ISSN Application No. 21650

Journal of Cloud Computing and Data Base Management

Volume No. 9

Issue No. 2

May - August 2023

ENRICHED PUBLICATIONS PVT. LTD

S-9, IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR-5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-47026006

Journal of Cloud Computing and Data Base Management

Aims and Scope

Journal of Cloud Computing and Database Management is a peerreviewed Print + Online journal of Enriched Publications to disseminate the ideas and research findings related to all sub-areas of Computer Science and IT. It also intends to promote interdisciplinary researches and studies in Computer Science and especially database management and cloud computing maintaining the standard of scientific excellence. This journal provides the platform to the scholars, researchers, and PHD Guides and Students from India and abroad to adduce and discuss current issues in the field of Computer Sciences.

Journal of Cloud Computing and Data Base Management

(Volume No. 9, Issue No. 2, May - August 2023)

Contents

Sr. No	Article / Authors Name	Pg No
1	Challenges of Big Data Applications in Cloud Computing - *Manoj Muniswamaiah, Tilak Agerwala, Charles C. Tappert*	1 - 13
2	Deduplication on Encrypted Big Data in Cloud - *Nehal Pandey, Nishant Jain, Nikshay Jain, Ishita Mattoo, Neha Hajar*	14 - 23
3	Secured Group Data Sharing in Cloud Computing - *Pooja Katurde, Rameshwari Konda, Trupti Mohite, Nisha Melkunde*	24 - 29
4	Replacing Phone Storage with Direct Cloud Computation System - *Ankita Aditya, Meet Shah, Tripti Jain*	30 - 37
5	Mitigating Cloud Security Threats using Cloud Access Security Brokers - *Shabnam Kaur, Rajandra Gupta*	38 - 43

Challenges of Big Data Applications in Cloud Computing

[1] Manoj Muniswamaiah, [2] Tilak Agerwala, [3] Charles C. Tappert
[1,2,3]Seidenberg School of CSIS, Pace University, White Plains, New York
E-mail: [1]mm42526w@pace.edu, [2]tagerwala@pace.edu, [3]ctappert@pace.edu

ABSTRACT

Big Data applications are used for decision making process for gaining useful insights hidden in large volume of data. Better analysis of data will result in faster, optimal and profitability of the organization. These big data applications are often deployed and executed on cloud computing platforms to take the advantage of scalability and complex computing which they offer. It eliminates the need for computing hardware and provides the infrastructure required for large data processing and analysis. Big data applications help in decision making process and at the same time it possess challenges in data transformation, heterogeneity and quality. This paper aims to provide challenges and issues of big data in cloud computing and also, some good practices which helps in big data analysis.

Keywords - Big Data; Cloud Computing; Data Transformation; Data Analysis; Data Warehousing

I. INTRODUCTION

The volume and information captured from devices and multimedia by organizations is increasing and has almost doubled every year. This big data generated is characterized to be huge, can be structured or unstructured which requires preprocessing and cannot be easily loaded into regular relational databases. Healthcare, finance, engineering, e-commerce and various scientific fields use these data for decision making and analysis. The advancement in data science, data storage and cloud computing has allowed for storage and mining of big data [1].

Cloud computing has resulted in increased parallel processing, scalability, virtualization of resources and integration with data storages. Cloud computing has also reduced the infrastructure cost required to maintain these resources which has resulted in the scalability of data produced and consumed by the big data applications. Cloud virtualization provides the process to share the resources and isolation of hardware to increase the access, management, analysis and computation of the data [1].

The goal of this paper is to provide challenges of big data applications in cloud computing with focus on data storage, transformation, heterogeneity and scalability in cloud computing platforms and good design principles which can be followed to improve the quality of the applications.

II. BIG DATA

Data which is difficult to store, manage and analyze through traditional databases is termed as “Big Data”. It requires integration of various technologies to discover hidden values from the data that is varied, complex and requires heavy computing. The characteristics of big data are.

1. Volume - Collection of data from different sources which would allow users to data mine the hidden information and patterns found in them.

2. Velocity - Data been streamed in real time from sources such as IoT devices. It is the speed at which data is transferred and consumed for collection and archiving.

3. Variety - Data collected in either structured or unstructured format from sensors and social networks. Unstructured data include text messages, audio, blogs.

4. Variability - Data flow can be highly inconsistent and varies during peak period and their ingestion into the data stores.

5. Value - Represents the hidden value discovered from the data for decision making.

6. Veracity - It refers to the reliability of the data source. It's importance is in the context and the meaning it adds to the analysis.

7. Validity - It refers to the accuracy of the data been collected for its intended use.

8. Vulnerability - It represents the security aspects of the data been collected and stored.

9. Volatility - How long the data needs to be stored historically before it is considered irrelevant.

10. Visualization - In-memory tools which are used to plot data points representing as data clusters or tree maps [2].

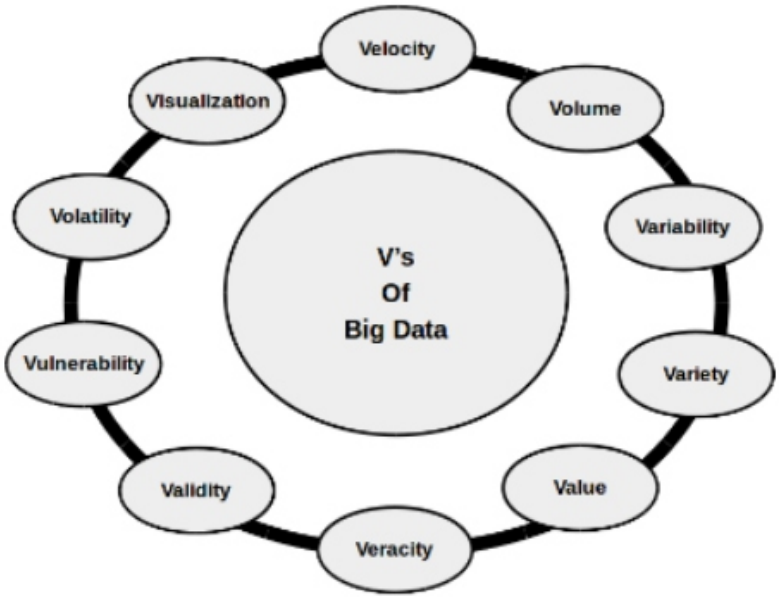


Figure 1 : V's Big Data

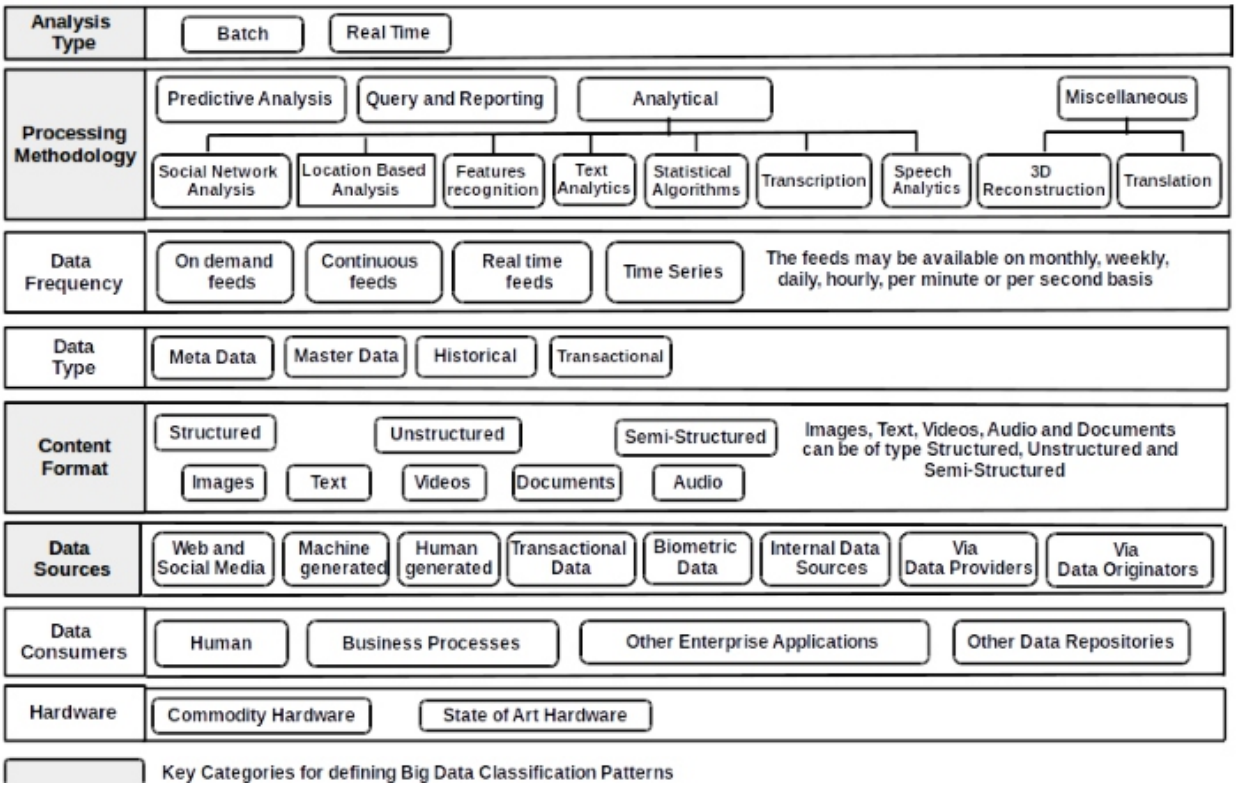


Figure 2 : Big Data Classification

Big data is classified based upon its source, format, datastore, frequency, processing methodology and analysis types as shown in figure 2.

2.1. BIG DATA CLASSIFICATION

Analysis Type - Whether the data is analyzed in real time or batch process. Banks use real time analysis for fraud detection whereas business strategic decisions can make use of batch process.

Processing Methodology - Business requirements determine whether predictive, ad-hoc or reporting methodology needs to be used.

Data Frequency - Determines how much of data is ingested and the rate of its arrival. Data could be continues as in real-time feeds and also time series based.

Data Type - It could be historical, transactional and real-time such as streams.

