



An Approach for Security of Cloud Databases and Accessing Data using Data Mining

¹Shrikant P. Kale, ²Prof. Nitin R. Chopde

¹M.E Scholar (Computer Science & Engg), GHRCEM Amravati, Maharashtra, India

²HOD, Dept. of CSE, GHRCEM Amravati, Maharashtra, India

ABSTRACT: A cloud storage system consists of a bunch of storage servers over the online. The foremost aim is to supply secure storage services over cloud storage system. There are several completely different techniques were exist for storage services, whereas providing Associate in Nursing data confidentiality solutions for the knowledge as a service paradigm unit of measurement still in operation and is not completed still. Placing essential knowledge within the hands of a cloud supplier ought to associate with the guarantee of security and convenience for storing data. We tend to propose a completely unique design that integrates cloud info services with knowledge confidentiality and the chance of capital punishment synchronic operations on encrypted data. This is often the primary answer at the bottom of geologically distributed customers to attach on to Associate in Nursing encrypted cloud info, and to execute synchronic and irregular operations collectively with those modifying the info structure. The projected design has the more improvement of eliminating midway proxies that bound the elasticity, availability, and scalability properties that area unit intrinsic in cloud-based solutions. The effectuality of the projected design is evaluated all the way through notional analyses and in depth experimental results supported a image achievement subject to the TPC-C regular benchmark for a range of numbers of clients and network latencies.

KEYWORDS—Cloud, security, confidentiality, SecureDBaaS, database

I. INTRODUCTION

Cloud computing could be a new computing typical that's engineered on virtualization, parallel and distributed computing, utility computing, and service-oriented design. within the last variety of years, cloud computing has emerged mutually of the foremost important paradigms within the IT trade, Cloud computing could be a idea that treats the resources on the net as a unified entity, a cloud. Users simply utilize services while not being troubled concerning however computation is completed and storage is managed. It focuses on scheming cloud storage for strength, confidentiality, and practicality. The cloud storage system is taken into consideration as AN immense scale circulated storage system that consists of the various independent storage servers. information strength might be a significant demand for storage systems. a way to produce information strength is to replacement a message given each storage server stores a replicate of the which means A Cloud administration system might be a circulated data that delivers computing as a service instead of a product. it's the distribution of resources, software, and knowledge between increase devices over a network that's usually net. It's expected that this variety can grow considerably within the future. An example of this is often software system as a Service, or SaaS, that is an purpose that's delivered through the browser to clients. Cloud applications connect with a info that's being run on the cloud and have varied degrees of efficiency. Some are manually organized, some are preconfigured, and a few are native. Native cloud databases are historically higher equipped and a lot of stable that people who are changed to adapt to the cloud. In cloud computing application software package and knowledgebases area unit moving to the centralized giant data centers. This mechanism brings concerning several new challenges, that haven't been well understood. Security and privacy issues is unit among the highest issues name within the approach of wider acceptance of cloud. In cloud computing the foremost disquiet is to form the protection to end user to safeguard files or data from unlawful user. Safety is that the chief intention of any data through that unauthorized individual cannot admittance your file or so as in cloud. We have got titled one planned style and style which can facilitate to cypher and rewrite the file at the user facet that supply security to data at rest equally as whereas moving.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Cloud computing is presently days rising field thanks to its performance, high availability, low cost. At intervals the cloud many services unit provided to the shopper by cloud. data store is main future that cloud service provides to the companies to store huge amount of storage capability. But still many companies are not able to implement cloud computing technology because of lack of correct security management policy and weakness in protection that lead to many challenge in cloud computing.

Cloud computing is internet based computing where virtual shared servers supply computer code, infrastructure, platform, devices and completely different resources and hosting to computers on a pay-as-you-use basis.

Users will access these services on the market on the “internet cloud” while not having any previous data on managing the resources concerned. Thus, users will concentrate additional on the core business processes instead of defrayment time on gaining data on resources required to manage their business processes.

Due to its low price, robustness, flexibility and ubiquitous nature, cloud computing is dynamical the method entities manage their information. However, numerous privacy issues arise whenever potentially perceptible in order is outsourced to the cloud. The projected theme prevents the cloud server from learning any probably sensitive plaintext within the outsourced databases. It also permits the information owner to entrust users to conducting content-level fine-grained personal search and decryption. Moreover, our idea chains personal questioning whereby neither the information owner nor the cloud server learns query details.

