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

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

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: One of the primary usage of cloud computing is data storage. Cloud provides huge capacity of storage for cloud users. To store and retrieve their data at anytime or anywhere it should be reliable and flexible. Currently many enterprises have started using cloud storage due to its advantages, but the problem lay in data security, data privacy and other data protection issues. It is a major setback for security and privacy of data storage in the field of cloud computing. 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. 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. This paper proposes architecture to address the security and privacy issue in cloud storage in order to protect the data stored in the cloud.

KEYWORDS: Database, Range Query, Privacy Preserving, Cloud Computing**.**

I. INTRODUCTION

The growing industry of cloud has provided a service paradigm of storage outsourcing that helps to reduce users' burden of IT infrastructure maintenance, and reduce the cost for both the enterprises and individual users. However, 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 - such as database system - to cloud.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. Therefore the objectives of security protection of the outsourced information to a cloud server are refined by partitioning the sensitive knowledge into two parts and store them in two non-colluding clouds.

Moreover a secure database service architecture is acknowledged by utilizing two non-colluding clouds in which the information learning and query rationale is divided into two clouds. Hence, perceiving just a single cloud can't help uncover private data. Other than a progression of intersection protocols to give numeric related SQL range queries [1] with privacy preservation is additionally executed and it won't uncover order related data to any of the two non-colluding clouds.

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

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

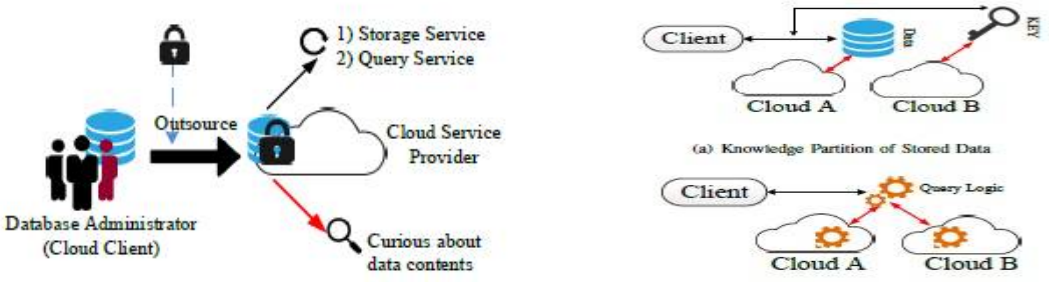


Fig1. Outsource Database and Services

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 [2][4]

X. Wu et al proposed data mining with big data [3] is very challenging task. It is troublesome for present and develop cluster preparing standards to adjust to the quickly developing information volume and the significant continuous prerequisites. Indeed, even part of work has been done on Big Data preparing and mining. The progress in new advancements and their information age at generous rate brought forth the Big Data. Subsequently, it requires a Big Data system to take a shot at the constant information. This structure gives awesome chances to the Data Mining ideal models utilizing Big Data way to deal with diminish the overhead of cost.

J.M. Bofhli et al proposed the Security and privacy-enhancing multi-cloud architectures [1]. This paper works as an summary paper where creators spoke about the security in open cloud and multiple cloud. Also the high potential for security forecasts in cloud computing have been argued. Homomorphic encryption and secure multiparty calculation rules to be remarkably boosting concerning both technical security and supervisory compliance. Though there is no single perfect way to deal with cultivate both security and legal compliance in an applicable way. The confinements of these practices just originate from their constrained applicability and high multifaceted nature being used.

III.EXISTING SOLUTIONS

We firstly give an overview of our existing two-cloud scheme, and then present the detailed interaction protocols to realize range query with privacy preservation on outsourced encrypted database. It becomes a critical issue to put sensitive service into the cloud, so encryption is needed before outsourcing sensitive data. In our proposed system, two clouds (refer to Cloud A and Cloud B, respectively) have been assigned distinct tasks in the database system: Cloud A provides the main storage service and stores the encrypted database. Meanwhile, Cloud B executes the main computation task, to figure out whether each numerical record satisfies the client's query request with its own security key. With the assumption of no collusion between two clouds, the knowledge of application logic can be partitioned into two parts in our proposed scheme, where each one part is only known to one cloud. As we will analyze in this paper, one single part of knowledge cannot reveal privacy of the data and the query.

Motivation:

Privacy is most vital factor in cloud and modern day data storage services. Many creators took a shot at security protection, yet private data can't be fully protected by some technique. Everybody has some private and confidential data that they don't share to any one, similarly all enterprises and organizations have numerous private information, they don't impart the information about this to anybody. If any of the information is leaked the organization's misfortune is sure shot. With the goal that we are turning on protection of the sensitive information. Present day innovation additionally takes a shot at privacy preservation [8] in the cloud servers.

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

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 6, Issue 5, May 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.