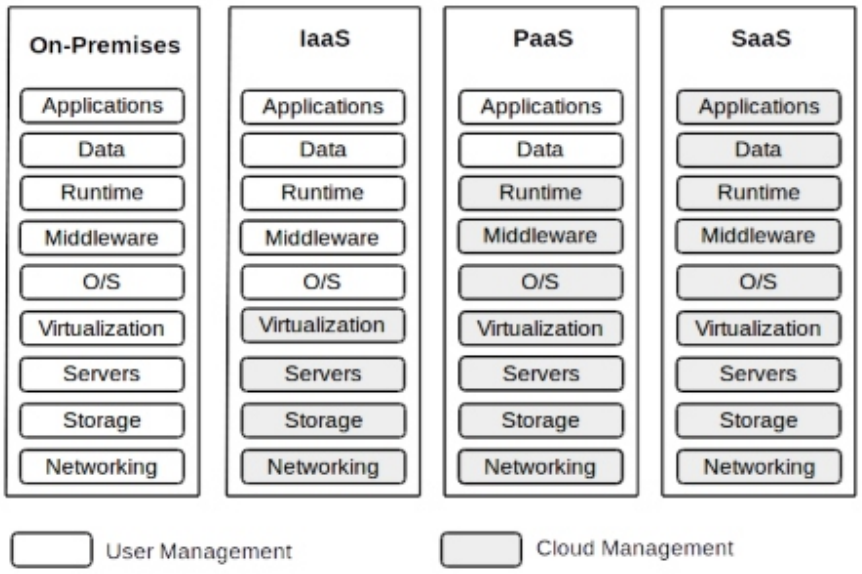


Figure 3 : Summary of Key Differences

Data Format - Structured data such as transactions can be stored in relational databases. Unstructured and semi-structured data can be stored in NoSQL data stores. Formats determine the kind of datastores to be used to store and process them.

Data Source - Determines from where the data is generated like social media, machines or human generated.

Data consumers - List of all users and applications which make use of the processed data [3].

III. CLOUD COMPUTING

Cloud computing has become default platform for storage, computation, application services and parallel data processing. It allows organizations to concentrate on core business without having to worry about the infrastructure, maintenance and availability of the resources.

Figure 3 shows the differences between on premise and cloud services. It shows the services offered by each computing layer and differences between them.

SaaS: Software as a Service

Software as a service represents the most commonly used business option in cloud services. It uses the internet to deliver applications to users. It does not require installations on client side as they run directly through web. In SaaS vendor manages all the servers, middleware and storage of the data. It eliminates users to install, manage and upgrade softwares.

PaaS: Platform as a Service

Platform as a Service provides developers with framework which they can use to build their applications. It allows business to design and create applications that are integrated in to PaaS software components. These applications are scalable and highly available since they have cloud characteristics.

IaaS: Infrastructure as a Service

Infrastructure as a Service delivers cloud computing infrastructure such as servers, storage, operating systems to organizations through virtualization technology. IaaS provides same capabilities as data centers without having to maintain them physically [4].Figure 4 represents the different cloud computing services been offered

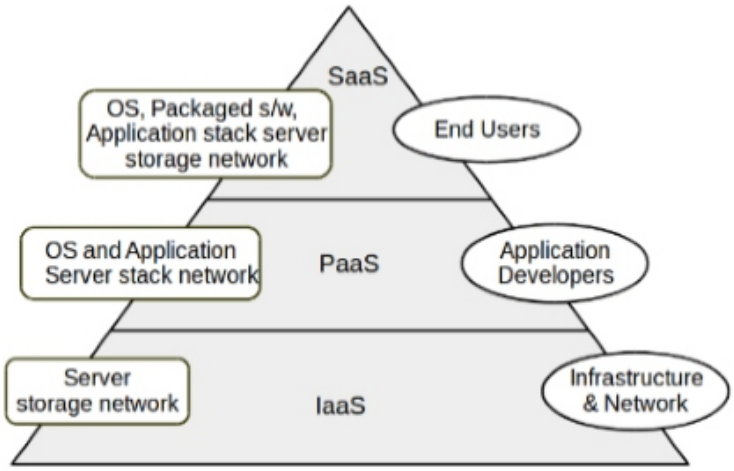


Figure 4 : Primary Cloud Computing Services

IV. RELATIONSHIP BETWEEN THE CLOUD AND BIG DATA

Cloud computing and big data go together, as cloud provides the required storage and computing capacity to analyze big data. Cloud computing also offers the distributed processing for scalability and also expansion through virtual machines to meet the requirements of exponential data growth.

It has resulted in the expansion of analytical platforms. This has resulted in service providers like Amazon, Microsoft and Google in offering big data systems in cost efficient manner.

Cloud computing environment has several providers and user terminals. Data is collected using big data tools later it is stored and processed in cloud. Cloud provides on-demand resources and services for uninterrupted data management.

The most common models for big analytics is software services such as (SaaS), Platform service like (PaaS) and Infrastructure service like (IaaS). Recently Cloud analytics and Analytics as a Service

(AaaS) are provided to clients on demand. Analytics as a Service (AaaS) provides services for a

fast and scalable way to integrate data in semi- structured, unstructured and structured format, transform and analyze them.

Virtualization simulates a virtual computing environment that can run operating system and applications on it. Virtualization reduces the workload and unifies them in to a physical server which helps in consolidation of multi-core CPUs in to one physical node.

This reduces and improves resource utilization and power consumption as compared to the multi-node setup. Virtualized big data applications like Hadoop provide benefits which cannot be provided using physical infrastructure in terms of resources utilization, cost and data management. Virtual data includes wide range of data sources and improves the data access from heterogeneous environments. It also enables high-speed data flow over the network for faster data processing.

Information privacy and security are one of the important aspects of big data in cloud as data is hosted and processed on the third party services and infrastructure. Service level agreements must be maintained between providers and consumers in order to bring confidence in users.

Security of big data in the cloud is important because data needs to be protected from malicious intruders, treats and also how the cloud providers securely maintain huge disk space [5].

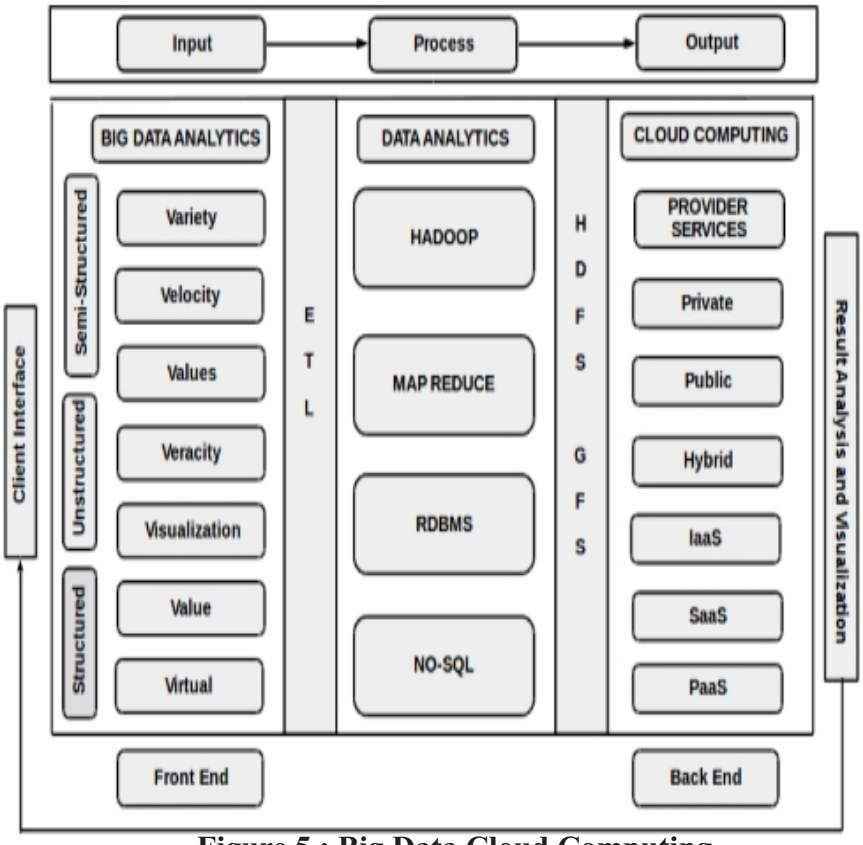


Figure 5 : Big Data Cloud Computing

The relationship between big data and cloud computing follows input, processing and output model as shown in Figure 5. The input is the data obtained from various data sources and are processed and stored using Hadoop and data stores. Processing steps includes all the tasks required to transform input data. Output is the result obtained after data been processed for analysis and visualization. Internet of Things (IoT) is one of the common factors between Cloud computing and big data. IoT devices include sensors, mobile devices which generate large amount of data which needs to be processed and analyzed in real time. Cloud providers allow data to be transmitted over internet or via lease lines. It provides a pathway for the data to navigate, store and be analyzed. Cloud computing provides common platform for IoT and big data. IoT is the source of the data and big data is an analytical technology platform of the data as depicted in the Figure [6].

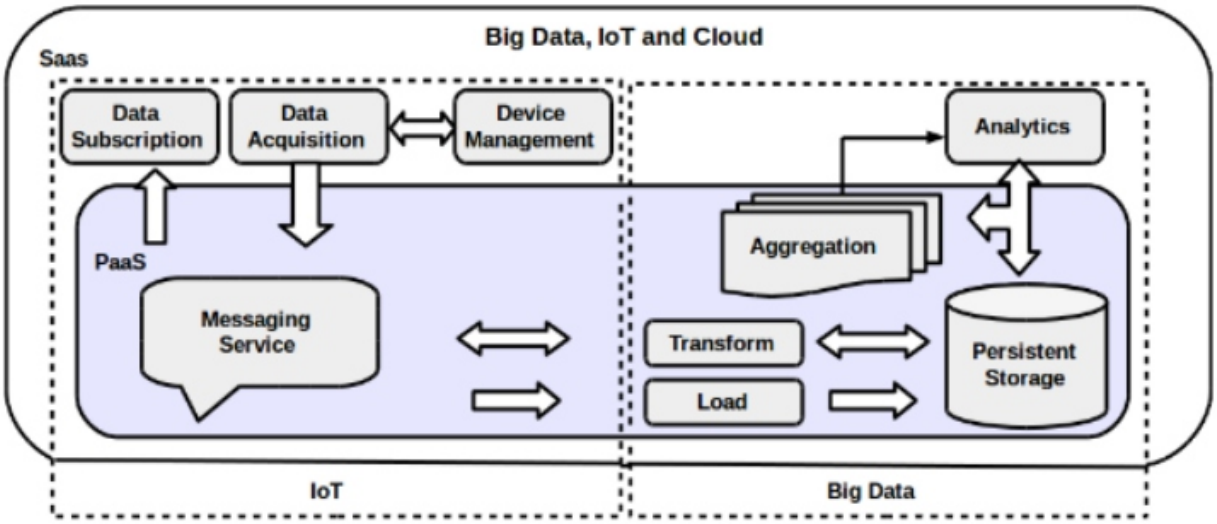


Figure 6 : Convergence of IoT, Big Data and Cloud Copmuting

CASE STUDIES

There are several case studies of big data on cloud computing.

A. Redbus

Redbus is an online travel agency for bus ticket booking in India. Redbus decided to use Google data infrastructure for data processing and analysis in order to improve customer sales and management of the ticket booking system [6].

B. Nokia mobile company

Nokia mobile phones are been used by many people for telecommunication. Nokia gathers large amount of data from mobile phones in petabyte scale for business decision strategies using Hadoop data warehouse for analytics [6].