II. RELATED WORK

Most software system or management systems area unit just software system packages that users can acquire to form, maintain or use a info. However, since the introduction of cloud computing, software system has morphed into a very new style of service with its own distinctive blessings and task specific advantages. For one issue, any style of cloud service model will need to use a passionate cloud software system therefore on extremely offer customers with tremendous access to information and databases. ancient DBMS's square measure just not discovered or equipped to have an effect on the strain of cloud computing. And in reality, if software system was deployed as a service as an area of an even bigger package provided, it'd potential be much more economical in its duties and therefore cheaper inside the long-standing time. All DBMS, despite whether or not or not ancient or cloud-based, square measure primarily communicators that perform as middlemen between the code package and so the information. but can be a cloud software system utterly completely different a regular one? For one issue, cloud-based software system area unit terribly ascendable . they are able to handle volumes of information and processes that will exhaust a typical software system. Despite their quality however, cloud software system area unit still somewhat lacking within their ability to resize to terribly big processes; this is {often|this can be} often expected to be remedied within the returning months and years however. Currently, the utilization of cloud DBMS's unit among the most used inside the testing and development of latest cloud applications and processes. however whereas an entire computer code area unit getting to be used on a cloud infrastructure. The SecureDBaaS style is tailored to cloud platforms and does not introduce any go-between proxy or broker server between the patron and so the cloud provider. Eliminating any certain intermediate server permits SecureDBaaS to understand an analogous accessibility, responsibility, and snap levels of a cloud DBaaS. completely different proposals supported intermediate server(s) were thought-about impracticable for a cloud-based resolution as a results of any proxy represents one purpose of failure and a system bottleneck that limits the foremost benefits (e.g., measurability, handiness, and elasticity) of a information service deployed on a cloud platform. in distinction to SecureDBaaS, architectures hoping on a certain intermediate proxy do not support the foremost typical cloud state of affairs where geographically unfold purchasers can at an equivalent time issue read/write operations and organisation modifications to a cloud information.

Propose a completely unique design that integrates cloud info services with information confidentiality and therefore the chance of execution coincidental operations on encrypted information. The projected design has the any advantage of eliminating intermediate proxies that limit the snap, availableness, and quantifiability properties that ar intrinsic in cloud-based solutions[1]. Proposed a system to develop a system that may give Security ANd Privacy to Cloud Storage conjointly to determine an secret writing based mostly System for shielding Sensitive information on the cloud and Structure however owner and storage Service supplier to control on encrypted Data[2].



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Concept of PhantomDB, that may be a new framework for finding this downside. PhantomDB maintains information security by encrypting the information before storing it on the server. projected theme to stop information access from unauthorized access, it propose a distributed theme to supply security of the datain cloud .This could be achieved by victimisation homomorphy token with distributed verification of erasure-coded information and stores the information and identifies the any tamper at the cloud server[3].Proposing AN application of a way to execute operations on encrypted information while not decrypting them which is able to give us with an equivalent results once calculations as if we've worked directly on the raw data[4].

Cryptography explores numerous {data secret writing|encoding|encryption} techniques like homophormic encryption, searchabe and structured secret writing, Identity based mostly secret writing, signature based mostly secret writing etc[5]. For information Authentication and security, cloud used the Rijndael secret writing formula in conjunction with EAP-CHAP[6]. The aim is to review the state of the art within the cloud databases and numerous architectures. It any assesses the challenges to develop cloud databases that meet the user needs and discusses popularly used Cloud databases[7]

The main focus is on implementation and benchmarking of a check system, that shows that our easy nevertheless effective answer overcomes most of the problems[8]. The data owner uses a random key to inscribe a file, wherever the random key's any encrypted with a collection of attributes victimisation KP-ABE. Then, the cluster manager assigns AN access structure and therefore the corresponding secret key to approved users, specified a user will solely decode a cipher text if and providing the information file attributes satisfy the access structure. to realize user revocation, the manager delegate's tasks of information file re secret writing and user secret key update to cloud servers[9].

III. PROPOSED METHODOLOGY

SecureDBaaS provides several unique features that differentiate it from previous work in the field of security for remote database services.

