IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Division of Data in Cloud for Optimal and Security using Fragment Placement Algorithm.

Ajay Bhandare[1], Pallavi More[2], Mr.P.A.Patel[3]

Bharti Vidyapeeth College Of Engineering (Navi Mumbai, Maharashtra, India)

1.ABSTRACT

Vast assortment of information is store on the computer storage that we tend to referred to as as a Cloud. To shield this information from the unauthorized user cloud supplier ought to implement all doable ways that to create the cloud attack proof. during this paper we've planned a method referred to as (DROPS) Methodology, Division and Replication of Optimum Performance and Security which will create our system safer from assailant to attack the system. In our System once the information is being uploaded on the cloud the file will get divided into small fragments at multiple location exploitation T-coloring graph technique which is able to store the little data at bound distance and at the random location so attack won't be able guess the situation which will proscribe him to hack the information. within the system we can additionally perform cryptography every Fragments so if assailant hacks anybody fragments he can ready to solely hack touch of information which is able to useless for him as each fragments will have separate cryptography key to forestall assailant to hack it. when confirmatory the authentic user the quick decoding method referred to as Iris algorithmic program are use that has high speed to gather all the fragments of provided information from the sender and true information are receive to receiver.

Keywords-Centrality, cloud security, fragmentation, replication, performance.

1. INTRODUCTION

The cloud computing paradigm has reformed the usage and management of the data technology infrastructure . Cloud computing is characterized by on-demand self-services, omnipresent network accesses, resource pooling, elasticity, and measured services . The said characteristics of cloud computing create it a hanging candidate for businesses, organizations, and individual users for adoption. However, the advantages of inexpensive, negligible management (from a users perspective), and large flexibility associate with augmented security consideration . Outsourcing information to a third-party body management, as is finished administrative in cloud computing, provides rise to security considerations .The data compromise could occur because of attacks by different users and nodes at intervals the cloud. Therefore, high security measures are needed to shield information at intervals the cloud. However, the used security strategy should additionally take into consideration the optimization of the info retrieval time. during this paper, we tend to propose Division and Replication of information within the Cloud for Optimal Performance and Security (DROPS) that together approaches the protection and performance problem. within

the DROPS methodology, we tend to divide a file into fragments, and replicate the fragmented information over the cloud nodes. every of the nodes stores solely one fragment of a specific record that ensures that even just in case of a successful attack, no meaningful data is disclosed to the assailant. Moreover, the nodes storing the fragments, are separated with bound distance by means that of graph T-coloring to ban associate assailant ofestimation

Outsourcing information to a third-party administrative control, as is finished in cloud computing, provides rise to security considerations. The data compromise could occur because of attacks by different users and nodes at intervals the cloud. Therefore, high security measures are needed to shield information at intervals the cloud. However, the used security strategy should additionally take into consideration the optimization of the info retrieval time. during this paper, we tend to propose Division and Replication of information within the Cloud for Optimal Performance and Security (DROPS) that together approaches the protection and performance problems. within the DROPS methodology, we tend to divide a file into fragments, and replicate the fragmented information over the cloud nodes.

2. LITERATURE REVIEW

D. Boru, D. KLIAZOVICH, F. GRANELLI, P. BOUVRY, and A. Y. ZOMAYA Energy-efficient information replication in cloud computing

Cloud computing is associate rising paradigm that has computing, communication and storage resources as a service over a network. Communication resources usually often become a bottleneck in commission provisioning for several cloud applications. Therefore, information replication that brings information(e.g., information bases)nearer to data shoppers (e.g., cloud applications) is seen as a promising answer. It permits minimizing network delays and information measure usage. during this paper we tend to study information replication in cloud computing information centers. in contrast to different approaches on the market within the literature, we tend to contemplate each energy potency and information measure consumption of the system. This is often additionally to the improved quality of service QOS obtained as a result of the reduced communication delays. The analysis results, obtained from each mathematical model and intensive simulations, facilitate to unveil performance and energy potency trade offs additionally as guide the planning of future information replication At the part level, there are two main alternatives for creating information center consume less energy:

(a) movement hardware parts down or (b) reducing hardware performance. each strategies are applicable to computing servers and network switches. once applied to the servers, the previous technique is often mentioned as dynamic power management (DPM) [11]. DPM ends up in most of the energy savings. It is the foremost economical if combined with the employment consolidation scheduler—the policy that permits increasing the quantity of idle servers which will that be place into a sleep mode, because the average load of the system usually stays below half- hour in cloud computing systems [11]. The second technique corresponds to the dynamic voltage and frequency scaling (DVFS) technology [12]. DVFS exploits the relation between power consumption P, provided voltage V, and in operation frequency f : $P = V2 * f$. Reducing voltage or frequency reduces the facility consumption. The result of DVFS is restricted , as power reduction applies solely to the center processing unit, whereas system bus, memory, disks additionally as peripheral devices continue overwhelming at their peak rates. kind of like computing servers, most of the energy-efficient solutions for installation depends upon (a) downgrading the in operation frequency (or transmission rate) or (b) powering down the complete device or its hardware parts so as to conserve energy. Power- aware networks were 1st studied by dynasty at el. [10]. In 2003, the primary work that planned a power-aware interconnection network used dynamic voltage scaling (DVS) links [10]. After that, DVS technology was combined with dynamic network termination shutdown (DNS) to further any optimize energy consumption [13].

Another technology which indirectly affects energy consumption is virtualization. Virtualization is widely used in current systems [20] and permits multiple virtual machines (V Ms) to share constant physical server. Server resources is dynamically provisioned to a VM supported the applying necessities. the same as DPM and DVFS power management, virtualization can be is applied in each the computing servers and network switches, however, with completely different objectives. In networking, virtualization permits implementation of logically different addressing and forwarding mechanisms, and will not essentially have the goal of energy.

B. Grubber, T. Wallops check, and E. Stocked Understanding cloud computing vulnerabilities. Discussions regarding cloud computing security usually fail to distinguish general problem from cloud-specific problem. To clarify the discussions regarding vulnerabilities, the authors outline indicators supported sound definitions of risk factors and cloud computing. Each day, recent point, blog entry, or different publication warns U.S.A. regarding cloud computing's security risks and threats; in most cases, security is cited because the most substantial roadblock for cloud computing uptake. however this discourse regarding cloud computing security problem makes it tough to formulate a tenable assessment of the particular security impact for 2 key reasons. First, in several of those discussions regarding risk, basic vocabulary terms - including risk, threat, and vulnerability - square measure usually used interchangeably, while not reference to re their several definitions. Second, not each issue raised is particular to cloud computing.
To achieve a tenable understanding of the "delta" that cloud computing adds with relevancy security problem, we tend to should analyze however cloud computing influences established security problem. A key issue here is security vulnerabilities cloud computing makes bound well-understood vulnerabilities a lot of important moreover as adds new ones to the combination. Before we tend to take a better consider cloud-specific vulnerabilities, however, we tend to should initial establish what a "vulnerability" extremely is. From a cloud client perspective the right-hand facet addressing probable magnitude of future loss isn't modified in any respect by cloud computing: the implication and supreme value of, say, a confidentiality breach, is strictly constant notwithstanding whether or not the info breach occurred among a cloud or a standard IT infrastructure. For a cloud service supplier, things look somewhat different: as a results of because cloud computing systems were decadently separated on constant infrastructure, a loss event may entail a significantly larger impact. however this truth is well grasped and incorporated into a risk assessment: no abstract work for adapting impact analysis to cloud computing looks necessary.
So, we tend to should hunt for changes on Figure 1's left-hand facet - the loss event frequency. Cloud computing may amendment the likelihood of a harmful event's prevalence. As we tend to show later, cloud computing causes important changes with in the vulnerability issue. Of course, moving to a cloud infrastructure may amendment the attackers' access level and motivation, moreover because effort and risk - a undeniable fact that should be thought of as future work. But, for supporting a cloud-specific risk assessment, it looks most profitable to start by examining the precise nature of cloud-specific vulnerabilities.