C. Tweet Mining in Cloud

Noordhuis et al. [6] used cloud computing to gather and analyze tweets. Amazon cloud infrastructure was used to perform all the computations. Tweets were crawled and later page ranking algorithm was applied. The data crawled had nearly 50 million nodes and 1.8 billion edges.

DATA STORES

Modern databases need to handle large volume and different variety of data formats. They are expected to deliver extreme performance and scale both horizontally and vertically. Database architects have produced NoSQL and NewSQL as alternatives to relational database. Below are characteristics of relational database, NoSQL and NewSQL [7].

Characteristic	RDBMS	NoSQL	New SQL
ACID compliance	Yes	No	Yes
OLAP/OLTP	Yes	No	Yes
Data analysis	Yes	No	Yes
Schema rigidity	Yes	No	Maybe
Data format flexibility	No	Yes	Maybe
Distributed computing	Yes	Yes	Yes
Scale up (vertical)/Scale out (horizontal)	Yes	Yes	Yes
Performance with growing data	Fast	Fast	Very Fast
Performance overhead	Huge	Minimal	Minimal
Popularity and community Support	Huge	Growing	Slow Growth

HADOOP TOOLS AND TECHNIQUES

Big data applications use various tools and techniques for processing and analyses of the data below table represents some of them [8].

Tools/Techniques	Description	Developed by	Written in
HDFS	Redundant and Reliable massive data storage	Introduced by Google	Java
Map Reduce	Distributed data processing framework	Introduced by Google	Java
YARN	Cluster resource management framework	Apache	Java
Storm	Stream based task parallelism	Twitter	Clojure
Spark	Stream based data parallelism	Berkeley	Scala
Map Reduce	Java API.	Introduced by Google	Java
Pig	Framework to run script language Pig Latin	Yahoo	Java
Hive	SQL-like language HiveQL	Facebook	Java
HCatalog	Relational table view of data in HDFS	Apache	Java
HBase	NoSQL column oriented	Google's BigTable	Java
Casandra	NoSQL column oriented	Facebook	Java
Flume	Import/Export unstructure or semi- structure data into HDFS. Data ingestion into HDFS.	Apache	Java
Sqoop	Tool designed for efficiently transferring bulk structured data (RDBMS) into HDFS and vies versa.	Apache	Java
Kafka	Distributed publish-subscribe messaging system for data integration	LinkedIn	Scala
Ambari	Web based cluster management UI	Hortonworks	Java
Mahout	Library of machine learning algorithms	Apache	Java
Oozie	Define collection of jobs with their execution sequence and schedule time	Apache	Java

Sentry	Role based authorization of data stored on an Apache Hadoop cluster.	Cloudera	Java
Ranger	Role based authorization of data stored on an Apache Hadoop cluster.	Hortonworks	Java
Zookeeper	Coordination service between hadoop ecosystems.	Yahoo	Java

V. RESEARCH CHALLENGES

Volume of data been generated worldwide doubles almost every year. Retail industries do millions of translations per day and also have established data warehouses to store data to take advantages of machine learning techniques to get the insight of data which would help in the business strategies. Public administration sector also use information patterns from data generated from different age levels of population to increase the productivity. Also, many of the scientific fields have become data driven and probe into the knowledge discovered from these data.Although cloud computing is been used for processing of big data applications there are several challenges in data storage, data transformation, data quality, privacy, governance [9].

Data Capture and Storage

Data gathered from various sensor devices, machine logs and networks keeps increasing every year. It has changed the way we store data and their access mechanism. Previously, hard disk drives (HDD) had poor I/O performance but solid-state drives (SSD) may alleviate I/O performance to some extent but not completely.

Data Transmission

Cloud data stores are used for data storage however, network bandwidth and security poses challenges.

Data Curation

It involves data archiving, management and retrieval process. Structured data is stored in data warehouse and data marts which requires preprocessing of data before loading data and also can be queried using Standard Query Languages.

Unstructured data is stored in NoSQL data stores which are schema free, support replication, distributed storage and consistency. There are various NoSQL data stores such as key-value, columnar, document and graph datastores which are specific to type of data which gets stored in them.

Scalability

Scalability is mainly manual and is static. Most of the big data systems must be elastic to handle data changes. At the platform level there is vertical and horizontal scalability.

Elasticity

Elasticity accommodates data peaks using replication, migration and resizing techniques. Most of these are manual instead being automated.

Availability

Availability refers to systems been available to users. One of the key aspect of cloud providers is to allow users to access one or more data services in short time even during security breach.

Data integrity

Data needs to be modified only by the authorized user or parties. Since the users may not be able to physically access the data, the cloud should provide mechanisms to check for the integrity of data.

Security and Privacy

Based on the service level agreement the data can be encrypted. But querying encrypted data would result in time consumption. User privacy can be de- identified, it's also been proved that de-identification can be reverse engineered.

Heterogeneity

Big data systems need to deal with different formats of data coming from various sources. Handling unstructured data during peak hours and processing them for analysis becomes a challenge.

Data Governance

Data governance specify the way data needs to be handled, data access policies have its life cycle. Defining the data cycle is not easy task and also its policies could lead to counter productiveness.

Data Uploading

Data is usually been uploaded through internet which is unsecure but results in time-consumption if they are encrypted and transmitted.

Data Recovery

Specifies the procedures and locations from where the data can be recovered. Generally there is only one destination from where the data is securely recovered.

Data Visualization

Data Visualization is used to represent knowledge graphically for better intuition and understanding. Ecommerce industries generate lot of data which needs to be turned into pictorial representation for better intuition.

VI. BIG DATA BUSINESS CHALLENEGES

Utilities: Power consumption prediction

Utility companies use smart meter to measure gas and electricity consumption. These devices generate huge volumes of data. A big data solution needs to monitor and analyze power generation and consumption using smart meters.

Social Network: Sentiment analysis

Social networking companies such as Twitter needs to determine what users are saying and topics which are trending in order to perform sentiment analysis.

Telecommunication: Predictive analytics

Telecommunication provides need to build churn models which depends on the customer profile data attributes. Predictive analytics can predict churn by analyzing the subscribers calling patterns.

Customer Service: Call monitor

Call center big data solutions use application logs to improve performance. The log files needs to be consolidated from different formats before they can be used for analysis.

Banking: Fraud Detection

Banking companies should be able to prevent fraud on a transaction or a user account. Big data solutions should analyze transactions in real time and provide recommendations for immediate action and stop fraud.

Retailers: Product recommendation

Retailers can monitor user browsing patterns and history of products purchased and provide a solution to recommend products based on it. Retailers need to make privacy disclosures to the users before implementing these applications [3].

VII. GOOD PRINCIPLES

Good Architectural Design

Big data architecture should provide distributed and parallel processing through cloud services. NoSQL can be used for high performance and faster retrieval of data. Lambda and Kappa architectures can be used for processing in real-time and batch processing mode.

Different Analytical Methods

Big data applications need to take the advantage of data mining, machine learning, distributed programming, statistical analysis, in-memory analytics and visualization techniques offered through cloud.

Use appropriate technique

No one technique can be used to analyze data. We must use appropriate technology stack to analyze the data.

Use in-memory analytics

It is not advisable to move data around. In-memory database analytics can be used to execute analytics where data resides. In-memory analytics also provides real-time processing of data.

Distributed data storage for in-memory analytics The data needs to be partitioned and stored in distributed data stores to take the advantage of in- memory analytics. Cloud computing infrastructure offers this distributed data storage solutions which must be adopted.

Coordination between tasks and data is required

To achieve scalability and fault-tolerance coordination between data and its processing tasks is required. Specialized cluster management frameworks as a Zookeeper can be used [10].

VIII. CONCLUSION

In the era of Big data of innovation and competition driven by advancements in cloud computing has resulted in discovering hidden knowledge from the data. In this paper we have given overview of Big data application in cloud computing and its challenges which could lead to further research.

REFERENCES

[1] https://arxiv.org/ftp/arxiv/papers/1705/1705.04928.pdf
[2] https://tdwi.org/articles/2017/02/08/10-vs-of-big-data.aspx
[3] https://www.ibm.com/developerworks/library/bd- archpatterns1/index.html
[4] https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the- difference-and-how-to-choose/
[5] https://www.ripublication.com/ijaer17/ijaerv12n17_89.pdf
[6] https://www.sciencedirect.com/science/article/abs/pii/S03064 37914001288?via%3Dihub
[7] https://www.informationweek.com/big-data/big-data-analytics/nosql-newsql-or-rdbms-how-to-choose/ a/d- i d/1297861
[8] https://hadoopabcd.wordpress.com/2015/02/03/the-hadoop- ecosystem-table/
[9] http://acme.able.cs.cmu.edu/pubs/uploads/pdf/IoTBD_2016_10.pdf
[10] https://www.sciencedirect.com/science/article/pii/S00200255 14000346

Deduplication on Encrypted Big Data in Cloud

[1] Nehal Pandey, [2] Nishant Jain, [3] Nikshay Jain, [4] Ishita Mattoo, [5] Neha Hajar
[1,2,3,4]School Of Computer Engineering, MIT Academy of Engineering, Alandi, Pune 412105, India
[5]Professor, School Of Computer Engineering, MIT Academy of Engineering, Alandi, Pune 412105, India
E-mail: [1]nehalpandey1996@gmail.com, [2]nishant.nishant00@gmail.com,
[3]nikshay.nomi@gmail.com, [4]ishitamattoo11@gmail.com, [5]nphajare@comp.maepune.ac.in

ABSTRACT

Cloud computing offers a latest approach of service provision by re-arranging varied resources over the net. the foremost major and widespread cloud service is data storage. So on maintain the privacy of data holders, data area unit sometimes hold on cloud in associated degree encrypted kind. However, encrypted data introduces provocation for cloud data duplication that becomes crucial for big data storage and method in cloud. Ancient replicating schemes cannot work on encrypted information[1].They cannot exile support in- formation access management and repeal. that's why, not of them could also be immediately deployed in follow. throughout this paper, we tend to gravitate to place forward a topic to deduplicate encrypted data hold on in cloud supported freehold challenge and proxy re-encryption[6]. It integrates cloud data deduplication with access management. we tend to tend to evaluate its performance supported exhaustive analysis and laptop simulations. The results show the superior efficiency and effectiveness of the theme for potential sen-sible activity, notably for big data deduplication in cloud storage[2].