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 service. The two clouds (refer to Cloud A and Cloud B), as the server's side, provide the storage and the computation service. Briefly depicts the architecture of our outsourced secure database system in our scheme. 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

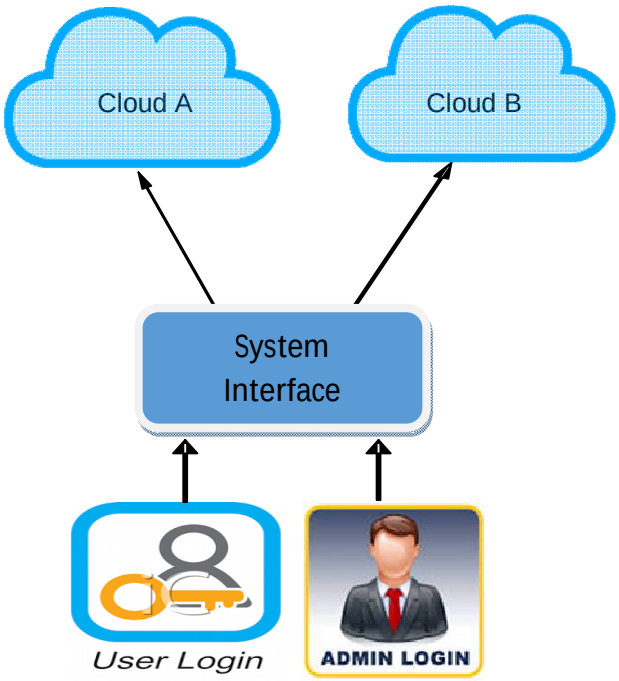


Fig 2. Proposed System Architecture

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

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

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

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.

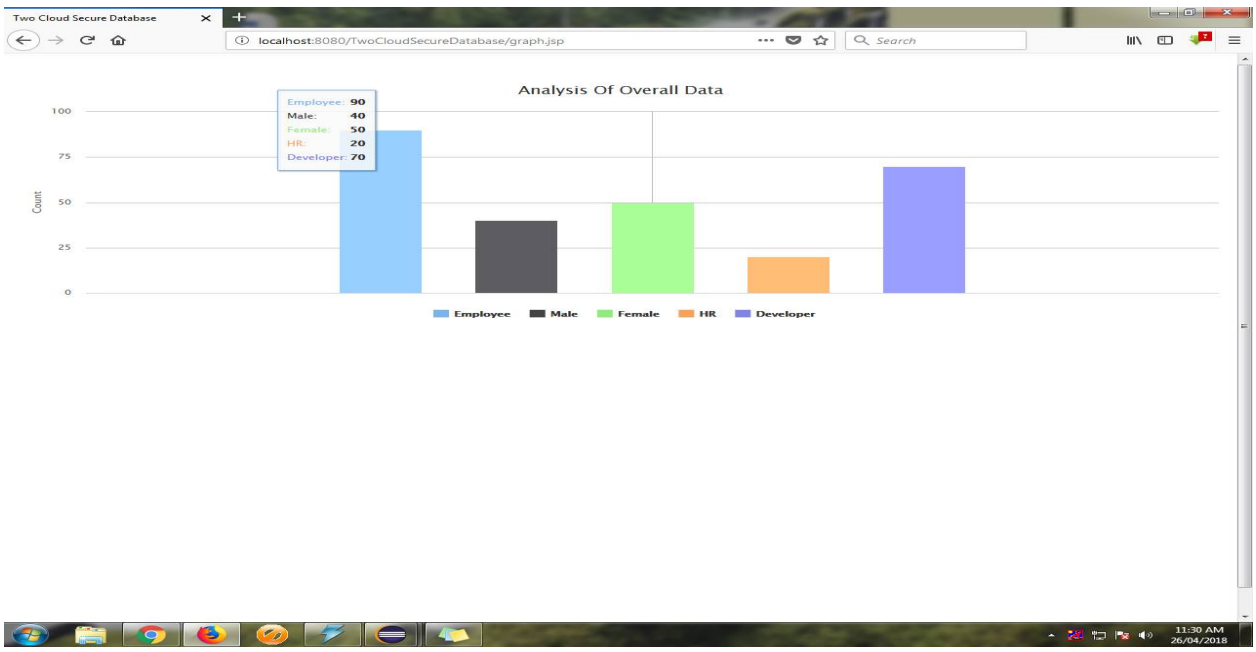
Step 4: Security Mechanism-

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. RESULT AND ANALYSIS

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 service. It analyzes a client's data and produces a following type of results:



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

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 6, Issue 5, May 2018

VII. CONCLUSION AND FUTURE SCOPE

In this paper, we presented 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. 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 architecture can meet the privacy-preservation requirements. Furthermore, performance evaluation result shows that our proposed architecture is 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] Kaiping Xue, Shaohua Li, Jianan Hong, Yingjie Xue, Nenghai Yu, and Peilin Hong "Two-Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving", IEEE Transactions on Information Forensics and Security ,2017

2] 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

3] 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.

4] 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

5] 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.

6]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.

7] 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.

[8] R. A. Popa, F. H. Li, and N. Zeldovich, "An ideal-security protocol for order-preserving encoding," in Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP'13). IEEE, pp. 463–477, 2013.