- SecureDBaaS provides several original choices that differentiate it from previous add the field of security for remote info services.
- It guarantees info confidentiality by allowing a cloud info server to execute coincident SQL operations (not exclusively read/write, however conjointly modifications to the info structure) over encrypted knowledge
- It provides identical convenience, elasticity, and measurability of the initial cloud DBaaS as a results of it does not would like any intermediate Response times are plagued by cryptology overheads that for many SQL operations are cloaked by network latencies.
- Multiple clients, presumably geographically distributed, will access at the same time and severally a cloud info service.
- It doesn't need a trusty broker or a trusty proxy as a result of tenant knowledge and data stored by the cloud database are always encrypted.

IV. RESULT ANALYSIS

Data Encryption and Decryption

In the first module, we make a provision of encrypting our personal data using encryption algorithm. We provide the data security and confidentiality using this application. We stored our personal data on the cloud in encrypted form using a key. By using the same key we can decrypt that data from cloud. We can encrypt ant text document, image and sound file using this application.

At the time of accessing this file from the cloud, we can deceypted the data by using the same key which is used during encrypt the data. In this way, we can provide the security and confidentiality to the data stored on the cloud using this application.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Plain text file data- in image format

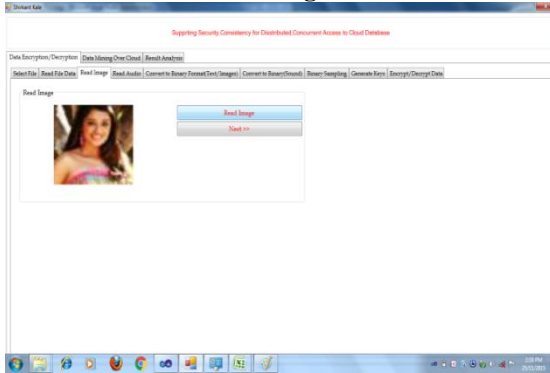


Figure1 -Normal Image

Data after Encryption- in image format

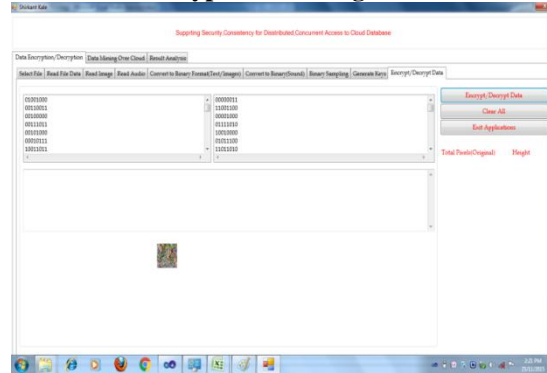


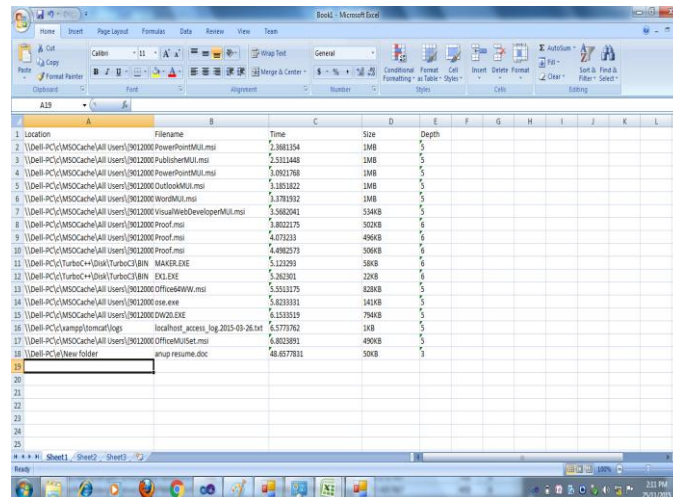
Figure2 - Encrypted image

Data Mining over Cloud

1) Result for group search

After clicking on start search, mining process gives the result of all possible matching file with file location, file name, actual time required for accessing a file, size of file and the depth of the file.

In group search analysis, mining process gives all the possible matching file present in the system which is in various format. In the application, we can directly accessing a file by clicking on the file. It shows the location of the file including size of the file and depth of the file. Result also shows time required for accessing file over cloud.