Keywords - Access Control, Big Data, Cloud Computing, Data Deduplication, Proxy Re-Encryption

I. INTRODUCTION

Cloud computing offer a replacement methodology of data Technology service by rearranging numerous resources (e.g. storage, computing) providing them to users supported their demands. The crucial and desired cloud service is knowledge. Storage service[3]. Cloud users transfer their personal or condential knowledge to {the knowledge|the info|the information} center of a Cloud Service supplier (CSP) and permits it to take care of these variety of data. Since intrusions and attacks to-wards sensitive knowledge at CSP aren't evitable . it's sagacious to require as a right that CSP can't be trustworthy by cloud users[4]. because of the quick growth of knowledge process and alternative review technologies, the privacy matter becomes serious. Hence, the great apply is just to source the encrypted knowledge to the cloud so as to safeguard knowledge security and user privacy. however similar or dissimilar users might transfer duplicated knowledge within the encrypted type to CSP, principally in situations wherever knowledge area unit shared among several users[5]. though storage of cloud area is large, knowledge duplication significantly misspend network resources, absorb an outsized quantity of energy, and complexes knowledge management. the event of various services additional makes it extreme to deploy systematic resource management mechanisms. severally, duplication becomes critical for giant knowledge storage and process within the cloud[6].

Reduplication has proved to achieve high value savings, e.g. reducing upto 90- 95 % of the storage required for backup applications and upto sixty eight % in customary in systems. Obviously, the savings, which might be passed back straightly or incidentally to cloud users, area unit signifcant to the political economy of cloud business[3]. manner to|a way to} manage the encrypted knowledge storage with the duplication in associate degree economical way may be a practicable issue. However, happiness to the current time industrial duplication answer cant handle the encrypted knowledge. gift answer for duplication endure from brute-force attacks. Reduplication has proved to achieve high value savings, e.g. reducing up to 90-95 % storage required for backup applications and up to sixty eight % within the customary systems[7]. Evidently, the savings, which might be came back back straightly or incidentally to the cloud users, area unit exceptional to the political economy of cloud business. manner to|a way to} manage the encrypted knowledge storage with deduplication in associate degree regular way may be a actual issue. However, gift industrial duplication solutions cant handle the encrypted knowledge. gift solutions for duplication endure from brute-force attacks[8].They cannot regulate knowledge access management and take back at a similar time. gift solutions cannot responsibility, security and privacy with sound performance. during this paper, we tend to had given a theme depend on knowledge freehold, stand against and Proxy Re-Encryption (PRE) to regulate encrypted knowledge storage with duplication. we've intention to resolve toughy|the problem} of duplication within the state of affairs wherever the information holder is untouchable or difficult to urge concerned. Meanwhile, the performance of knowledge duplication in our theme. isn't developed by the dimensions of knowledge, so applicable for giant data[9].

II.HISTORY AND BACKGROUND

Encrypted information Reduplication Cloud storage service supplier like Mozy, Dropbox, Google Drive etal. perform duplication to consume less area by keeping one copy of every uploaded. However, if the shoppers often code their information, storage savings by duplication ar fully lost[2]. it's as a result of the encrypted information ar keep as completely different constituents by applying varied encoding keys. Existing industrial solutions fail in encrypted information duplication. as an example, DeDu is associate degree economical duplication system, however it cannot manage encrypted information. Restore duplication and client-side encoding could be a active analysis topic. Message-latched encoding (MLE) intends to resolve this downside. the foremost necessary of showing MLE is focused encoding (CE), found by Douceur and other[4]s. cerium was used at intervals a good vary of economic and analysis storage service systems. Let M be a less information, a consumer 1st computes a key K hectometer by employing a cryptographical hash operate H to M, so computes cipher text C EK;M via a oppressive biradial encoding schemes. A second client B can code identical M and it'll manufacture identical C, that allows duplication. However, cerium is subject to a elementary security disadvantage, namely, status to down brute-force wordbook attacks. Knowing that the target information M underlying the target cipher text C is drawn from a wordbook S fM1; . . .; Mng of size n,

associate degree wrongdoer will recapture M within the time for n jSj off-line encryptions: for every i 1; . . . ; n, it merely Encrypts Mi to receive a cipher text indicated as Ci and returns Mi specified C Ci. This works as a result of cerium is oppresive and keyless[5]. the protection of cerium will solely be done once the target information is drawn from a large area to exhaust. different downside of cerium is that it's not versatile in grips information access management by information holders, primarily for information revocation method, since it's impractical for information holders to come up with identical new key for information re-encryption. a picture duplication theme adopts 2 servers to realize variability of duplication[6]. The cipher text C of cerium is encrypted with the assistance of a user key so send to the servers. It doesn't alter the information sharing when duplication is finished among completely different users. Cloud duplication conjointly focuses to cope up with the interior security exposures of cerium, however it cannot solve the matter caused thanks to information deletion. {a information|a knowledge|an information} holder UN agency takes the information from the cloud will still access identical data as a result of the information holder is aware of the information encoding key if the information isn't deleted from the cloud fully.

III. MATHEMATICAL MODEL

Mathematical Model:

1. S= I,O,P,F,s,Ic)
2. Identify set of input as I

Let I =Set of outsourced data sets by corresponding data user

3. Identify set of output as O

Let O=store unique file on cloud server .

4. Identify the set of processes as P PRE= proxy re- encryption v. AP=Authorized Party. Uo=set of owners.

SE=Symmetric Encryption CSP=Cloud Service Provider Sk=Symmetric Key

Op= Output of System

5. Identify failure cases as F

F=store duplicate file on cloud server and unable to find file ownership.

6. Identify success as s.

s=check duplicate file that is already store on cloud server If file already exist then duplicate file is not stored on cloud only give reference to new file.

Identify the initial condition as Ic Ic= Outsourced data with its privacy privileges to be maintain)

IV. LITERATURE SURVEY

A Veritable Data Reduplication Scheme in Cloud Computing Author Name: Z. C. Wen, J. M. Luo, H. J. Chen, J. X. Meng, X. Li, and J. Li

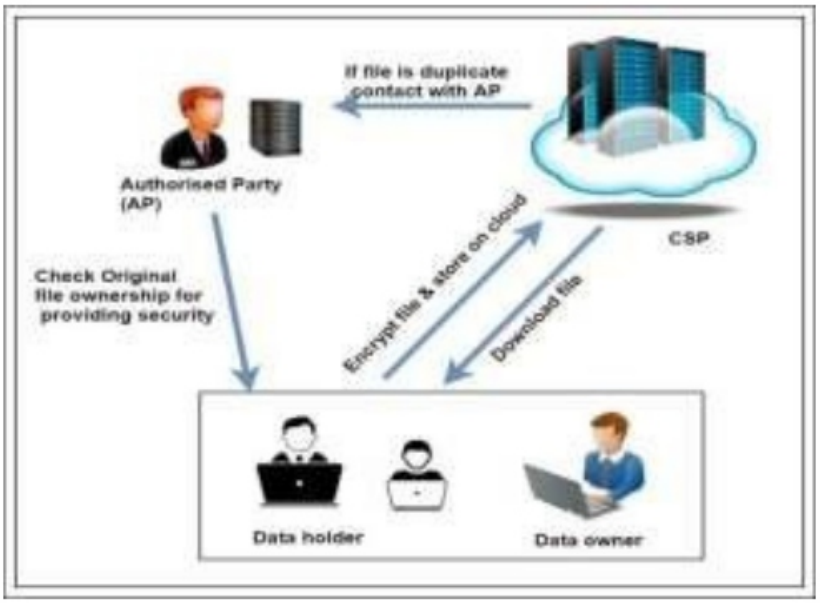


Fig. 1. Architecture Diagram:

Description: A key technique which is used to conserve the storage cost at the cloud storage server is called reduplication. Image is one of the crurial data type which is stored in cloud, but is not frequently discussed in previous works done on reduplication. This paper research on the issue and also recognizes the reduplication of image storage which is in the cloud. In this we consider a task in which we allow a cloud server to check the accuracy of reduplication. Our scheme consists of various advantages over the previous work done, whose framework can be described with the help of following algorithms. At First, before each of the user uploads an encrypted image, he will calculate its hash value which act as a fingerprint. Then, the fingerprint will be sent to both the cloud servers for scrutinizing the duplicates. If the Storage and verification servers both will respond to the user that there is no duplication, then the user can easily transfer his data to the servers. Else, if the fingerprint is consistently found, then the user will give up uploading the data for duplication. Especially, when the fingerprint is only matched with one server, it indicates that the results are conflicting and at least one of server is not valid. The analysis of security and efficiency is also presented in this paper.

A hybrid cloud undertakes to secure the authorized duplication Author Name: J. Li, Y. K. Li, X. F. Chen, P. P. C. Lee, and W. J. Lou

Description: Data duplication is one of the main data compression techniques which is used for removing duplicate copies of same data, and it is mostly used in cloud storage in order to reduce the storage space in cloud and also save bandwidth. In order to protect the confidentiality of suspective data while using duplication, an encryption technique is put forward to encrypt the data before outsourcing it. So to protect the data security, this paper makes the first attempt to solve the problem of authorized data duplication. As it is different from traditional duplication systems, the differential benefits of users are also considered in duplicate check apart from the data itself. We also present various new duplication constructions which support vallidated duplicate check in a hybrid cloud architecture. Security analysis is used for demonstrating that our scheme is protected in terms of the definitions which are specified in the suggested security model.

As a proof of our concept, we implemented a prototype of our suggested and authorized duplicate check and conducted a test of experiments using our prototype. We showed that our suggested authorized duplicate check scheme incurs minimum overhead as compared to normal operations.

Diminishing impact of data fragmentation produced by in-line duplication Author Name: C. Dubnicki, W. Kilian, M. Barczynski, and M. Kaczmarczyk

Description: Deduplication results in data fragmentation, because logically there is a continuous data which is spread over many disk locations. this work is focused on fragmentation which is created by duplicates from previous backups of the same backup set, also these duplicates are very regullar due to frequent full backups which contains a lot of unchanged data. For systems which have in-line dedup , they detect duplicates during writing and also avoids saving them, such fragmentation causes data from the latest backup being spread across the older back- ups. As a result of this, the duration of restore from the new backup can be signicantly increased, and sometimes can be higher than doubled. We suggest an algorithm which is known as context- based rewriting (CBR) to minimize this drop in restore performance for new backups by shifting these fragments to earlier backups, which are barely used for restoring. By selecting and rewriting a few per-centage of duplicates during backup, we can decrease the drop in restore bandwidth from 12-55 percent to only 4-7 percent, as shown by inspection driven by a set of backup traces. All this achieved only with small increase in writing time, between 1 and 5 percent. Since we rewrite only rear duplicates and previous copies of rewritten data are elimented from the background, the whole process introduces little and temporary space overhead.

DeyPoS: Deduplicatable Dynamic Proof of Storage for Multi-User Environments Author Name: Xiang Zhang, Ruiying Du, Jing Chen, Guoliang Xue, Qianhong Wu, and Kun He Description: Dynamic Proof of Storage (PoS) is a useful cryptographic primitive that give permission to user to check the integrity of outsourced document and also to update the data efficiently into a cloud server.

