PROPOSED SYSTEM ARCHITECTURE

Due to the drawbacks in existing system we are proposing a system which 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 entrusted 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.

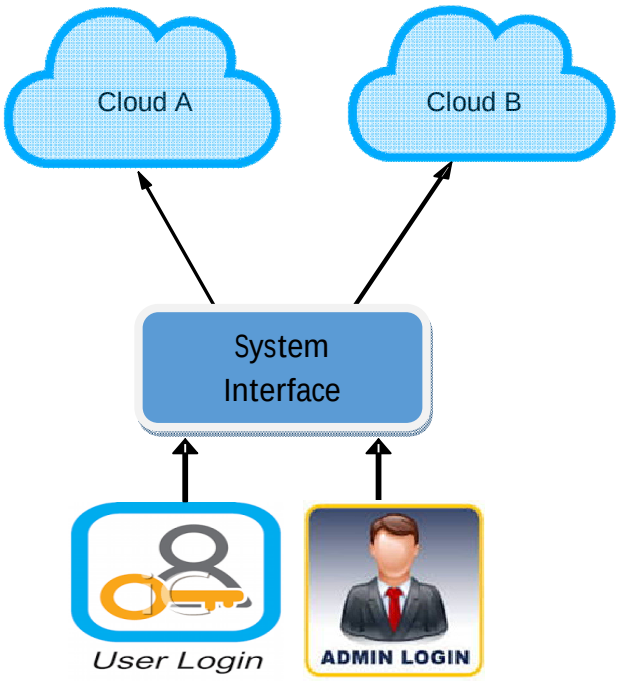

Fig 2. Proposed System Architecture

V. PROPOSED ALGORITHM

Step 1: Admin Login-

Our proposed secure database system includes a database administrator, and two non-colluding clouds. In this model, the database administrator can be implemented on a client's side from the perspective of cloud

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 4, April 2018

service. The two clouds (refer to Cloud A and Cloud B), as the server's side, provide the storage and the computation service.

Step 2: User Login-

It is authorized user login where the user uploads data to the cloud database. The two clouds work together to respond each query request from the client/authorized users (availability). For privacy concerns, these two clouds are assumed to be non-colluding with each other, and they will follow the intersection protocols to preserve privacy of data and queries (privacy).

Step 3: System Interface-

In our scheme, the knowledge of stored database and queries is partitioned into two parts, respectively stored in one cloud. The mechanism guarantees that knowing either of these two parts cannot obtain any useful privacy information. To conduct a secure database, data are encrypted and outsourced to be stored in one cloud (Cloud A), and the private keys are stored in the other one (Cloud B). For each query, the corresponding knowledge includes the data contents and the relative processing logic.

Step 4: Security Mechanism-

We proposed to use Blowfish [6] symmetric block cipher algorithm to encrypt block data of 64-bits at a time. It will follow the feistel network and this algorithm is divided into two parts.

1. Key-expansion
2. Data Encryption

VI. CONCLUSION AND FUTURE SCOPE

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. Furthermore, performance evaluation result shows that our proposed architecture are efficient.

To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, we propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability.

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 multi keyword 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] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.