International Journal of Science Engineering and Advance Technology

Efficient Database Outsource to Twin Cloud With Security and Privacy

[1]P. Ammeswara Rao, [2] V. Aditya Ramalingeswar Rao
[1] Final Master of Science in Computer Science, Ideal college of Arts and Sciences, Vidyut Nagar, Kakinada, East Godavari, AP, India
[2] Associate Professor, Department of Computer Science, Ideal college of Arts and Sciences, Vidyut Nagar, Kakinada, East Godavari, AP, India

ABSTRACT:
Database is held and treated in cloud server, which is outside the control of data owners. For the numerical range query those arrangements cannot deliver adequate confidentiality defense in contradiction of practical challenges, e.g., confidentiality leakage of statistical properties, access design. Also, augmented number of queries will unavoidably leak more info to the cloud server. In this paper, we propose two-cloud building for secure database, with a series of connection protocols that deliver privacy preservation to numerous numeric-related range queries. Safety analysis demonstrates that confidentiality of arithmetical information is muscularly protected against cloud providers in our planned scheme.

KEYWORDS: outsourcing, Cloud, encryption.

1INTRODUCTION:
The increasing manufacturing of cloud has deliver a service model of storage/computation subcontracting helps to lessen users' weight of IT infrastructure care, and lessen the cost for both the creativities and discrete users. Yet, due to the discretion apprehensions that the cloud service wage-earner is supposed semi-trust, it turn out to be a life-threatening issue to put subtle service into the cloud, so encryption or complication are needed before outsourcing sensitive data - such as database system - to cloud .Due to the supposition that cloud provider is honest-but-curious, the cloud strength try his/her best to get private information for his/her own welfares. Even inferior, the cloud could onward such subtle information to the commercial contestants for profit, which is an into lerable working danger.

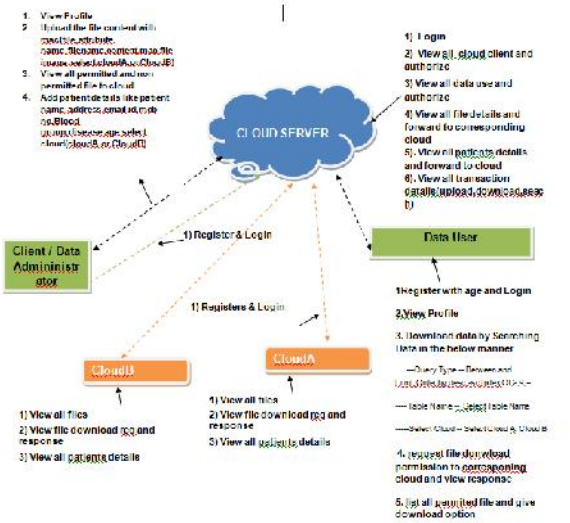
2LITERATURE SURVEY:
2.1we opinion out Catalano-Fiore's VDB outline from vector promise is susceptible to the so-called forward automatic update (FAU) attack. Also, we suggest a new VDB outline from vector pledge based on the knowledge of commitment obligatory. The construction is not only civic demonstrable but also secure under the FAU attack. Besides, we verify that our creation can accomplish the looked-for security goods.

2.2 Seeing the cloud data are lively in nature, the suggested project additional supports safe and well-organized lively operations on subcontracted data, counting block modification, removal, and add. Examination demonstrations the future scheme is extremely well-organized and hardy in contradiction of Byzantine failure, malicious data modification attack, and even server conspiring outs.

3PROBLEM DEFINTION:
From the view of privacy word, here the data not only embrace lastingly stored information but also each brief request request .Moreover and outstandingly, as the hypothesis in some existing works, we shoulder that the two clouds A and B are non-colluding: Cloud A follows the procedure to add obligatory complication to defend privacy against cloud B, so that cloud B cannot get extra secluded information in the communications with Cloud A. No isolated information is transported yonder the scopes of procedures.

4PROPOSED APPROACH:
We first give an impression of our proposed two-cloud scheme, and then present the detailed interaction protocols to understand choice query with privacy preservation on outsourced encrypted database. The anticipated device can reservation the confidentiality of data and query requests in contradiction of each of the two clouds. We present a token based scheme, which can limit the number of items and the variety of columns that Cloud can only course.

5 SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

Potential Threats and Privacy Requirements

It defines the latent threats and the confidentialitynecessities when the folder is subcontracted to civic cloud. The stored data innards and the query processes. Though there are countless data encryption schemes, some fail to runsatisfactoryconcealmentsafeguarding after arithmetical analysis: Recurring and large-amount query progressions not only leak the entree patterns, but also divulge the stored encrypted data with time.

Data contents Module:

Order Preserving Encryption (OPE), which is widely used in making the secure database, with provision of range queries, straightly leaks the arithmeticalinfo in the encryption field. Also, the leak of figure properties is part of the nature of subcontracted cloud database provision: the cloud can absorb the statistical properties by recurrent query needs.

Query pattern Module.

The inquirydesign also coversconfidentiality information, as they can disclose the client's drive of the query. Even inferior, such pattern can seepage some arithmetical properties,.wedeclare that an subcontractedprotected database providing numeric-related queries oughtavoid the succeeding private information from actualitygained by the honest-but-curious clouds.

Privacy of Item Values Modules:

A supremeoutline is required to stylenaught of the arithmetical properties be escaped to the inquiring clouds. But, the secrecy leakage of arithmeticalbelongings in a real-world outsourced folder system is expected, as frequentsubgroup of data rather than cosmos requires knowledge for filtering. For occurrence, if the client requests to repossess a from the outsourced database, a cloud server short of any acquaintance of the order can only coming back all items of the database to the client, which is not functioning.