Although there are many researchers who have suggested many dynamic PoS schemes in a single user environments, the problem in a multi-user environments is not been examined properly. A practical multi-user cloud storage system is the one which needs a secure client- side cross-user deduplication technique, which give license to a user to skip the uploading process and gain the ownership , when the other owners have uploaded the same data into the cloud server. As per foremost of our knowledge, none of the existing dynamic PoSs can bear this technique. In this paper, idea of deduplicatable dynamic proof of storage is proposed and also proposed an efficient construction called as DeyPoS, to achieve the dynamic PoS and also secure cross-user deduplication, concurrently. By taking the challenges of structure diversity and private tag generation, we bulid a novel tool called Homomorphic Authenticated Tree (HAT). It helped us to verify the security of our creation, and also the theoretical analysis and experimental result showed that our creation is efficient.

Provable ownership of files in deduplication cloud storage Author Name: Chao Yang1,2, Jian Ren2* and Jianfeng Ma1 Description: With the rapid usage of cloud storage services, a large amount of data is being saved at remote servers, so a latest technology, client- side deduplication, which is used for storing only one copy of repeating data, is prefered which is used to identify the clients deduplication and also helps to store the bandwidth of uploading copies of already current files to the server. It was recently found, that this promising technology is vulnerable to some new kind of attack in which by learning just a small piece of information in the file, that is its hash value, an attacker is able to acquire the entire file from the server. In this paper, inorder to resolve this problem, we prefer a cryptographically secure and efficient scheme for a client to validate to the server his ownership on the basis of actual possession of the entire original file instead of only partial information about it. The scheme that we are using utilizes the technique of spot checking in which the client only needs to access small portions of the original file, dynamic coefficients and randomly chosen indices of the original files. This huge security analysis shows that the suggested scheme can help to produce provable ownership of the file and it also maintains big detection chances of client misbehavior. Both performance analysis and simulation result shows that our suggested scheme is much more efficient than the existing schemes, especially it helps to reduce the burden of the client.

V. SCREENSHOTS

- **Home Page**

- **User Register**

- **User Login**

- **Upload File**

- **Verify File**

VI. CONCLUSION

Interoperability between hospitals doesn't solely facilitate in rising patient security and quality of care however it additionally reduces time and resources that square measure pay on formatting conversion. ability is most significant that the amount of hospitals that square measure collaborating in go will increase if single hospital doesn't facilitate ability, the remaining hospitals square measure required to convert formatting of their clinical information to exchange knowledge for go. Once the amount of hospitals that doesn't facilitate ability, complication for go is enlarged in proportion. The advantage of API service as our at the quantity of resources that hospitals need to apportion for ability is barely minimum. Therefore, providing system that helps ability by looking forward to a cloud computing platform could also be smart and that we offer the QR code security for patients knowledge that hold on on cloud.

REFERENCES

[1] Z. C. Wen, J. M. Luo, H. J. Chen, J. X. Meng, X. Li, and J. Li, A verifiable data deduplication scheme in cloud computing, in Proc. Int. Conf. Intell. Netw. Collaborative Syst., 2014, pp. 8590, doi:10.1109/INCoS.2014.111.

[2] J. Li, Y. K. Li, X. F. Chen, P. P. C. Lee, and W. J. Lou, A hybrid cloud approach for secure authorized deduplication, IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 5, pp. 12061216, May 2015, doi:10.1109/TPDS.2014.2318320.

[3] P. Meye, P. Raipin, F. Tronel, and E. Anceaume, A secure twophase data deduplication scheme, in Proc. HPCC/CSS/ICESS, 2014, pp. 802809, doi:10.1109/HPCC.2014.134.

[4] J. Paulo and J. Pereira, A survey and classification of storage deduplication systems, ACM Comput. Surveys, vol. 47, no. 1, pp. 130, 2014, doi:10.1109/HPCC.2014.134.

[5] Y.-K. Li, M. Xu, C.-H. Ng, and P. P. C. Lee, Efficient hybrid inline and out-of-line deduplication for backup storage, ACM Trans. Storage, vol. 11, no. 1, pp. 2:1-2:21, 2014, doi:10.1145/2641572.

[6] Z. Yan, X. Y. Li, M. J. Wang, and A. V. Vasilakos, Flexible data access control based on trust and reputation in cloud computing, IEEE Trans. Cloud Comput., vol. PP, no. 99, Aug. 2015, doi:10.1109/ TCC.2015.2469662, Art. no. 1..

[7] P. Meye, P. Raipin, F. Tronel, and E. Anceaume, A secure twophase data deduplication scheme, in Proc. HPCC/CSS/ICESS, 2014, pp. 802809, doi:10.1109/HPCC.2014.134.

[8] J. Paulo and J. Pereira, A survey and classification of storage deduplication systems, ACM Comput. Surveys, vol. 47, no. 1, pp. 130, 2014, doi:10.1109/HPCC.2014.134.

[9] Y.-K. Li, M. Xu, C.-H. Ng, and P. P. C. Lee, Efficient hybrid inline and out-of-line deduplication for backup storage, ACM Trans. Storage, vol. 11, no. 1, pp. 2:1-2:21, 2014, doi:10.1145/2641572.

[10] M. Fu, et al., Accelerating restore and garbage collection in deduplication-based backup systems via exploiting historical information, in Proc. USENIX Annu. Tech. Conf., 2014, pp. 181192.

[11] M. Kaczmarczyk, M. Barczynski, W. Kilian, and C. Dubnicki, Reducing impact of data fragmentation caused by in-line deduplication, in Proc. 5th Annu. Int. Syst. Storage Conf., 2012, pp. 15:115:12, doi:10. 1145/2367589.2367600.

[12] M. Lillibridge, K. Eshghi, and D. Bhagwat, Improving restore speed for backup systems that use inline chunk-based deduplication, in Proc. USENIX Conf. File Storage Technol., 2013, pp. 183198.

[13] L. J. Gao, Game theoretic analysis on acceptance of a cloud data access control scheme based on reputation, M.S. thesis, Xidian Univer-sity, State Key Lab of ISN, School of Telecommunications Engineering, Xian, China, 2015.

[14] Z. Yan, X. Y. Li, M. J. Wang, and A. V. Vasilakos, Flexible data access control based on trust and reputation in cloud computing, IEEE Trans. Cloud Comput., vol. PP, no. 99, Aug. 2015, doi:10.1109/ TCC.2015.24696 62, Art. no. 1.

Secured Group Data Sharing in Cloud Computing

[1] Pooja Katurde, [2] Rameshwari Konda, [3]Trupti Mohite, [4] Nisha Melkunde
[1,2,3,4]Student, Zeal College of Engineering and Research, Narhe, Pune, India
E-mail: [1]poojakaturde12@gmail.com, [2]rameshwarikonda1997@gmail.com,
3truptimohite@gmail.com, 4shreemelkunde@gmail.com

ABSTRACT

Secure data access and effective data sharing in public cloud is an problem to solve. This paper focuses on the secure data sharing and storage. It will provide high security and efficiency. In this mechanism, group members can communicate with each other anonymously. Group members will use a common conference key to share and store data securely on cloud. Note that: An elliptic curve cryptography is utilized for secured key generation.

Keywords - Group Data Sharing, Anonymous, Elliptic Curve Cryptography(ECC).

I. INTRODUCTION

In the cloud computing the data sharing is the technique that allows the user to access the data over the cloud. Cloud system can be used for the data sharing facilities. This can provide more benefits to the users and the organization where data sharing is done. With various users from different organizations shares data in the cloud, time and cost requires less as compared to manually exchanging of data. The Cloud provide to many privacy and security attacks for the data which is share. Cloud computing not only provides limitless computing resources but it also provides limitless storage resources to the users. The cloud storage is essential part in the cloud computing. The simple solution provided by existing system is to users data confidential from the untrusted server is by encrypting the data, before uploading it on cloud.

Our main aim is to achieve the anonymous data sharing and access in cloud computing. To achieve this we are using two algorithms: One is AES (Advanced Encryption Standard) and another is ECC (Elliptic Curve Cryptography).

II.LITERATURE REVIEW

Block design -based Key agreement for Group Data Sharing in Cloud Computing paper introduces block design based key agreement protocol. We can add multiple participants in the group. In which flexibly extend the number of participants in the cloud. In these paper we provide the flexibility. But the drawback of this paper is we can not provide the more properties like anonimity, traceablity. New Algorithms for secure Outsourcing of modular Exponentiations paper describes encryption and decryption by using the outsource-secure Cramer shoup encryptions. The disadvantage of it is, it will perform some other expensive operations such as scalar operations like multiplications. The Secure

Attribute based data sharing for resource limited users in cloud computing paper aims to tackle the computation efficiency and security issues of the data sharing.

III. RELATED WORK

In order to overcome the vulnerabilities, we have proposed an effective access control for cloud computing. It provides data confidentiality, scalability. So, each data file is encrypted with a random key and subsequently the random key will be encrypted by the KA-ABE.A secrete key is maintained by the group manager which is distributed to the authorized users and can be used to decrypt the data. Group manager has only the right to delete a data file. As earlier the scheme is only designed specifically for the one to many communications. Whereas a number of studies has been proposed to protect user‟s privacy. Here, both anonymity and traceability are well supported by employing the group signature technique. The key management System falls into two categories one is key generation & distribution.

The second is the key agreement where all the members in the determine a common conference key. It provides Anonymity as when a user or a group manager wants to give the access of the data only to the selective users of the group that action will be anonymous to the other users. An encrypted key is sent to those users, that key and the key in the database is compared and then only the data is accessible to the users. Also it provides Traceability as when the data is accessed by any user it is notified to the Group manager. In the cloud environment key distribution may be vulnerable since centralized controller is the bottleneck of the system. Moreover, the large amount of computation for a common conference key may effect on centralized controller. Many researchers are trying to design of data sharing schemes in the cloud. But even though the problems need to be resolved. In this paper, we focus on constructing an efficient and secure data sharing scheme that can support anonymous and traceable group data sharing in cloud computing. Moreover, many-to-many group data sharing is supported in the proposed scheme.

IV. THE PROPOSED SCHEME

The presented scheme can be applied to group data sharing in cloud computing with high security and efficiency. Our scheme is divided in 3 parts: Encryption and decryption, Key generation, file access. The proposed system is that the manager or the group members can share the file in the group. But if the group members wants to share the file then they must be register as a manager first and then they can upload the file. In addition we can create the group on the spot means we have all the list of the member who is register in system as members then we select the group members at the time of uploading the file. Also if the manager wants to delete the uploaded file then he must ask or take the permission of the group members. Vice versa if the group member wants to delete the file then they will take permission of the manager.

A. Encryption and Decryption

Advanced Encryption Standard is a symmetric key algorithm which is used for encryption and decryption. AES uses different size data inputs as 128 bits, 192 bits and 256 bits.It provides different key lengths and processes the multiple rounds of operations.

