International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Review Article

Supporting Security and Consistency for Distributed, Concurrent Access to Cloud Databases: A Review

Shrikant Kale[Á*] and Nitin R. Chopde [Á]

[Á]Department of Computer Science & Engineering, G. H. Raisoni College of Engg & Management Amravati, Maharashtra, India

Accepted 15 Nov 2014, Available online 01 Dec 2014, **Vol.4, No.6 (Dec 2014)**

Abstract

A cloud storage system consists of a group of storage servers over the web. The most aim is to produce secure storage services in a very cloud storage system. There square measure many totally different techniques were exist for storage services, whereas providing an information confidentiality solutions for the information as a service paradigm square measure still in operating and isn't completed still. We tend to propose a unique design that integrates cloud information services with knowledge confidentiality and therefore the risk of corporal punishment synchronic operations on encrypted knowledge. Coding schemes square measure wont to give knowledge confidentiality, knowledge hardiness and practicality. We tend to use associate coding knowledge and Key verification for implementing for knowledge secure storage. The planned design has the additional advantage of eliminating intermediate proxies that limit the physical property, accessibility, and measurability properties that square measure intrinsic in cloud-based solutions. We tend to propose associate design for higher security and confidentiality of an information hold on within the cloud databases. The efficaciousness of the planned design is evaluated through theoretical analyses and intensive experimental results supported a paradigm implementation subject to the TPC-C customary benchmark for various numbers of shoppers within the network. Coding schemes square measure wont to give knowledge confidentiality, knowledge hardiness and practicality. We tend to use associate coding knowledge and Key verification for implementing for knowledge secure storage.

Keywords: *Cloud, security, confidentiality, SecureDBaaS, database*

Introduction

Cloud computing is a new computing paradigm that is engineered on virtualization, parallel and distributed computing, utility computing, and service-oriented design. within the last many years, cloud computing has emerged mutually of the foremost potent paradigms within the IT business, Cloud computing may be a thought that treats the resources on the web as a unified entity, a cloud. Users simply use services while not worrying regarding however computation is completed and storage is managed. It focuses on coming up with cloud storage for hardiness, confidentiality, and functionality. The cloud storage system is taken into account as an outsized scale distributed storage system that consists of the many freelance storage servers. Knowledge hardiness may be a major demand for storage systems. a method to produce knowledge hardiness is to duplicate a message specified every storage server stores a replica of the message. A Cloud direction system (CDBMS) may be a distributed information that delivers computing as a service rather than a product. It's the sharing of resources, software, and knowledge between multiply devices over a network that is generally the web. It's expected that this range can grow considerably within the future. Associate example of this is computer code as a Service, or SaaS, that is associate application that's delivered through the browser to customers. Cloud applications connect with a information that's being run on the cloud and have variable degrees of potency. Some square measure manually designed, some square measure preconfigured, and a few square measure native. Native cloud databases square measure historically higher equipped and additional stable that those who square measure changed to adapt to the cloud.

Cloud Computing has been visualized because the next-generation design of IT Enterprise. In cloud computing application computer code and knowledge bases square measure moving to the centralized massive data centers. This mechanism brings regarding several new challenges, that haven't been well understood. Security and privacy considerations, however, square measure among the highest considerations standing within the method of wider adoption of cloud. In cloud computing the most concern is to produce the safety to finish user to safeguard files or knowledge from unauthorized user. Security is that the main intention of any technology through that unauthorized trespasser cannot access your file or knowledge in cloud. we've got styled one planned design and design which will facilitate to write and rewrite the file at the user facet that give security to knowledge at rest yet as whereas moving.

*Corresponding author: **Shrikant Kale**

Cloud computing is currently days rising field as a result of its performance, high accessibility, low cost. Within the cloud several services square measure provided to the shopper by cloud. Knowledge store is main future that cloud service provides to the businesses to store immense quantity of storage capability. however still several firms don't seem to be able to implement cloud computing technology attributable to lack of correct security management policy and weakness in protection that cause several challenge in cloud computing.

Cloud computing is web primarily based computing wherever virtual shared servers give computer code, infrastructure, platform, devices and different resources and hosting to computers on a pay-as-you-use basis. Users will access these services offered on the "internet cloud" while not having any previous information on managing the resources concerned. Thus, users will concentrate additional on the core business processes instead of outlay time on gaining information on resources required to manage their business processes. Attributable to its low value, robustness, flexibility and omnipresent nature, cloud computing is ever-changing the method entities manage their knowledge. However, various privacy concerns arise whenever potentially sensitive data is outsourced to the cloud. The planned theme prevents the cloud server from learning any probably sensitive plaintext within the outsourced databases. It also allows the database owner to delegate users to conducting content-level fine-grained private search and decryption. Moreover, our theme supports non-public questioning whereby neither the information owner nor the cloud server learns query details.