7TWO CLOUD SCHEME:

INPUT: CLOUD A, CLOUD B, CLIENT, DB ADMIN,QUERY

STEP1: in Table Creation after the client rents the cloud service, he/she will outsource the database application to the cloud.

STEP2: For each column of the table the client randomly selects a symmetric key K, and then use it to encrypt each column name.

STEP3: For each item its values in multiple columns should also be encrypted.

STEP4: In Query Request When the client wants to retrieve some data from the outsourced database, he/she firstly generates a SQL query.

STEP5: The client encrypts the range boundary value a with the public key PK in Pallier Cryptosystem.

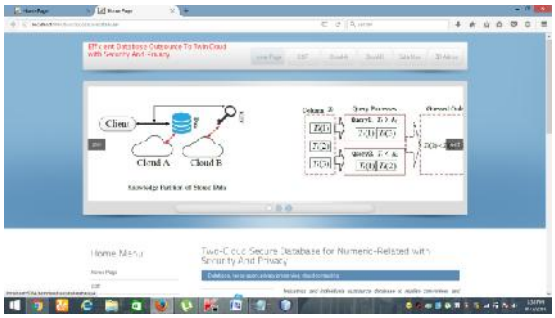
STEP6: In Generate the token. The client analyzes the query request and figures out how many columns are involved. Then, the client generates the corresponding token.sss

STEP7: In tSend the query request Then the client sends the encrypted query request to Cloud A.

STEP8: According to the mapped index j, Cloud A sends the corresponding rows in the table, as the query response, to the client.

STEP9: After receiving the response, the client can decrypt the items with SK to obtain the required data, and removes dummy items that does not satisfy the query predicate.

8RESULTS:



Cloud computing, database, privacy preserving,range query

Outsourced database, serviseand the privacy risk

Two cloud database architecture and knowledge partition prototype

EXTENSION WORK:

We extending the two cloud scheme with SHA-1 algorithm which validate the integrity of cloud database data as well as query .for encryption and decryption of data AES-256 bit algorithm is used to reduce communication overhead.

9CONCLUSION:

Weaccessible a two-cloud stylewith successions of contact protocols for outsourced database service, which certifies the concealment preservation of data contents, numericalchattels and query pattern. At the same time, with the backing of range queries, it not only safeguards the discretion of static data, but also speaksimpendingsolitude leakage in arithmetic properties or after hefty number of query routes. Retreatexamination shows that our arrangement can encounter the privacy-preservation supplies. Furthermore, presentationassessmentconsequence shows that our suggested scheme is well-organized.

10REFERENCES:

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph et al., “A view of cloud computing,” Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, “Toward secure and dependable storage services in cloud computing,” IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

[3] K. Xue and P. Hong, “A dynamic secure group sharing framework in public cloud computing,” IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.

[4] J.W. Rittinghouse and J. F. Ransome, Cloud computing: implementation, management, and security. CRC press, 2016.

[5] D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.

[6] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: architecture, applications, and approaches,” Wireless Communications and Mobile Computing, vol. 13, no. 18, pp. 1587–1611, 2013.

[7] R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, “CryptDB: protecting confidentiality with encrypted query processing,” in Proceedings of the 23rd ACM Symposium on Operating Systems Principles. ACM, 2011, pp. 85–100.

[8] C. Curino, E. P. Jones, R. A. Popa, N. Malviya et al., “Relational cloud: A database-as-a-service for the cloud,” 2011, http://hdl.handle.net/1721. 1/62241.

[9] D. Boneh, D. Gupta, I. Mironov, and A. Sahai, “Hosting services on an untrusted cloud,” in Advances in Cryptology-EUROCRYPT 2015. Springer, 2015, pp. 404–436.

[10] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, “Verifiable computation over large database with incremental updates,” IEEE Transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016.

[11] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, “New publicly verifiable databases with efficient updates,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015.

[12] S. Benabbas, R. Gennaro, and Y. Vahlis, “Verifiable delegation of computation over large datasets,” in Annual Cryptology Conference. Springer, 2011, pp. 111–131.

[13] W. Li, K. Xue, Y. Xue, and J. Hong, “TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage,” IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 5, pp. 1484–1496, 2016.

[14] K. Xue, Y. Xue, J. Hong,W. Li, H. Yue, D. S.Wei, and P. Hong, “RAAC: Robust and auditable access control with multiple attribute authorities for

public cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 953–967, 2017.

[15] R. A. Popa, F. H. Li, and N. Zeldovich, "An ideal-security protocol for order- on Security and Privacy (SP'13). IEEE, 2013, pp. 463–477.

[16]Kaiping Xue[1],Shaohua Li[2],Jianan Hong[3],"Two-Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving"

Pattapagalu Ammeswara Rao is a student of Ideal College of Arts and Science Kakinada. Presently he is in Final Master of Science in Computer Science this college and affiliated to AdikaviNannaya University, Rajamahendravaram, Andhra Pradesh. His area of interest includes Computer Networks and Object-Oriented Programming languages, all current trends and techniques in Computer Science.

VIDIYALA ADITYA RAMALINGESWARA RAO presently working as a Assistant Professor in P.G.Department of Computer Sciences in Ideal college of Arts and Sciences(P.G.Courses) Kakinada. He obtained M.Sc(Computer Science) from Andhra University Vishakapatnam. And he did M.Tech(Computer Science and Engineering) from AacharyaNagarjuna University Guntur. He havelecturership in Computer Science and Applications and have an Experience of 15 years of teaching.