Algorithm 1:

State=M AddRoundKey(State,&w[0]) for i=1 step 1 to 9
subBytes(state) shiftrows(state) mixcolumns(state,&w[i*4]) end for
subbytes(state) shiftrows(state) AddRoundKey(state,&w[40])

B. Key Generation

Elliptic Curve Cryptography is public key cryptography which is used to generate key. ECC provides security and also generates smaller size key. ECC is more powerful than RSA because of its features like faster computations, low power consumption and saves memory etc.

Algorithm 2:

1. Select a random number „a" within range of n.
2. Generate public key Q=a*P.

P is the point on the curve. Q is public key and „a" is private key.

3. Encryption:- Consider M is the point on the curve.

C1= a*P C2= M+k*Q

4. Decryption:- M= C2-a*C1

C. File Access

Group member will request for data to the manager. The manager sends authorized information to the cloud. One secret key will be generated and sent to the group member. With this member can access data from cloud.

V. SYSTEM ARCHITECTURE

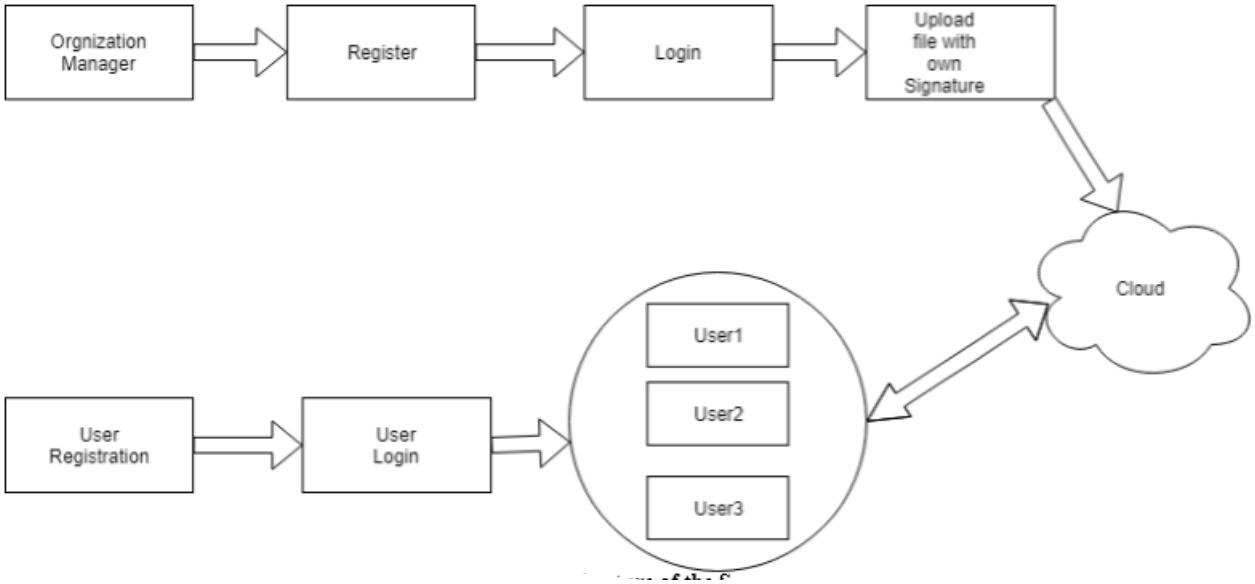


Fig. 1. Architecture of the System

This system is useful for the different organization but we consider this system for the business organization . In our system we have three modules first is OWNER , second is CLOUD, and third is CLIENT.

OWNER: firstly owner or any member of the organization register to the system and then upload the file with own signature using ECC and use AES algorithm for the file encryption. Owner manage the group members and also manage the authorizing the group members.

CLOUD: is used for the data storage .In cloud user can store the unlimited data efficiently and conveniently. Cloud also provide the sharing of data service .Cloud is used because cloud cannot delete or modify the users uploaded data .

CLIENT : Same as owner client register to the system if the owner send the file in group then it is visible to that group members otherwise another members of that system are anonymous to that process. Using AES algorithm and the using key the group member can download that encrypted file .

V. CONCLUSION

We provide the secure data transmission of the data. The group data sharing is done with the help of group signature technique. The signature is generated by using the Key generation method. In addition, our scheme can support the traceability of user identity in an anonymous environment. And also we sends the message to the admin that how many users access the file.

FUTURE SCOPE

Our main aim is to securely save the data on the cloud and access it securely. This can be used in the business organizations . As efficient access control is achieved with respect to group signature technique. Like in the business organization there are various departments so any confidential file can only be sent to the selected users and this will be anonymous to the others.

REFERENCES

[1] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re- encryption scheme for secure data sharing in a cloud environment," Inf. Sci., vol. 258, pp. 355–370, Feb. 2014.

[2] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 9, pp. 2386–2396, Sep. 2014.

[3] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute- based data sharing for resource-limited users in cloud computing," Comput. Secur., vol. 72, pp. 1–12, Jan. 2018, doi: 10.1016/j.cose.2017.08.007.

[4] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," IEEE Trans. Depend. Sec. Comput., to be published, doi: 10.1109/TDSC.2017.2725953.

[5] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," IEEE Trans. Depend. Sec. Comput., vol. 12, no. 5, pp. 546–556, Sep. 2015.

Replacing Phone Storage with Direct Cloud Computation System

[1] Ankita Aditya, [2] Meet Shah, [3] Tripti Jain

[1,2]Department of Computer Science and Engineering, Pesit Bangalore South Campus, Bangalore, India

[3]Department of Electronics and Communication Engineering, Pesit Bangalore South Campus, Bangalore, India

E-mail: [1]ankita.aditya20@gmail.com, [2]meet19061999@gmail.com, [3]triptijain2207@gmail.com

ABSTRACT

- In this technical era of computation, around 83.5 percent of population use Gmail, Dropbox, Netflix, and yes, the interesting one google assistant, etc. All these trending applications, leverages cloud computing to touch the heights of its advantage. The expanded power of computation and the capacity of the cloud enlightens the current phase by enabling to store information according to user preferences. It provides customized and simplified solutions and products based on the preferences of users. And the magical wand which uplift the cloud computing features is it's fast and efficient storage system. Well, many a times the user has lost data by some sort of accidental deletion. Also many a times we get notification to update your databases. The users Did not invest their money in deploying local system. Here comes our notion to enhance this system and boost up the computing system. The system which we are proposing can definitely put a remarkable change in the industry. The backbone of the system is based on the mathematical structure, graph theory. It involves providing a direct link for data flow to the main cloud sever having a temporary buffer.

Keywords - Cloud Computing, Efficient Storage System, Simplified Solutions, Backbone, Graph Theory.

I. INTRODUCTION

"I don't need a hard disk in my computer if I can get to the server faster, because it is always about how you do computing not where you do computing" It's a famous saying of Steve Jobs, Co-founder, CEO and Chairman of Apple Inc. which will ultimately change your notion regarding computing sector. In this technical era of computation, around 83.5 percent of population use Gmail, Dropbox, Netflix, and yes, the interesting one google assistant, etc. All these trending applications, leverages cloud computing to touch the heights of its advantage. Have you ever thought about it, why it is so? Well, the answer is pretty obvious and most of you might be knowing the reason, it is only because of efficient storage and fast access computing system, i.e. cloud computing. The expanded power of computation and the capacity of the cloud enlightens the current phase by enabling to store information according to user preferences. It provides customized and simplified solutions and products based on the preferences of users. And the magical wand which uplift the cloud computing features is it's fast and efficient storage system, and here comes our notion to enhance this system and boost up the computing system. Well, have you lost your data by some sort of accidental deletion? Did you also get notification

to update your databases? Did you also invest your money in deploying local system? Well, if you have gone through all these phases then the system which we are proposing can definitely put a remarkable change in the industry.

Workflow: The backbone of the system is based on one of the mathematical structure i.e. graph theory.

In this upgraded system we are trying to provide a direct link to the main cloud sever having a temporary buffer as an intermediate platform. Suppose a user is framing a document for his office chores, then all the data which he will type in textual format will get stored in that buffer area and keeps updating its allocation space based on the size of the file he is creating. As soon as the work get finished, it will get uploaded to the cloud. To retrieve the data, the user has to sign in to his/her cloud account via captive portal and then they can access their data easily. Hence, this computation system helps in enhancing the processor's speed eliminates the problem of "lack of storage".

II.STATISTICS

According to arecent survey from, to upload a video via the a broadband connection, we require nearly 300 seconds of time. (1-5 Mbps upload speed) On an average it will take in between 30 seconds to max of 3 minutes to upload. Internet connection is the major factor which affects the uploading speed, besides this, size of the file to be uploaded and the quality also plays a significant role in the uploading process.

If users want to upload a file of size nearly 2GB, or any file of duration approx 2 hrs, via broadband connection then it will take 20 minutes with a 5Mbps upload speed or 90 minutes with upload speed of 1MBPS.

To upload a file of size nearly 4GB, or any file of duration ap prox 4 hrs, via broad band connection then it will take 60 minutes with a 5Mbps upload speed or 5 to 6 hrs with upload speed of 1MBPS.

Any device having a 3G connection can take around twice as long it takes to upload the content as the 1Mbps of speed mentioned.

Thus, we calculated the overall time required to upload 1GB, 100GB, and 1000GB (or 1TB) of data using normal upload speed will be 1Mbps, 2Mbps, 5Mbps, 10Mbps, 20Mbps, and finally, just hits 1000Mbps (1Gbps) drastically , which are the speeds commonly used for Google Fiber advertises.

	1 GB	100 GB	1000 GB
1Mbps	2.5 hrs.	10 days	99 days
2Mbps	1.25 hrs.	5 days	50 days
5Mbps	28 min	2 days	20.3 days
10Mbps	14 min	1 day	10.2 days
20Mbps	7 min	12 hrs.	5.1 days
1000Mbps	8 seconds	1minutes	2.5 hrs.

Our computations are rounded off to the nearest timephase and include 10 percent of the connection overheaded.

But the system that we propose involves all the data getting stored in the buffer area and keeps updating its allocation space based on the size of the file he is creating. As soon as the work get finished, it will get uploaded to the cloud. To retrieve the data, the user has to sign in to his/her cloud account via captive portal and then they can access their data easily. Hence, this computation system helps in enhancing the processor's speed eliminates the problem of "lack of storage".

So this default uploading to the cloud eliminates the uploading of large amount of data in one go and also the issue of large amount of upload time and lack of storage

III. ANALOGY WITH LINUX TERMINAL

In analogy to the system which we are proposing, the mobile phone which we are using will act as a terminal. As in Linux system, we have terminal commands to navigate the system directories, files, and folders and access all the data which are present, in the similar manner our phone will act as that terminal spot from which the data can be accessed. So, users would not have to face the problem of draping. The most powerful advantage of having this system in phone is that, it provides a great Graphical User Interface (GUIs). Users don't have to do anything manually; it does multi-tasking. This system keeps track of your data so users don't have to worry about any accidental loss of data, as the computation takes care of the backup process also. Hence, this computational system makes the phone efficient, cost-effective and user friendly.

