IPHV8I1039X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

IMPROVE THE PERFORMANCE AND PRIVACY IN CLOUD DATA

[#1]**JULURU AJAY KUMAR, M.Tech Student,**

[#2]**V.SUNEETHA, Assistant Professor,**

Dept of CSE,

MALLA REDDY COLLEGE OF ENGINEERING AND TECHNOLOGY, HYD, T.S., INDIA

Abstract: Data perturbation is a popular technique for privacy preserving cloud computing . The main problem in data perturbation is data quality and query privacy, capable query processing and low in house processing cost. In the existing system we face order preserving encryption (OPE) and cryptoindex are vulnerable to the attacks. It is necessary to allow single or multiple keyword in the search and display relevant document. We satisfying these requirements we propose a RASP range query algorithm and kNN-R algorithm. These are using for secure range query access for cloud systems. The RASP method combines OPE and random noise injection and expansion the dimensionality and finally we provide the strong flexibility to attacks on the disturbed information and queries. The RASP allows indexing and efficient query processing. The kNN-R algorithm minimizes in-house processing workload.

Keywords: *cloud, privacy, encryption, kNN-R algorithm, OPE, Secure DBAAS.*

I.INTRODUCTION

Cloud Computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and help the users focus on their core business instead of being impeded by IT obstacles. The main enabling technology for cloud computing is virtualization. Virtualization generalizes the physical infrastructure, which is the most rigid component, and makes it available as a soft component that is easy to use and manage. By doing so, virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure utilization. On the other hand, autonomic computing automates the process through which the user can provision resources on-demand. By minimizing user involvement, automation speeds up the process and reduces the possibility of human errors. Users face difficult business problems every day. Cloud computing adopts concepts from Service-oriented Architecture that can help the user break these problems into services that can be integrated to provide a solution. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained in the domain of SOA to allow global and easy access to cloud services in a standardized way. Cloud computing also leverages concepts from utility computing in order to provide metrics for the services used. Such metrics are at the core of the public cloud pay-per-use models. In addition, measured services are an essential part of the feedback loop in autonomic computing, allowing services to scale on-demand and to perform automatic failure recovery. Cloud computing is a kind of grid computing; it has evolved by addressing the QoS (quality of service) and reliability problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional parallel computing techniques.

II. BACKGROUND ISSUES

Threats and opportunities of the cloud:

Critical voices including GNU project initiator Richard Stallman and Oracle founder Larry Ellison warned that the whole concept is rife with privacy and ownership concerns and constitute merely a fad. However, cloud computing continues to gain steam with 56% of the major European technology decision-makers estimate that the cloud is a priority in 2013 and 2014, and the cloud budget may reach 30% of the overall IT budget.

According to the Tech Insights Report 2013: Cloud Succeeds based on a survey, the cloud implementations generally meets or exceeds expectations across major service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Several deterrents to the

widespread adoption of cloud computing remain. Among them, are: reliability, availability of services and data, security, complexity, costs, regulations and legal issues, performance, migration, reversion, the lack of standards, limited customization and issues of privacy. The cloud offers many strong points: infrastructure flexibility, faster deployment of applications and data, cost control, adaptation of cloud resources to real needs, improved productivity, etc. The early 2010s cloud market is dominated by software and services in SaaS mode and IaaS (infrastructure), especially the private cloud. PaaS and the public cloud are further back.

Privacy:

The increased use of cloud computing services such as Gmail and Google Docs has pressed the issue of privacy concerns of cloud computing services to the utmost importance. The provider of such services lie in a position such that with the greater use of cloud computing services has given access to a plethora of data. This access has the immense risk of data being disclosed either accidentally or deliberately. Privacy advocates have criticized the cloud model for giving hosting companies' greater ease to control—and thus, to monitor at will—communication between host company and end user, and access user data (with or without permission). Instances such as the secret NSA program, working with AT&T, and Verizon, which recorded over 10 million telephone calls between American citizens, causes uncertainty among privacy advocates, and the greater powers it gives to telecommunication companies to monitor user activity. A cloud service provider (CSP) can complicate data privacy because of the extent of virtualization (virtual machines) and cloud storage used to implement cloud service. CSP operations, customer or tenant data may not remain on the same system, or in the same data center or even within the same provider's cloud; this can lead to legal concerns over jurisdiction. While there have been efforts (such as US-EU Safe Harbor) to "harmonies" the legal environment, providers such as Amazon still cater to major markets (typically to the United States and the European Union) by deploying local infrastructure and allowing customers to select "availability zones." Cloud computing poses privacy concerns because the service provider can access the data that is on the cloud at any time. It could accidentally or deliberately alter or even delete information. This becomes a major concern as these service providers, who employ administrators which can leave room for potential unwanted disclosure of information on the cloud.

Privacy solutions:

Solutions to privacy in cloud computing include policy and legislation as well as end users' choices for how data is stored. The cloud service provider needs to establish clear and relevant policies that describe how the data of each cloud user will be accessed and used. Cloud service users can encrypt data that is processed or stored within the cloud to prevent unauthorized access

Security:

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of "applied security" and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security. The relative security of cloud computing services is a contentious issue that may be delaying its adoption. Physical control of the Private Cloud equipment is more secure than having the equipment off site and under someone else's control. Physical control and the ability to visually inspect data links and access ports is required in order to ensure data links are not compromised. Issues barring the adoption of cloud computing are due in large part to the private and public sectors' unease surrounding the external management of security-based services. It is the very nature of cloud computing-based services, private or public, that promote external management of provided services. This delivers great incentive to cloud computing service providers to prioritize building and maintaining strong management of secure services. Security issues have been categorized into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. Solutions to various cloud security issues vary, from cryptography, particularly public key infrastructure (PKI), to use of multiple cloud providers, standardization of APIs, and improving virtual machine support and legal support.

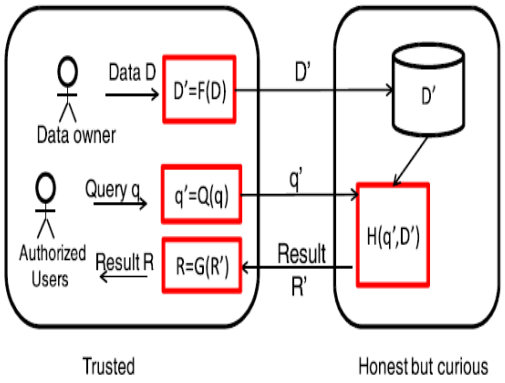
Cloud computing offers many benefits, but is vulnerable to threats. As cloud computing uses increase, it is likely that more criminals find new ways to exploit system vulnerabilities. Many underlying challenges and risks in cloud

IPHV8I1039X
International Journal Of Advanced Research and Innovation -Vol.8, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

computing increase the threat of data compromise. To mitigate the threat, cloud computing stakeholders should invest heavily in risk assessment to ensure that the system encrypts to protect data, establishes trusted foundation to secure the platform and infrastructure, and builds higher assurance into auditing to strengthen compliance. Security concerns must be addressed to maintain trust in cloud computing technology.

Existing System: In the existing method, the data protection in the cloud data is Network-based services, which appear to be provided by real server hardware and are in fact served up by virtual hardware simulated by software running on one or more real machines, Such virtual servers do not physically exist and can therefore be moved around and scaled up or down on the fly without affecting the end user, somewhat like a cloud becoming larger or smaller without being a physical object. The crypto indexing method is used in the existing , it is used to find the attacks on the data, OPE(Order Preserving Encryption) is used to detect the fault node or attack types on the data. Query services are slow for responding the optimized problems.

Proposed System: Identification of trusted user, non-trusted user is difficult in database content types. Here we propose a novel method random space perturbation (RASP) data perturbation method to provide secure and efficient range query and kNN query services for protected data in the cloud. The RASP data perturbation method combines order preserving encryption, dimensionality expansion, random noise injection, and random projection, to provide strong resilience to attacks on the perturbed data and queries. The encryption technique may varies the users side, the RASP specifies the randomized key sets to allocate the key for data. We can analyze the attacks on data and quires on data requests.RSAP provides the multi range secure transmission.



System architecture

In cloud environments, the cost of guaranteeing a certain consistency level on top of replicated data is to be considered. Strong consistency is costly; on the other hand, weak consistency is cheaper, but may lead to high operational costs of compensating the effects of anomalies and access to stale data. The first generation cloud DBMS's provide on the weak consistency in order to provide maximum scalability and availability. It is sufficient for satisfying requirements related to consistency of simple cloud applications. However, more sophisticated like web shops, online stores and credit card services requires strong consistency levels. The advantages of cloud such as availability and scalability are not yet exploited by existing commercial and open source DBMS's which provide strong consistency [12]. SO-1SR (self-optimizing 1SR) is a novel protocol for replicated data in a cloud that dynamically optimize all phases of transaction executions. System model of SO-1SR assumes that applications are built on the top of a cloud data environment.

III. DISTRIBUTED AND CONCURRENT ACCESS TO ENCRYPTED CLOUD DATABASES

In a cloud context, where critical information is placed in infrastructures of untrusted third parties, ensuring data confidentiality is of paramount importance [1], [2]. This requirement imposes clear data management choices: original plain data must be accessible only by trusted parties that do not include cloud providers, intermediaries, and Internet; in any untrusted context, data must be encrypted. Satisfying these goals has different levels of complexity depending on the type of cloud service. There are several solutions ensuring confidentiality for the storage as a service paradigm while guaranteeing confidentiality in the database as a service (DBaaS) paradigm is still an open research area. In this context, we propose SecureDBaaS as the first 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.

The architecture design was motivated by a threefold goal: to allow multiple, independent, and geographically distributed clients to execute concurrent operations on encrypted data, 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. The possibility of combining availability, elasticity, and scalability of a typical cloud DBaaS with data confidentiality is demonstrated through a prototype of Secure DBaaS that supports the

execution of concurrent and independent operations to the remote encrypted database from many geographically distributed clients as in any unencrypted DBaaS setup. To achieve these goals, Secure DBaaS integrates existing cryptographic schemes, isolation mechanisms, and novel strategies for management of encrypted metadata on the un trusted cloud database. This paper contains a theoretical discussion about solutions for data consistency issues due to concurrent and independent client accesses to encrypted data. In this context, we cannot apply fully homomorphic encryption schemes because of their excessive computational complexity. The SecureDBaaS architecture is tailored to cloud platforms and does not introduce any intermediary proxy or broker server between the client and the cloud provider. Eliminating any trusted intermediate server allows SecureDBaaS to achieve the same availability, reliability, and elasticity levels of a cloud DBaaS. Other proposals based on intermediate server(s) were considered impracticable for a cloudbased solution because any proxy represents a single point of failure and a system bottleneck that limits the main benefits of a database service deployed on a cloud platform. Unlike SecureDBaaS, architectures relying on a trusted intermediate proxy do not support the most typical cloud scenario where geographically dispersed clients can concurrently issue read/write operations and data structure modifications to a cloud database. A large set of experiments based on real cloud platforms demonstrate that SecureDBaaS is immediately applicable to any DBMS because it requires no modification to the cloud database services. Other studies where the proposed architecture is subject to the TPC-C standard benchmark for different numbers of clients and network latencies show that the performance of concurrent read and write operations not modifying the SecureDBaaS database structure is comparable to that of unencrypted cloud database. Workloads including modifications to the database structure are also supported by SecureDBaaS, but at the price of overheads that seem acceptable to achieve the desired level of data confidentiality. The motivation of these results is that network latencies, which are typical of cloud scenarios, tend to mask the performance costs of data encryption on response time. The overall conclusions of this paper are important because for the first time they demonstrate the applicability of encryption to cloud database services in terms of feasibility and performance.

IV. SECURE DBAAS

Secure DBaaS is designed to allow multiple and independent clients to connect directly to the untrusted cloud DBaaS without any intermediate server. We assume that a tenant organization acquires a cloud database service from an untrusted DBaaS provider. The tenant then deploys one or more machines and installs a Secure DBaaS client on each of them. This client allows a user to connect to the cloud DBaaS to administer it, to read and write data, and even to create and modify the database tables after creation. We assume the same security model that is commonly adopted where tenant users are trusted, the network is untrusted and the cloud provider is honest-but-curious, cloud service operations are executed correctly, but tenant information confidentiality risk. The information managed by SecureDBaaS includes plaintext data, encrypted data, metadata, and encrypted metadata. Plaintext data consist of information that a tenant wants to store and process remotely in the cloud DBaaS. To prevent an untrusted cloud provider from violating confidentiality of tenant data stored in plain form, SecureDBaaS adopts multiple cryptographic techniques to transform plaintext data into encrypted tenant data and encrypted tenant data structures because even the names of the tables and of their columns must be encrypted. SecureDBaaS clients produce also a set of metadata consisting of information required to encrypt decrypt data as well as other administration information. Even metadata are encrypted and stored in the cloud DBaaS. SecureDBaaS moves away from existing architectures that store just tenant data in the cloud database, and save metadata in the client machine or split metadata between the cloud database and a trusted proxy. When considering scenarios where multiple clients can access the same database concurrently previous solutions are quite inefficient. Solutions based on a trusted proxy are more feasible, but they introduce a system bottleneck that reduces availability, elasticity and scalability of cloud database services. SecureDBaaS proposes a different approach where all data and metadata are stored in the cloud database. SecureDBaaS clients can retrieve the necessary metadata from the untrusted database through SQL statements, so that multiple instances of the SecureDBaaS client can access to the untrusted cloud database independently with the guarantee of the same availability and scalability properties of typical cloud DBaaS. Encryption strategies for tenant data and innovative solutions for metadata management and storage are described.

4.1 Sequential SQL Operations

We describe the SQL operations in SecureDBaaS by considering an initial simple scenario in which we assume that the cloud database is accessed by one client. Our goal here is to highlight the main processing steps; we do not take into

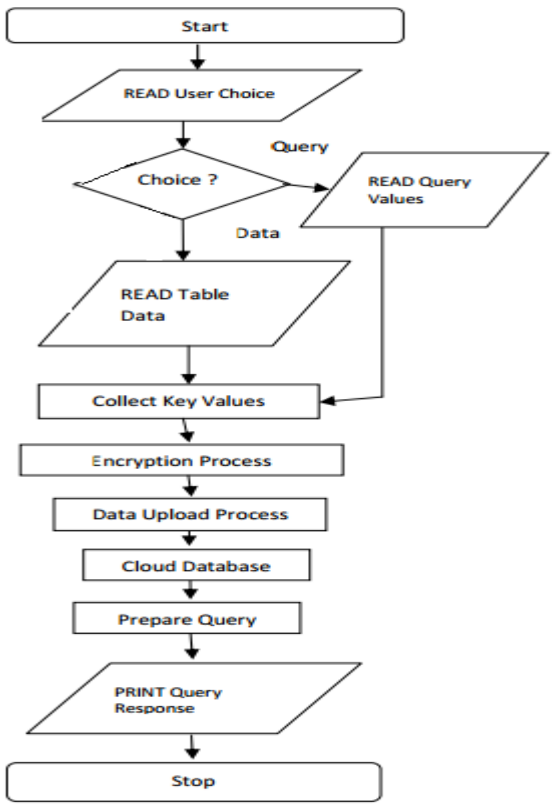
account performance optimizations and concurrency. The first connection of the client with the cloud DBaaS is for authentication purposes. SecureDBaaS relies on standard authentication and authorization mechanisms provided by the original DBMS server. After the authentication, a user interacts with the cloud database through the SecureDBaaS client. SecureDBaaS analyzes the original operation to identify which tables are involved and to retrieve their metadata from the cloud database. The metadata are decrypted through the master key and their information is used to translate the original plain SQL into a query that operates on the encrypted database. Translated operations are then executed by the cloud database over the encrypted tenant data. As there is a one-to-one correspondence between plaintext tables and encrypted tables, it is possible to privileges on some tables. User privileges can be managed directly by the untrusted and encrypted cloud database. The results of the translated query that includes encrypted tenant data and metadata are received by the SecureDBaaS client, decrypted and delivered to the user. The complexity of the translation process depends on the type of SQL statement.

4.2 Concurrent SQL Operations

The support to concurrent execution of SQL statements issued by multiple independent clients is one of the most important benefits of SecureDBaaS with respect to state-of-the-art solutions. Our architecture must guarantee consistency among encrypted tenant data and encrypted metadata because corrupted or out-of-date metadata would prevent clients from decoding encrypted tenant data resulting in permanent data losses. A thorough analysis of the possible issues and solutions related to concurrent SQL operations on encrypted tenant data available in the online supplemental material. Here, we remark the importance of distinguishing two classes of statements that are supported by SecureDBaaS: SQL operations not causing modifications to the database structure, such as read, write, and update; operations involving alterations of the database structure through creation, removal and modification of database tables. In scenarios characterized by a static database structure, Secure DBaaS allows clients to issue concurrent SQL commands to the encrypted cloud database without introducing any new consistency issues with respect to unencrypted databases. After metadata retrieval, a plaintext SQL command is translated into one SQL command operating on encrypted tenant data. As metadata do not change, a client can read them once and cache them for further uses, thus improving performance. SecureDBaaS is the first architecture that allows concurrent and consistent accesses even when there are operations that can modify the database structure. In such cases, we have to guarantee the consistency of data and metadata through isolation levels, such as the snapshot isolation that we demonstrate can work for most usage scenarios.

V. SYNCHRONIZED ENCRYPTED DATABASE MANAGEMENT METHOD FOR CLOUDS

The Secure DBaaS framework is enhanced to support concurrent database structure modification scheme with minimum overhead. Digital signature based data integrity verification mechanism is integrated with the system. Encrypted query submission model is used to secure the query values. Access control mechanism is used to allow users to grant permissions for other users. Cloud database security scheme is enhanced with data verification mechanism. Access privilege management scheme is integrated with the system. Encrypted query processing is used to secure the user query values. The system is divided into six major modules. They are cloud database, key management, data upload process, privilege management, query processing and database reconstruction.



The cloud database module is designed to manage client data values. Key distribution process is handled under key management module. Table creation and update operations are carried out under the data upload process. User access permissions are assigned under the privilege management module. Query processing module is designed to execute encrypted queries in the cloud database. Database structure modifications are performed under the database reconstruction module.

5.1 Cloud Database

User accounts are created and maintained under the cloud database. The system separately manages the user data and meta data values. Data values are stored in encrypted format. Query processing is performed under the cloud database environment.

5.2 Key Management

The key management process is used to maintain the key values. Multiple Crypto System (MCS) is used for the key management process. Separate key values are used for user data and meta data. Cloud database issues the key value to secure the query submission process.

5.3 Data Upload Process

Client application is used for the data upload process. Database tables are created and maintained in the data upload process. Meta data and records are encrypted before the upload process. Encrypted table data values are stored in the user storage area under the cloud database.

5.4 Privilege Management

User access permissions are assigned in the privilege management process. Privileges are assigned for the tables. Insert, delete, update and select permissions are used in the data sharing process. Re-encryption process is applied in the data sharing process.

5.5 Query Processing

Data download operations are carried out using query submission process. Encrypted query values are submitted to the cloud database. Cloud database prepare the query response and transfer to the client. Response data values are decrypted using the client secret key.

5.6 Database Reconstruction

Database tables are modified in the database reconstruction process. Column addition and deletion operations are supported in the reconstruction process. Concurrent user access is allowed in the database. Table data values are reassigned in the database manipulation process.

VI. CONCLUSION

Cloud database services are integrated with data confidentiality and concurrent access models. Secure database as a service (Secure DBaaS) Framework is used to manage data access in encrypted cloud databases. The Secure DBaaS scheme is enhanced with data integrity features. Concurrent database structure modification and query security tasks are improved with security methods. The system eliminates the intermediate proxies in database management process. Database structure modification mechanism is adopted for multi user environment. The system improves the availability and scalability features. The response time in query processing is reduced by the system.

REFERENCES

[1] M.Armbrust et al.,"A View of Cloud Computing," Comm. of the ACM, pp. 50-58, 2010.

[2] W.Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Technical Report Special Publication 800-144,NIST, 2011.

[3] A.J. Feldman and E.W. Felten, "SPORC: Group Collaboration Using Untrusted Cloud Resources," Proc. Ninth USENIX Conf. Operating Systems Design and Implementation, Oct. 2010.

[4] V. Ganapathy and R. Motwani, "Distributing Data for Secure Database Services," Proc. Fourth ACM Int'l Workshop Privacy and Anonymity in the Information Soc., Mar. 2011.

[5] P. Mahajan and M. Walfish, "Depot: Cloud Storage with Minimal Trust," ACM Trans. Computer Systems, vol. 29, no. 4, article 12, 2011.

[6] "Oracle Advanced Security," Oracle Corpo ration,http://www.oracle.com/technetwork/data base /options/advanced-security, Apr. 2013.

[7] A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felten, "SPORC: Group Collaboration Using Untrusted Cloud Resources," Proc. Ninth USENIX Conf. Operating Systems Design and Implementation, Oct. 2010.

[8] Ferretti, Luca, et al. "Security and confidentiality solutions for public cloud database services." SECURWARE 2013, The Seventh International Conference on Emerging Security Information, Systems and Technologies. 2013.

[9] Ferretti, Luca, Michele Colajanni, and Mirco Marchetti. "Access control enforcement on query-aware encrypted cloud databases." Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on. Vol. 2. IEEE, 2013.

[10 Ferretti, Luca, Michele Colajanni, and Mirco Marchetti. "Supporting security and consistency for clouddatabase." Cyberspace Safety and Security. Springer Berlin Heidelberg, 2012. 179-193.

[11] Dr. M. Newlin Rajkumar, Brighty Batley C, Dr.V.Venkatesakumar, Ancy George, Scholar, P. G., and P. G. Scholar. "Survey on the Concurrency Control Protocols for Encrypted Cloud Databases."

[12] S.M. Hema Latha , S.Ganesh, "A Brief Survey on Encryption Schemes in Cloud Environments"-2013.

[13] Pathak, Ajeet Ram, and B. Padmavathi. "Survey of Confidentiality and Integrity in Outsourced Databases."

[14] Khan, Abdul Wahid, et al. "A Literature Survey on Data Privacy/Protection Issues and Challenges in Cloud Computing." IOSR Journal of Computer Engineering (IOSRJCE) ISSN (2012): 2278-0661.