Proposed System:

- *User will access his/her information anytime .*
- *User will access the records and alter anytime*
- *user has to request Admin if they needs to access their records.*
- *Admin will grant access to different user by sharing special grant to the user.*
- *The records square measure encrypted and hold on within the kind of Hash values in the ledger.*

Existing Technology:

- *This cloud storage that permits data to maneuver electronically between organizations.*
- *Using an cloud computing to browse and write a record isn't solely potential through a digital computer however, looking on the sort of system and cloud settings, may be potential through mobile devices that square measure handwriting capable, tablets and smartphones.*
- *Cloud storage embrace access to to private information hold on that makes individual notes from an AN without delay visible and accessible for user.*

DISADVANTAGES OF EXISTING SYSTEM

- *The information compromise might occur because of attacks different other users and nodes among the cloud.*
- *The used security strategy should conjointly take under consideration the improvement of the info retrieval time.*

Hardware and Software Requirement *1.Hardware Requirement*

4GB RAM.

200GB HDD.

INTEL 1.66 GHZ PROCESSOR PENTIUN

2. Software Requirement

Operating System : Windows 7 ,8 ,9

Technology :JAVA, SERVLET, JSP, HTML5 / CSS3, BOOTSTRAP, JQUERY

Database:MYSQL Tool : Eclipse

3. Implementation

We square measure developing a reliable and safer cloud for our system. Work can save the time and resources utilized in downloading, up- dating, and uploading the file once more.. Moreover, the implications of protocol in cast over the DROPS methodology got to be studied that's is relevant to distributed information storage and access. data was Get table by AN mortal just in case of a winning attack. No node within the cloud, hold on over one fragment of constant file.

- *Front-End(HTML,CSS,j Query,Ajax)*

1. First, we have designed the front end using HTML(hypertext markup language) and CSS(cascading style sheet).

2. Every form inside the web portal is designed using HTML and VCSS.

- *DATABASE*

1. *Next, we've got created a information for storing numerous information into the INFO*
2. *SQL Server 2008 categorical may be a free edition of SQL Server that is an ideal information platform for learning and building desktop and tiny server applications.*
3. *In ASP.net there's an online. Configure file to attach with the information and net application*

- *BACK-END(JAVA,Bootstrap,JSP)*

1. *we've got used Java, Bootstrap and JSP for face.*
2. *Java may be high-level programming language developed by Sun Micro systems. Instead, Java programs are interpreted by the Java Virtual Machine, or JVM, which runs on multiple platforms. This suggests all Java programs area unit multi platform and may run on different platforms, together Macintosh, Windows, and UNIX system computers*
3. *one in every of the foremost widely used programming languages, Java is used as the server-side language for many back-end development comes, together with those involving huge information and golem development. Java is conjointly commonly used for desktop computing, different mobilecomputing,games, and numerical computing.*

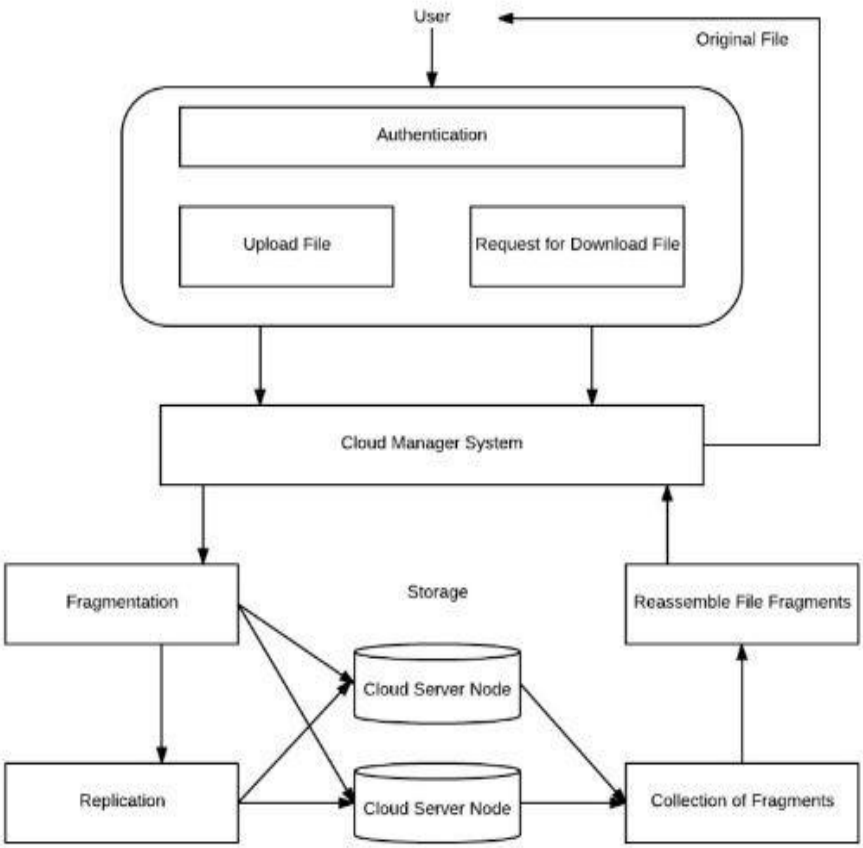
- *ENCRYPTION*

1. *To perform encryption first we have created a PUBLIC Static class called Encryption.*
2. *Inside the encryption class, we have created a function called Encrypt*
3. *This will perform encryption on file and write the data on file*
4. *Write Byte((byte)data).*

- *DECRYPTION*

1. *Decryption is inverse to Encryption first we created a PUBLIC class called Decryption.*
2. *In the next step it will decrypt the data and write the data on the output file*
3. *Fs Output.Write Byte((byte)data);*
4. *Block Diagram*

SYSTEM ARCHITECTURE:-



Conclusion

We proposed the DROPS methodology, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time. The data file was fragmented and the
fragments are dispersed over multiple nodes. The nodes were separated by means of T-coloring. The
fragmentation and dispersal ensured that no significant information was obtainable by an adversary in
case of a successful attack. No node in the cloud, stored more than a single fragment of the same file.
The performance of the DROPS methodology was compared with full-scale replication techniques. The results of the simulations revealed that the simultaneous focus on the security and performance, resulted
in increased security level of data accompanied by a slight performance drop.
Currently with the DROPS
methodology, a user has to download the file, update the contents, and upload it again. It is strategic to

develop an automatic update mechanism that can identify and update the required fragments only. The

aforesaid future work will save the time and resources utilized in downloading, updating, and uploading

the file again. Moreover, the implications of TCP incast over the DROPS methodology need to bestudied

that is relevant to distributed data storage and access.

6.Reference

- *Sunil S Mhamane and L.M.R.J Lobo "Use of Hidden Markov Model as Internet Banking*
- *Fraud Detection" International Journal of Computer Applications (0975 – 8887) Volume 45–*
- *No.21, May 2012*
- *Pankaj Richhariya et al "A Survey on Financial Fraud Detection Methodologies" BITS,*
- *Bhopal," International Journal of Computer Applications (0975 – 8887) Volume 45 No.22, May*
- *2012*
- *"Credit Card Fraud Detection Using Hidden Markov Model Shailesh S. Dhok (2012).*
- *A Survey on Hidden Markov Model for Credit Card Fraud Detection Anshul Singh, Devesh*
- *Narayan.*
- *Raghavendra Patidar, Lokesh Sharma Credit Card Fraud Detection using Neural*
- *Network(2011).*
- *Fraud Detection of Credit Card Payment System by Genetic Algorithm K. Rama Kalyani,*
- *D.UmaDevi (2012).*
- *An Oracle White Paper. Oracle Real Application Clusters (RAC) ; 2013.*
  EMC INC. Geenplum Database: Critical Mass Innovation, Architecture White Paper ; 2010.