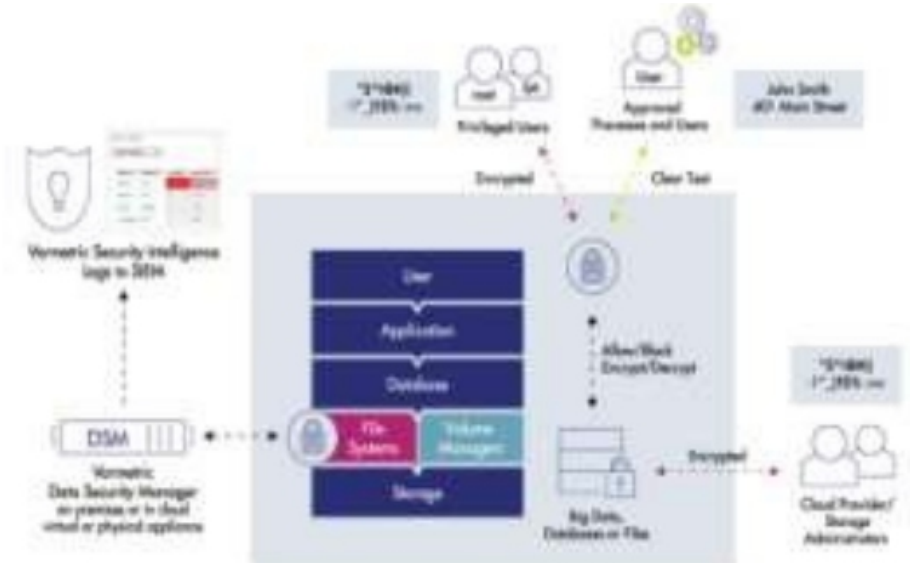
IV. SECURITY MODELLING

The computational world has becoming more and more complex day by day. The main thing to be focused on the data privacy.

We are proposing a new advanced security modelling system for this. In this security model, the user will create a local repository i.e. local user database type of platform, then it will redirect the path to establish a temporary security validation, this validation certificate is now used by the user for authentication purpose over a period of time. This authentication steps include the user name, local host name, user id, start and stop time and other security attributes to access. Whenever user wants to use the available resources on the cloud provided by the service provider, they need to go for manual authentication process. This process will take place between the user and the application system. In case if the security certificate is expired, then a local security algorithm will run at the backend side and it is mapped with the specific application user wants to run.

As per the requirements of the user, the cloud computational system will generate the list of accessible resources and pass it to the user agent as a GUI interface. To connect with the specific cloud services, API user agent will come into pictures Through security API user agent connects specific cloud services.

The model focuses on the following components of the security:
I) Security validation (ii)Protection of data(iii)security of data and its services (vi)threats and attacks detections.



V. SECURITY VALIDATION

This part of computation ensures the accuracy and services of the data on the cloud. The significance of security module in the proposed cloud computing position is accessible by various customers and service providers which want to make use of or provide plenty of services and applications in the practical world. The providers of cloud computing prove the users that the services and data of the computation are valid, suppose for example, appropriate signature algorithms. This protection part will also provide work for technical protection such as One Time Password and 2FA [1] [22].

Security Policies: These are the basis of a resonance system for completion. Most organizations implement security solutions without framing any foundation of security policies, and social standards on firewall.

Advanced Encryption Standard (AES): AES is a security algorithm published by the National Institute of Standards and Technology (NIST). It is the most adopted algorithm based on symmetric key encryption system. It performs computation on bytes rather than bits, treats 128 bits of plaintext block as 16 bytes. The packet of 16 bytes' data is converted into 4*4 square matrix. It performs computation on the entire block of data by using substitutions. The key size used for an AES cipher gives the number of transformation rounds used in the encryption process. Following are the keys and number of rounds possible:

- 10 rounds for every frame of 128-bit keys.
- 12 rounds for every frame of 192-bit keys.
- 14 rounds for every frame of 256-bit keys.

VI. ADVANTAGES

As said by MR EDWARD TELLER, A Hungarian- American theoretical physicist known as THE FATHER OF HYDROGEN BOMB: "The science of today is the technology of tomorrow". Believing in Mr. Edward Teller, we believe the science of our proposed system can be the technology of tomorrow

There are numerous advantages of cloud computing.

1) Universal Information Access:

The user does not need to take the documents along with him as the data stay in the cloud and can be accessed whenever there is an internet connection and a computer or even mobile in this advanced technical generation. The documents are instantly available from wherever the user is.

2) Latest Version Availability

The document edited at home is updated document at work. The biggest asset of cloud is it always hosts the latest version of the data as long as the user is connected giving security by keeping the user's data out of danger of having an outdated version

3) Instant Software Updates

Updates happen automatically and is available to the user the next time the user logs in to cloud. So the user need not to pay for upgrade or download of the latest version making it cost effective as well.

4) Improved document format compatibility

There are less format incompatibilities when everyone uses cloud as their primary tool for sharing data and data backup.

VII. BENEFITS OF PROPOSED SYSTEM

The root of the proposed system is cloud computing so the system automatically inherits all the advantages and benefits of cloud computing.

Along with the advantages of cloud computing there are some added benefits that makes the proposed system more feasible and advantageous

1) The proposed system eliminates the need of high priced and high powered devices to run cloud computing's applications
2) Since application runs on cloud, the phone doesn't require the memory space that is demanded by traditional system reducing cost by eliminating storage responsibility from the phone.
3) As no programs have to be loaded or files have to be saved in the memory, less memory makes more efficient processor and more improved performance.
4) Easier group collaboration provides the proposed system with another and important asset as multiple users can collaborate easily and efficiently on documents and projects

Amazon's Elastic Compute Cloud(EC2) And Simple Storage Solution(S3) are some examples of web companies exploiting the fact that they have data storage capacities that can be hired out to others allowing data stored remotely to be temporarily cached on PC, mobile phones or other Internet – linked devices.

VIII. LIMITATIONS

1) Features may be limited like for example you can do a lot more with gallery in your phone rather than online terminal based offering.
2) It can be a slow process. Even with a fast connection, web based application and online accessing on cloud can sometimes be slower than accessing similar data on your phone.
3) Security is another major limitation as stored data is on cloud and it may result in insecure data and unauthorized access to data.
4) Theoretically data on cloud is always safe replicated across multiple machines. But on the off chance if the data goes missing, there is no physical data backup.
5) It doesn't work on low speed internet connection making it difficult to work in remote areas.

IX. SCOPE IN FUTURE

The main issue of today's storage system can be easily handled by this system. Data encryption and integrity safeguards the user from unauthorized access to the portal. This works on remote auditing mechanism, which enables the user to store their data in any of the remote storage location. As our proposed system deals with the confidentiality, integrity and the availability which are encapsulated in a CSP Service level contract agreement to the customers. This system deals with various type of fault tolerance mechanism, which helps to improve the functionality and efficiency of the system. Also with google and other giant IT companies coming up with high speed connection in Gbps, the system we propose can be the best fitted storage system in the market. Also the feature of increasing the processing speed is itself a boon that can serve as the next big thing in the future. Therefore, there is high possibility that this model can replace and dominate the debility of various previous models in the market. In future, it has all the features to give a new direction to the storage system in the field of computation and can give spark to its efficiency and reliability. Thus the proposed direct computing system has great scope and can show a new direction for storage in the information and technology industry.

X. CONCLUSION

The main issue of today's storage system can be easily handled by this system. Data encryption and integrity safeguards the user from unauthorized access to the portal. This works on remote auditing mechanism, which enables the user to store their data in any of the remote storage location. As our proposed system deals with the confidentiality, integrity and the availability which are encapsulated in a CSP Service level contract agreement to the customers. This system deals with various type of fault tolerance mechanism, which helps to improve the functionality and efficiency of the system. Also with google and other giant IT companies coming up with high speed connection in Gbps, the system we propose can be the best fitted storage system in the market. Also the feature of increasing the processing speed is itself a boon that can serve as the next big thing in the future. Therefore, there is high possibility that this model can replace and dominate the delibity of various previous models in the market. In future, it has all the features to give a new direction to the storage system in the field of computation and can give spark to its efficiency and reliability. Thus the proposed direct computing system has great scope and can show a new direction for storage in the information and technology industry.

REFERENCES

[1] https://www.researchgate.net/publication/319183514_STUD Y_ON_SECURITY_MODEL_IN_CLOUD_ COMPUTING
[2] TED talk by John Easton, https://youtu.be/8H3WaMzDiTo
[3] http://www.thecloudcomputing.org/2018/research.html
[4] Cloud Computing by Dr Kumar Saurabh

Mitigating Cloud Security Threats using Cloud Access Security Brokers

[1] Shabnam Kaur, [2] Rajandra Gupta
[1,2]KMS College of IT & Management, India
E-mail: kmscollegedasuya@gmail.com

ABSTRACT

The importance of Network cloud is increasing and it is accepting a developing attention in the scientific and industrial communities. Cloud Computing has already started to revolutionize the method we store and access data. Security issues in Network cloud computing are some of the biggest concerns surrounding the technology. To promote cloud computing in a wide range of apps, security issues required to be resolved. Data breaches of cloud services are increasing every year due to hackers, who is always trying to exploit the security vulnerabilities of the architecture of cloud. Cloud Access Security Brokers (CASBs) are one of the fastest growing security technologies, today because they provide cloud service visibility, data security, threat protection, and compliance. CASBs are an effective and easy way to mitigate the top cloud security threats and security practitioners look to trusted CASB suppliers as key accomplices to help exhort on key cloud security decisions. The research is to implement information dispersal algorithms to prevent Data Breaches using Cloud Access Security Brokers.

Keywords - Network cloud, Security Issues, Cloud Access Security Brokers (CASBs), Information Dispersal Algorithm, Data Breaches.

I. INTRODUCTION

We are rapidly moving towards a Cloud majority world. Be that as it may, Cloud adoption has likewise presented another set of risks, both inner and external. The cloud access security broker can provide stronger cloud protection at a lower cost than traditional security processes and tools. Multiple types of security policy enforcements required:

- Authenticated access
- Single sign-on
- Data loss prevention
- IP restriction
- Device restriction and device profiling
- Geographical restriction
- Time zone restriction
- Early Malware detection and prevention

A CASB can be used to prevent data breaches. A CASB behaves as a guard, permitting the organisation to extend the reach of their security policies beyond their own infrastructure. A cloud access security broker is on-premises or cloud based programming that sits between cloud service clients and cloud

applications, and screens all action and authorizes security policies. A CASB can offer an assortment of services, including however not constrained to monitoring user action, warning administrators about possible risky actions, upholding security policy consistence, and naturally preventing malware. According to Gartner, by 2020, 85% of large enterprises will use a cloud access security broker solution for their cloud services, which is up from less than 5% in 2015.There are many different implementations and types of Cloud Access Security Brokers (CASBs). Enterprises require sophisticated capabilities to secure their cloud footprint. A CASB should:

- Protect your entire cloud footprint, including IaaS, SaaS, and PaaS
- Provide optimal performance with no user impact
- Integrate with your existing security investments through a simple deployment

II. CASBs ARE MANDATORY FOR CLOUD

The rise of SaaS - pervasive According to Cisco Global Cloud Index reports, 58% of all cloud remaining tasks at hand will be SaaS. Indeed, even the financial services sector—since quite a while ago considered a laggard in SaaS appropriation—now utilizes SaaS for 42% of its applications. Numerous SaaS applications have constrained visibility and control choices. SaaS reception is getting to be unavoidable in enterprises, which compounds the dissatisfaction of security teams searching for visibility and control. As a primary concern the SaaS Security Gaps, this paper depict, at a high-level state, four mainstays of expected CASB usefulness: visibility, consistence, information security and threat protection.