Literature Survey

Most package or direction systems square measure merely computer code packages that users will acquire to make, maintain or use a information. However, since the introduction of cloud computing, package has morphed into a completely new kind of service with its own distinctive edges and task specific benefits. For one factor, any kind of cloud service model can get to use an avid cloud package so as to really give customers with glorious access to knowledge and databases. Ancient DBMS's square measure merely not got wind of or equipped to handle the strain of cloud computing. And after all, if DBMS was deployed as a service as a part of a bigger package provided, it might doubtless be way more economical in its duties and thus cheaper within the long-standing time. All DBMS, despite whether or not ancient or cloud-based, square measure basically communicators that operates as middlemen between the OS and therefore the information. However, may be a cloud package totally different a standard one? For one factor, cloud-based package square measure extraordinarily scalable. They're ready to handle volumes of knowledge and processes that will exhaust a typical package. Despite their measurability but, cloud package square measure still somewhat lacking within their ability to proportion to extraordinarily massive processes; this can be expected to be remedied in the returning months and years but. Currently, the utilization of cloud DBMS's square measure in the main employed in the testing and development of latest cloud applications and processes. However, whereas a complete package is used on a cloud infrastructure.

The SecureDBaaS design is customized to cloud platforms and doesn't introduce any negotiator proxy or broker server between the shopper and therefore the cloud supplier. Eliminating any sure intermediate server permits SecureDBaaS to attain an equivalent accessibility, responsibility, and physical property levels of a cloud DBaaS. Different proposals supported intermediate server(s) were thought of unfeasible for a cloud-based answer as a result of any proxy represents one purpose of failure and a system bottleneck that limits the most edges (e.g., measurability, accessibility, and elasticity) of a information service deployed on a cloud platform. in contrast to SecureDBaaS, architectures relying on a sure intermediate proxy do not support the most typical cloud state of affairs wherever geographically distributed shoppers will at the same time issue read/write operations and knowledge structure modifications to a cloud information.

Luca ferretti, Michele Colajanni and small Marchetti proposes 'Distributed, synchronic and freelance Access to Encrypted Cloud Databases' in which they propose a unique design that integrates cloud information services with knowledge confidentiality and therefore the risk of corporal punishment synchronic operations on encrypted knowledge. The planned design has the additional advantage of eliminating intermediate proxies that limit the physical property, accessibility, and scalability properties that are intrinsic in cloud-based solutions (Luca Ferretti, Michele Colajanni, and Mirco Marchetti, 2014).

Mohit Marwaha, Rajeev Bedi proposes 'Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing' Objective of their System is to develop a system that may give Security and Privacy to Cloud Storage. Also Establish associate coding primarily based System for shielding Sensitive knowledge on the cloud and Structure however owner and storage Service supplier to work on encrypted knowledge (Mohit Marwaha, Rajeev Bedi, 2013).

Akshar Kaul proposes 'Query process in Encrypted Cloud Databases'. In this work we tend to gift PhantomDB, that may be a new framework for resolution this downside. PhantomDB maintains knowledge security by encrypting the info before storing it on the server (Akshar Kaul,2013).

Deepanchakaravarthi Purushothaman and Dr. Sunitha Abburu proposes 'An Approach for knowledge Storage Security in Cloud Computing'. the most objectives of this paper square measure to stop knowledge access from unauthorized access, it propose a distributed theme to give security of the detain cloud .This could be achieved by victimization similarity token with distributed verification of erasure-coded knowledge. Also planned theme dead stores the knowledge and identifies the any tamper at the cloud server (Deepanchakaravarthi Purushothaman and Dr. Sunitha Abburu,2012).

Maha TEBAA, Saïd EL Hajji, Abdellatif EL GHAZI proposes 'Homomorphic Encryption Applied to the Cloud Computing Security' in which they square measure

proposing associate application of a technique to execute operations on encrypted knowledge while not decrypting them which can give North American country with an equivalent results once calculations as if we've got worked directly on the data(Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI,2012).

Simarjeet Kaur proposes 'Cryptography and coding In Cloud Computing' explores numerous {data coding|encoding|encryption} techniques like homophormic encryption, searchable and structured coding, Identity primarily based coding, signature primarily based coding etc(Simarjeet Kaur,2012).

Sanjoli Singla, Jasmeet Singh proposes 'Cloud Data Security using Authentication and Encryption Technique' in this research paper, we've got used the Rijndael Encryption Algorithm together with EAP-CHAP(Sanjoli Singla, Jasmeet Singh,2013).

Indu Arora and Dr. Anu Gupta proposes 'Cloud Databases: A Paradigm Shift in Databases' The goal of this paper is to review the state of the art within the cloud databases and numerous architectures. It additional assesses the challenges to develop cloud databases that meet the user needs and discusses popularly used Cloud databases(Indu Arora and Dr. Anu Gupta, 2012).

Francesco Pagano and Davide Pagano proposes 'Using In-Memory Encrypted Databases on the Cloud' They focus on implementation and benchmarking of a check system, that shows that our straightforward nonetheless effective answer overcomes most of the issues (Francesco Pagano, Davide Pagano,2011).

Yu *et al*. bestowed a scalable and fine-grained knowledge access management theme in cloud computing supported the KP-ABE technique. The knowledge owner uses a random key to write a file, wherever the random secret's additional encrypted with a collection of attributes victimization KP-ABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, specified a user will solely rewrite a cipher text if and providing the info file attributes satisfy the access structure. Also said that to reach user revocation, the manager delegate's tasks of knowledge file re coding and user secret key update to cloud servers.

Objectives

All presently offered cloud package area unit comparatively new. SQL azure, the sole fully relational package offered, began full production at the start of 2012 and still has some size limitations; Microsoft plans to cut back, and eventually elevate, these restrictions

Today, package as a cloud service area unit used primarily for development and testing of applications-wherever information sizes area unit tiny and problems with security and collocation with multiple users don\'t seem to be concern. One huge blessings of cloud package is their elasticity: the additional you employ, the additional you pay; the less you employ, the less you pay. Initially, cloud DBMSs can have a control for vendors needing a less expensive platform for development. As cloud infrastructure with DBMSs gains maturity particularly in quantifiability, dependableness and security, cloud implementations used for short projects such as tiny division applications and fast development platforms can show marked price reductions compared with implementations at intervals the IT department. This blessings strengthened by the power to line up a cloud package surroundings while not the utilization of costly IT personnel.

The speed of setup are a primary driver to fast preparation of systems while not the standard needs and coming up with necessary for IT comes at intervals the IT department. this may conjointly cut back the requirement for IT to retort to short notice and short length comes, reducing overall prices in IT. knowledge management applications area unit potential candidates for preparation within the cloud.

Conclusion

We propose associate innovative design that guarantees confidentiality of knowledge keep publicly cloud databases. in contrast to progressive approaches, our answer doesn\'t accept associate intermediate proxy that we tend to think about one purpose of failure and a bottleneck limiting availableness and quantifiability of typical cloud information services. an oversized a part of the analysis includes solutions to support synchronous SQL operations (including statements modifying the information structure) on encrypted information issued by heterogeneous and presumably geographically spread shoppers.

It is value observant that experimental results supported the TPC-C customary benchmark show that the performance impact of knowledge coding on interval becomes negligible as a result of it\'s cloaked by network latencies that square measure typical of cloud eventualities. specially, synchronous browse and write operations that don\'t modify the structure of the encrypted information cause negligible overhead. Dynamic eventualities characterized by (possibly) synchronous modifications of the information structure square measure supported, however at the worth of high machine prices. These performance results open the house to future enhancements that we tend to square measure work.

References

Luca Ferretti, Michele Colajanni, and Mirco Marchetti(2014), Distributed, Concurrent ,and Independent Access to Encrypted Cloud Databases, IEEE Transactions on Parallel And Distributed Systems, Vol. 25, No. 2.

Mohit Marwaha, Rajeev Bedi(2013), Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, ISSN (Print): 1694-0784 | ISSN (Online): 1694-0

Akshar Kaul(2013), Query Processing in Encrypted Cloud Databases, A Project Report Submitted in partial fulfillment of the requirements for the Degree of Master of Engineering In Computer Science and Enginee

Deepanchakaravarthi Purushothaman and Dr.Sunitha Abburu(2012), An Approach for Data Storage Security in Cloud Computing, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, ISSN (Online): 1694-0814

Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI(2012), Homomorphic Encryption Applied to the Cloud Computing

Security, Proceedings of the World Congress on Engineering, Vol I WCE 2012, July 4 - 6, 2012, London, U.K

Simarjeet Kaur(2012), Cryptography and Encryption In Cloud Computing", VSRD-IJCSIT, Vol. 2 (3),242-24

Sanjoli Singla, Jasmeet Singh(2013), Cloud Data Security using Authentication and Encryption Technique, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue .

Indu Arora and Dr. Anu Gupta(2012), Cloud Databases: A Paradigm Shift in Databases, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3 ISSN (Online): 1694-081

Francesco Pagano, Davide Pagano(2011), Using In-Memory Encrypted Databases on the Cloud, IEEE 978-1-4577-1186-2/11

H. Hacigu¨mu¨ s¸, B. Iyer, and S. Mehrotra(2002), Providing Database as aService, Proc. 18thIEEE Int'l Conf. Data Eng., Feb. 2002.

C. Gentry(2009), Fully Homomorphic Encryption Using Ideal Lattices,Proc.41st Ann. ACM Symp. Theory of Computi

R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan(2011), CryptDB: Protecting Confidentiality with Encrypted QueryProcessing, Proc. 23rd ACM Symp. Operating Systems Principl

H. Hacigu¨mu¨ s¸, B. Iyer, C. Li, and S. Mehrotra(2002), ExecutingSQL over Encrypted Data in the Database-Service-ProviderModel, Proc. ACM SIGMOD Int'l Conf. Management Da

J. Li and E. Omiecinski(2005), Efficiency and Security Trade-Off inSupporting Range Queries on Encrypted Databases, Proc. 19thAnn. IFIP WG 11.3 Working Conf. Data and Applications Security

E. Mykletun and G. Tsudik(2006), Aggregation Queries in theDatabase-as-a-Service Model, Proc. 20th Ann. IFIP WG 11.3Working Conf. Data and Applications Security.