Location	Filename	Time	Size	Depth
\\Dell-PC\MSOCCache\All Users\9612000\PowerPointMUI.msi		5.3681254	1MB	5
\\Dell-PC\MSOCCache\All Users\9612000\PublisherMUI.msi		5.5311448	1MB	5
\\Dell-PC\MSOCCache\All Users\9612000\PowerPointMUI.msi		5.6921768	1MB	5
\\Dell-PC\MSOCCache\All Users\9612000\OutlookMUI.msi		5.1803822	1MB	5
\\Dell-PC\MSOCCache\All Users\9612000\WordMUI.msi		5.3791932	1MB	5
\\Dell-PC\MSOCCache\All Users\9612000\VisualBasicDeveloperMUI.msi		5.5882041	154KB	5
\\Dell-PC\MSOCCache\All Users\9612000\Proof.msi		5.8022175	302KB	6
\\Dell-PC\MSOCCache\All Users\9612000\Proof.msi		4.673233	496KB	6
\\Dell-PC\MSOCCache\All Users\9612000\Proof.msi		4.6982573	396KB	6
\\Dell-PC\TurboC++\Disk1\TurboC3\BIN\MAKER.EXE		5.122293	58KB	6
\\Dell-PC\TurboC++\Disk1\TurboC3\BIN\DLI.EXE		5.263202	129B	6
\\Dell-PC\MSOCCache\All Users\9612000\Office4W.msi		5.5531375	828KB	5
\\Dell-PC\MSOCCache\All Users\9612000\ese.exe		5.8233331	141KB	5
\\Dell-PC\MSOCCache\All Users\9612000\DW20.EXE		6.1533519	794KB	5
\\Dell-PC\kvm\p\format\logs\localhost_access_log_2015-09-26.txt		6.5773767	1KB	5
\\Dell-PC\MSOCCache\All Users\9612000\OfficeAutoStat.msi		6.8633951	490KB	5
\\Dell-PC\New folder\snip_resume.docx		48.6077811	50KB	3

Figure 3- Result for group search

2) Result for file search

After clicking on start search, mining process gives the result of all possible matching file with file location, file name, actual time required for accessing a file, size of file and the depth of the file.

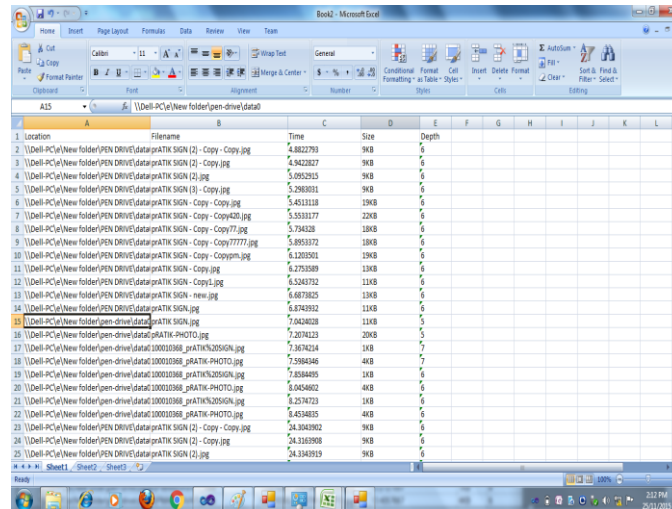
We can directly access a particular file by clicking on the location of the file. Also we can update a file directly after accessing it.

In the file search, we can search a particular format file by selecting a particular extension of the file. Application will generate a result of selected extension of the file.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015



Location	Filename	Time	Size	Depth
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN [2] - Copy.jpg		4.8822793	9KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN [2] - Copy.jpg		4.9422827	9KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN [2].jpg		5.0512935	9KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN [3] - Copy.jpg		5.2880311	9KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN - Copy.jpg		5.4513118	19KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN - Copy.jpg		5.5533177	22KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN - Copy.jpg		5.736428	18KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN - Copy.jpg		5.8953372	18KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN - Copy.jpg		6.1205901	19KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN - Copy.jpg		6.2753589	18KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN - Copy.jpg		6.5249732	11KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN - new.jpg		6.6077825	19KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN.jpg		6.8793932	11KB	6
\\Dell-PC\New folder\pen-drive\data\pratik SIGN.jpg		7.0434028	11KB	5
\\Dell-PC\New folder\pen-drive\data\pratik PHOTO.jpg		7.2074123	20KB	5
\\Dell-PC\New folder\pen-drive\data\100010388_pratik205SIGN.jpg		7.3674214	1KB	7
\\Dell-PC\New folder\pen-drive\data\100010388_pratik PHOTO.jpg		7.5984846	4KB	7
\\Dell-PC\New folder\pen-drive\data\100010388_pratik205SIGN.jpg		7.8394949	1KB	6
\\Dell-PC\New folder\pen-drive\data\100010388_pratik PHOTO.jpg		8.0454052	4KB	6
\\Dell-PC\New folder\pen-drive\data\100010388_pratik205SIGN.jpg		8.2517473	1KB	6
\\Dell-PC\New folder\pen-drive\data\100010388_pratik PHOTO.jpg		8.4534835	4KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN [2] - Copy.jpg		24.3843902	9KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN [2] - Copy.jpg		24.3169308	9KB	6
\\Dell-PC\New folder\PEN DRIVE\data\pratik SIGN [2].jpg		24.5349319	9KB	6

Figure 4- Result for group search

Advantages of Proposed System:

- The projected design doesn't need modifications to the cloud information, and it is immediately applicable to existing cloud DBaaS, like the experimented PostgreSQL and Cloud database, Windows Azure and Xeround .
- There are theoretical and sensible limits to increase our resolution to different platforms and to incorporate new secret writing algorithmic rule.
- It guarantees information confidentiality by permitting a cloud information server to execute cooccurring SQL operations (not solely read/write, however also modifications to the information structure) over encrypted data.
- It provides a similar availability, elasticity, and quantifiability of the initial cloud DBaaS as a result of it doesn't need any intermediate server.

V. CONCLUSION

We propose associate innovative design that guarantees confidentiality of knowledge hold on publically cloud databases. Not like progressive approaches, our answer doesn't have faith in associate intermediate proxy that we tend to think about one purpose of failure and a bottleneck limiting accessibility and quantifiability of typical cloud info services. An oversized part of the analysis includes solutions to support synchronal SQL operations (including statements modifying the info structure) on encrypted information issued by heterogynous and presumably geographically spread purchasers.

It is value perceptive that experimental results supported the TPC-C traditional benchmark show that the performance impact of data writing on interval becomes negligible as a results of it's covert by network latencies that ar typical of cloud eventualities. above all, contemporaneous browse and write operations that do not modify the structure of the encrypted data cause negligible overhead .Dynamic eventualities characterized by (possibly) contemporaneous modifications of the information structure ar supported, but at the price of high method costs. These performance results open the realm to future enhancements that we have a tendency to tend to investigation.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

REFERENCES

- [1] Luca Ferretti, Michele Colajanni, and Mirco Marchetti, "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases," IEEE transaction on parallel and distributed system, vol. 25, No. 2, February 2014.
- [2] Mohit Marwaha, Rajeev Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing," IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.
- [3] R.A. Popa, C.M.S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted QueryProcessing," Proc. 23rd ACM Symp. Operating Systems Principles, Oct. 2011.
- [4] Deepanchakaravarthi Purushothaman1, Dr.Sunitha Abburu, "An Approach for Data Storage Security in Cloud Computing," IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012 .
- [5] Maha TEBA, Saïd EL HAJJI and Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security", Proceedings of the World Congress on Engineering 2012 Vol 1 WCE 2012, July 4 - 6, 2012, London, U.K
- [6] Samarjeet Kaur, "Cryptography and Encryption In Cloud Computing," VSRD-IJCSIT, Vol. 2 (3), 2012, 242-249.
- [7] Sanjoli Singla, Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013.
- [8] Indu Arora1 and Dr. Anu Gupta2, "Cloud Databases: A Paradigm Shift in Databases," IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012.
- [9] Francesco Pagano, D Davide Pagano, "Using In-Memory Encrypted Databases on the Cloud," IEEE 978-1-4577-1186-2/11/\$26.00 ©2011.
- [10] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R. Motwani, "Distributing Data for Secure Database Services," Proc.Fourth ACM Int'l Workshop Privacy and Anonymity in the Information Soc., Mar. 2011.
- [11] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
- [12] E. Damiani and F. Pagano, "Handling confidential data on the untrusted cloud: an agent-based approach," Cloud Computing 2010, pp. 61-67
- [13] G.Jai Arul Jose, C.Sajeev, "Implementation of Data Security in Cloud Computing", International Journals of P2P Network Trends and Technology, Vol. 1, Issue 1, 2011.

BIOGRAPHY

Shrikant P. Kale is a student of G. H. Raisoni College of Engineering and Management, Amravati. He is pursuing Master of Engineering (ME) in Computer Science and Engineering. His research interests are Data Mining, cloud Computing, Computer Network, etc.