Adoption of IaaS is growing rapidly IaaS is considered the fastest-growing cloud services market. Many enterprises are moving their entire infrastructure to the cloud.

Erode in Manual Approaches The people-centric approaches won't work. In practical terms, accomplishment with this methodology is about inconceivable as a result of the time and cost related to manual forensics and the lack of skilled labor. Instead a CASB does it for you—saving time and eliminating human error. A CASB uses machine learning and automation to provide a secure and compliant use of cloud services across multiple providers and technologies. For example, a CASB should include integration with your existing enterprise security solutions such as security information and event management (SIEM), identity as a service (IDaaS), and next generation firewalls (NGFW).

III. DATA STORAGE SECURITY SCHEMES

Different schemes that ensure security of data stored in servers are explained as follows:

In 1993, Cloud Framework Security (CFS) was presented which empowers security of information very still in the system. CFS has been accounted for in [1]. Cryptographic document systems are customized toward single-client workstations and depend on client supplied passwords for information encryption [2]. This method is not great for Cloud frameworks as Cloud frameworks include dispersed nature of system of servers where information is to be put away and these servers will be utilized by various clients. Additionally, utilization of passwords for information security is firmly precluded; on the grounds that, most regular assault on such frameworks is beast constrain assault particularly because of clients' propensity of keeping passwords basic and essential [3,4,5]. Hence this strategy is not recommended.

In [6], another scheme for dividing secret into shares and reconstructing the secret back from its shares is explained. In this scheme, additional information is added in the shares of the secret. This additional information is a message and the message is retrieved along with file (secret) on reconstructing the file (secret).

Shamir's algorithm: In 1976, a simple (k, n) threshold scheme was explained and this scheme is reported in. According to this scheme data is divided into n pieces and up to k pieces are required to get data. k-1 pieces will not reveal any information about data (secret). This scheme is based on polynomial .

interpolation: given k points (x_i, y_i) with distinct x such that for each x, there is one and only one polynomial q(x) of degree k-1 such that $q(x_i) = y_i$ for all i. supposes data D is a number (ASCII value). To divide it into pieces D_i, a random polynomial $a_0 + a_1 x + \ldots a_{k-1} x^{k-1}$ of k-1 degree is selected in which $a_0 = D$.

Shortcomings of this scheme are as follows:

a) Size of each piece is approximately equal to the size of data. Hence this method is space inefficient.

This method does not solve the problem of vulnerability of integrity in AWS [7].

Rabin's efficient dispersal of information for security, load balancing, and fault tolerance: In [8], another scheme is explained for dividing data into pieces/shares. In this scheme, the way of dividing secret into pieces is different from [9]

Purposes of this arrangement are according to the following:

a) Size of all of the mystery is little space which makes it effective.

b) If any piece of data is adjusted during its keep focused, examination will help in making sense of which piece is changed.

Shortcomings of this arrangement are following:

a) Management and limit of secret keys.

b) Also, affirmation of the key requires learning of the secret key, however, then whoever can read the data can in like manner adjust it without being recognized.

IV. PROPOSED METHOD

To construct the security of data sent away in servers of Cloud organization suppliers and to perform destinations of this investigation, the security is proposed for Cloud Access Security Brokers (CASBs). In the proposed computation, two arrangements have been used and one of them is 'Information Dispersal figuring (IDA)'. For executing proposed work, some data is divided into the inside the shares. The usage of IDA in the proposed plan helps in guaranteeing security of information. A second course of action that has been utilized as a part of the proposed figuring is security key. Keys help in guaranteeing validity of data. This key is created by using RSA cryptography. Both the public and private keys can encode a data, the inverse key from the one used to scramble a message is utilized to decode it. This property is one motivation behind why RSA has turned into the most broadly utilized awry algorithm. The steps followed in the proposed work are as per the following:

Steps:

1. In the initial step, File (secret to be put away) or message is taken from the user.
2. In the second step, the document is divided into shares and after that encryption of the shares is performed in the third step.
3. In the fourth step, every offer of the record and its separate key from the picture is sent to various servers. The ids of the servers and names of documents containing shares of record and its particular key are put away in the Cloud Access Security Broker (CASB).
4. In request to remake the document, the client enters the record name and key from any customer framework. These subtle elements are looked from the Cloud screen.
5. On getting the shares, 'Recreation of record or message' is executed and the document (secret) or the message is recovered using the information provided by (CASB)
6. A message is sent to client and client checks if the message got is same as the duplicate of message with him.
7. If document or message is right, then the record is conveyed to the customer.

Test Results

For the tests, certain attacks have been generated like the way attacks are performed in Cloud systems. These attacks will confirm that objectives have been achieved by the proposed information dispersal algorithm by Cloud Access Security Broker.

Recovery of Data Even If Some Number Of Servers Are Damaged

The servers attacked by hacker can vary. It can be one server or more than one server. Different attacks have been generated to verify whether the first objective of this research "Recovery of data even if some (within a limit) number of servers is damaged" has been achieved or not. As studied earlier, at least, k servers are required to reconstruct the file from its shores, two tests have been performed.

For instance, we have taken sample.txt file having size of 815 bytes. We have divided the files into the shares of 200 characters each. So we get 5 shares. These shares are then encrypted using the keys. All information related to shares is maintained by Cloud Access Security Broker (CASB).

For retrieval of the sample.txt file from the servers, all the shares are concatenated after decryption. The file retrieved has the size 815 bytes. Again for retrieval of the file CASB is responsible for information related to the file.

V. RESULTS CONCLUDED FROM DIFFERENT ALGORITHMS

Parameters / Algorithms	Recovery of data	Integrity of data	Confidentiality of data
Shamir's Algorithm [7]	✗	✗	✓
Distributed Fingerprints and Secure Information Dispersal [8]	✓	✓	✓
A Tree Based Recursive Information Hiding Scheme [9]	✗	✓	✓
PROPOSED ALGORITHM	✓	✓	✓

According above results, In Shamir's Algorithm the data recovered is not as per saved on the server, confidentiality is maintained. Using this algorithm the integrity is violated. , In Tree Based Recursive Information Hiding Scheme the data recovered was not as saved on the server, confidentiality and

integrity was maintained. In the proposed algorithm, data recovered is same as saved on the server and Integrity and confidentiality is maintained. It is important to maintain confidentiality, integrity and recovery of complete data.

VI. CONCLUSION

The cloud access security broker (CASB) can help to move to the cloud safely. It protects the cloud users, data, and apps. This paper provides a simulation tool to manage the risks in the cloud app ecosystem. It is important to develop a comprehensive information security program and train them to monitor and research anomalous activities. The proposed paper is maintaining the confidentiality, integrity and recovery of data stored in the cloud using CASB cloud service.

REFFERENCES

[1] M. E. Smid and D. K. Branstad, "The data encryption standard: Past and future," Proc. IEEE, vol. 76, no. 5, pp. 550-559, May 1988

[2] Emily Maltby, "Small companies look to Cloud for savings in 2011," http://online.wsj.com/article/SB10001 4240529702035132 04576047972349898048.html, December 29, 2010.

[3] Lenk, M. Klems, J. Nimis, S. Tai, F. Karlsruhe, and T. Sandholm, "What's Inside the Cloud? An Architectural Map of the Cloud Landscape," in Proc. of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, IEEE Computer Society, pp. 23–31, 2009.

[4] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "A View of Cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[5] [John, "Top 10 Enterprises in the Cloud," http://www.johnmwillis.com/other/top-10-entperises-in- the-Cloud/, Jul. 13, 2008.

[6] "Google App Engine," http://en.wikipedia.org/wiki/Google_App_Engine.

[7] Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[8] H. Krawczyk, "Distributed Fingerprints and Secure Information Dispersal," in Proceedings of the 12th annual ACM symposium on Principles of distributed computing, 1993

[9] Parakh, A. and Kak, S. 2010 "A Tree Based Recursive Information Hiding Scheme" proceedings of IEEE ICC 2010 – Communication and Information System Security Symposium (ICC"10 CISS"), May 23-27, Cape Town, South Africa.

[10] Gartner: The Growing Importance of Cloud Access Security Brokers - http://www.computerweekly.com/ news/2240223323/Clou d-access-brokers-top-security-technology-says-Gartner

[11] Gartner: Emerging Technology Analysis: Cloud Access Security Brokers - http://www.ciphercloud.com/ 2014/09/30/public-cloud- security-demands-cloud-access-security-broker-casb/

[12] https://www.netskope.com

[13] Medina, A. Lakhina, I. Matta, and J. Byers, "BRITE: An Approach to Universal Topology Generation," in Proc. of MASCOTS '01, August 2001.

[14] Bitglass: The Definitive Guide to Cloud Access Security Brokers

[15] CipherCloud looks to stay at the head of the cloud security class

[16] Ciphercloud: 10 Minute Guide to Cloud Encryption Gateways

[17] Ciphercloud: Cloud Adoption & Risk Report in North America & Europe – 2014 Trends

[18] NetworkWorld: How the cloud is changing the security game

[19] Adallom: The Case For A Cloud Access Security Broker

[20] Adallom: Cloud Risk Report Nov 2014

[21] Check Point Capsule and Adallom Integration

[22] HP - Adallom: Proven Cloud Access Security Protection Platform

[23] Adallom : to Offer Comprehensive Cloud Security Solution for Businesses With HP

[24] PingOne - Skyhigh: PingOne & Skyhigh Cloud Security Manager

[25] ManagedMethods: Role of Enterprise Cloud Access Security Broker

[26] Standing at the Crossroads: Employee Use of Cloud Storage.

[27] Cloud Computing: Security Threats and Tools

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).
2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);
3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);
4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Address of the Editorial Office:

Enriched Publications Pvt. Ltd.
S-9,IInd FLOOR, MLU POCKET,
MANISH ABHINAV PLAZA-II, ABOVE FEDERAL BANK,
PLOT NO-5, SECTOR -5, DWARKA, NEW DELHI, INDIA-110075,
PHONE: - + (91)-(11)-45525005

Notes: