IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-4 E-ISSN: 2347-2693

An Efficient Deduplication Mechanism for Big Data Analysis in Cloud Environments

M. Murugesan[1*], A. Kalaiyarasi[2]

[1]Dept.of CSE, M.Kumarasamy College of Engineering, Karur,India
[2]Dept.of CSE, M.Kumarasamy College of Engineering, Karur,India

**Corresponding Author: murugesanm.cse@mkce.ac.in*

Available online at: www.ijcseonline.org

Received: 14/Mar/2018, Revised: 20/Mar/2018, Accepted: 05/Apr/2018, Published: 30/Apr/2018

***Abstract*—**With the consistent and exponential increment of the quantity of clients and the span of their information, information deduplication turns out to be increasingly a need for distributed storage suppliers. By putting away a one of a kind duplicate of copy information, cloud suppliers significantly diminish their capacity and information exchange costs. These immense volumes of information require some down to earth stages for the capacity, handling and accessibility and cloud innovation offers every one of the possibilities to satisfy these necessities. Information deduplication is alluded to as a procedure offered to distributed storage suppliers (CSPs) to dispense with the copy information and keep just a solitary one of a kind duplicate of it for storage room sparing reason.In this paper, we display a plan that allows an all the more fine-grained exchange off. The instinct is that outsourced information may require distinctive levels of assurance, contingent upon how mainstream it is: content shared by numerous clients.We show an originalfelt that isolates data according to their reputation. In light of this thought, we outline an encryption arrange for that ensures semantic security for obnoxious information and gives weaker security and better putting away and transmission restrict benefits for eminent information. Subsequently, information de-duplication can be able for standard information, while semantically secure encryptionguarantees unsavory substance. We can use the backup recover system at the time of blocking and also analyze frequent login access system.

***Index Terms*—**Cloud storage, Chunks, Similarity matching, Data security, Backup Recovery

I. INTRODUCTION

Cloud computing is a processing worldview, where an expansive pool of frameworks are associated in private or open systems, to give powerfully adaptable foundation to application, information and record stockpiling. With the approach of this innovation, the cost of calculation, application facilitating, content stockpiling and conveyance is decreased altogether [3]. It is a down to earth way to deal with encounter coordinate money saving advantages and it can possibly change a server farm from a capital-concentrated set up to a variable valued condition. Cloud processing depends on an exceptionally central principles of reusability of IT abilities. The distinction that distributed computing brings contrasted with customary ideas of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to widen skylines crosswise over hierarchical limits. Forrester [1] characterizes distributed computing as: "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption". It is a technology that uses the internet and central remote servers to maintain data and applications and allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Cloud computing examples are Yahoo email, Gmail, or Hotmail. Data deduplication is a technique for reducing the amount of storage space an organization needs to save its data. In most organizations, the storage systems contain duplicate copies of many pieces of data. For example, the same file may be saved in several different places by different users, or two or more files that aren't identical may still include much of the same data.Alongsidelow proprietorship costs and flexibility, customers require the confirmation of their data and protection guarantees through encryption[1]. To make data organization flexible deduplication we are use Encryption for secure deduplication organizations. Unfortunately, deduplication and encryption are two conflicting advances. While the motivation behind deduplication is to distinguish vague data parts and store them just once, the inevitable result of encryption is to make two unclear data partitions in discernable in the wake of being mixed. This suggests if data are mixed by customers standardly as like shared authority, the appropriated stockpiling provider can't have any kind of effect deduplication since two vague data sections will be

assorted after encryption. On the other hand, if data are not mixed by customers, mystery by can't be guaranteed and data are not secured against curious appropriated stockpiling providers.There are two kinds of deduplication as far as the size: (I) record level deduplication, which finds redundancies between various documents and evacuates these redundancies to diminish limit requests, and (ii) blockleveldeduplication, which finds and expels redundancies between information pieces. The document can be partitioned into littler settled size or variable-estimate pieces. Utilizing fixedsize squares improves the calculations of piece limits, while utilizing variable-estimate squares [2].A methodology which has been proposed to meet these two conflicting requirements is Label age and AES Plan whereby the encryption key is by and large the result of the hash of the data area. In spite of the way that encryption is all in all a not too bad plausibility to achieve security and deduplication meanwhile, it shockingly encounters distinctive without a doubt comprehended weaknesses. The mystery issue can be managed by encoding tricky data previously outsourcing to remote servers. Nearby low ownership costs and versatility, customers require the confirmation of their data and characterization guarantees through encryption[4].In this paper, we address the a for said security issue to propose a common expert to the files which Deduplictedbased security protecting confirmation for the cloud information stockpiling, which acknowledges verification and approval without bargaining a client's private data.The basic data chunk similarity is shown in fig 1.

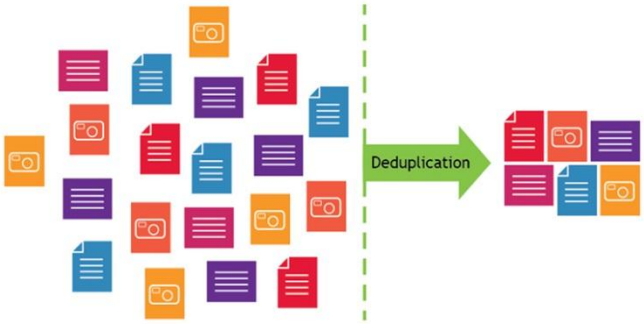

Fig 1: Data deduplication

II. Related Work

X. Zhang, et.al,..[1]propose a novel way to deal with effectively accomplish security safeguarding over dispersed and incremental informational collections on cloud. To proficiently refresh anonymized informational collections within the sight of new information, ordering structure of semi identifiers is set up on anonymized informational collections. Semi identifiers, which speak to the gatherings of anonymized information, are filed for productivity. Besides, comparable information records are set on similar hubs to decrease correspondence cost crosswise over information stockpiling hubs when anonymized informational indexes are summed up or concentrated to accomplish obscurity prerequisites and high information utility. An ordinarily utilized protection display k-namelessness is utilized to gauge security in our examination, i.e., security prerequisites are meant by a limit k. Further, sub-tree speculation plot is used to achieve information anonymization. A calculation is intended to satisfy our approach in like manner. Trial assessment on certifiable informational indexes shows that with our approach, the proficiency of security conservation over incremental informational indexes can be enhanced altogether finished existing methodologies.

T. Yang, et.al,…[2]executed an exceptionally versatile two-stage TDS approach for information anonymization in view of MapReduce on cloud. To make utilization of the parallel capacity of MapReduce on cloud, characterization required in an anonymization procedure is part into two stages. In the first, unique datasets are parceled into a gathering of little datasets, and those datasets are anonymized in parallel, making transitionally comes about. In the second one, the middle of the road comes about are collected into one, and further anonymized to accomplish steady k-unknown informational collections. It use MapReduce to achieve the solid calculation in the two stages. A gathering of MapReducejobs are intentionally outlined and facilitated to perform specializations on informational collections cooperatively. It assesses the approach by directing trials on true informational indexes. Trial comes about demonstrate that with the approach, the adaptability and proficiency of TDS can be progressed. It assess the approach by leading analyses on certifiable informational indexes. Trial comes about show that with the approach, the adaptability and effectiveness of TDS can be enhanced fundamentally finished existing methodologies. The significant commitments of the examination are triple. Initially, it inventively apply MapReduce on cloud to TDS for information anonymization and purposely outline a gathering of imaginative MapReduce occupations to solidly achieve the specializations in a very adaptable manner. Besides, it propose a two-stage TDS way to deal with increase high adaptability by means of enabling specializations to be directed on various information segments in parallel amid the main stage.

N. Laptev, et.al,…[3] analyzedEarly Precise Outcome Library structure (Lord) has been composed and created to give this truly necessary usefulness in this way crossing over any barrier between the mushrooming information sizes and the reaction time prerequisites. To accomplish this, we investigate and apply intense techniques and models created in insights to appraise comes about and the precision got from examined information. We propose a strategy and a framework that upgrade the work process calculation on enormous informational collections to accomplish the coveted exactness while limiting the time and the assets required. In this exhibit we will introduce the Lord prototype1 and its instinctive GUI interface which helps the client through the progressive periods of 'enormous

information' examination. This model speaks to likewise the beginning stage for a formal investigation of the apparatus ease of use we are wanting to lead. The early guess strategies introduced are additionally imperative for adaptation to internal failure, where just a segment of the information is accessible and the mistake estimation is required to decide whether hub recuperation is important. Delta support strategies reuse the outcomes crosswise over examples of various sizes, while the coordination with the mainstream MapReduce system takes into consideration misusing the intrinsic parallelism of bootstrapping. Besides Duke's basic Programming interface takes into consideration simple particular of mining calculations that take full favorable position of system.

T. Condie, et.al,…[4] executed The democratization of information has filled the gathering of (much more!) monstrous informational collections. Stages for expansive scale investigation are being worked for separating experiences that upgrade benefits and advance tasks. Be that as it may, the present suite of stages can just catch a little part of machine learning calculations at scale. Those that drop out of extension incite arrangements that mishandle the expected programming model or propel the execution of a different framework. This prompts creation pipelines worked out of safeguarding wire and paste code for moving information all through various subsystems. The issue is additionally confounded by the presumption that every framework expect responsibility for whole machine, or, best case scenario the VM, constraining directors to partition the bunch into machine subsets; doling out a solitary framework to each. Asset moderators like YARN and Mesos are being worked to address this issue with a thin virtualization layer that multiplexes larger amount frameworks on a solitary brought together machine bunch. However, the information researcher is still left with the issue of finding the correct framework and programming model for their information examination errand, expecting one even exists, and arranging their answer underway.

A. Aboulnaga, et.al,…[5] provide the framework for Parallel database frameworks and MapReduce frameworks (most quite Hadoop) are basic parts of the present foundation for Enormous Information examination. These frameworks procedure different simultaneous workloads comprising of complex client demands, where each demand is related with an (unequivocal or verifiable) benefit level target. For instance, the workload of a specific client or application may have a higher need than different workloads. Or then again, a specific workload may have strict due dates for the culmination of its solicitations. The exploration zone of Workload Administration centers around guaranteeing that the framework meets the administration level targets of different solicitations while in the meantime limiting the assets required to accomplish this objective.

III. EXISTING METHODOLOGIES

Numerous frameworks have been produced to give secure capacity however customary encryption systems are not reasonable for pressure purposes. Deterministic encryption, specifically concurrent encryption, is a decent contender to accomplish both classification and pressure yet it experiences surely understood shortcomings which don't guarantee security of unsurprising records against word reference assaults. And furthermore existing framework makes utilization of intermediary re-encryption, has been proposed yet data on execution and overhead were not given.Unfortunately, compression loses its viability in conjunction with end-to-end encryption [1],[2]. End-to-end encryption in a capacity framework is the procedure by which information is scrambled at its source before entrance into the capacity framework. It is turning into an undeniably noticeable necessity because of both the quantity of security episodes connected to spillage of decoded information and the fixing of part particular laws and controls. Unmistakably, if semantically secure encryption is utilized, record pressure is inconceivable, as nobody separated from the proprietor of the unscrambling key can choose whether two figure writings relate to the same plaintext. Paltry arrangements, for example, compelling clients to share encryption keys or utilizing deterministic encryption, miss the mark regarding giving adequate levels of security. As an outcome, stockpiling frameworks are relied upon to experience major rebuilding to keep up the present plate/client proportion within the sight of end-to-end encryption [5]. The plan of capacity productivity works by and large and of pressure works specifically that don't lose their viability in nearness of end-to-end security is accordingly still an open issue.The existing methodologies contain:

3.1 File-level de-duplication

It is ordinarily known as single-illustration storing, record level data de-duplication ponders a report that must be chronicled or support that has recently been secured by checking each one of its attributes against the document. The record is revived and put just if the record is surprising, if not than only a pointer to the present report that is secured references. Simply the single case of archive is saved in the result and appropriate copies are supplanted by "stub" which centers to the main record [6][8].

3.2 Traditional Encryption algorithm:

In spite of the fact that it is realized that information deduplication gives more advantages, security and protection concerns emerge in light of the fact that the client's touchy information is helpless to both the outcast and insider assaults. Along these lines, while considering the standard encryption methods to secure the customers tricky data there are various issues are connected. Customary encryption gives data characterization yet it isn't great with Deduplication [7],[9]. As in standard encryption unmistakable customers scramble their data with their own keys. Hence, the undefined

data of the assorted customers will incite distinctive ciphertext which is making the information deduplication relatively unthinkable in this customary approach [10]. The fundamental advance of the calculation as shows:

KeyGenSE: k is the key age calculation that produces κ utilizing security parameter I

EncSE (k, M): C is the symmetric encryption calculation that takes the mystery κ and message M and after that yields the ciphertext C;
DecSE (k, C): M is the symmetric decoding calculation that takes the mystery κ and ciphertext C and afterward yields the first message M.

3.3 Limitations:

- Compression check only with file name and not file content
- Could not achieve secure access control under a dynamic ownership changing environment
- Security degradation of the cloud service

IV. PROPOSED METHODOLOGIES

Capacity proficiency capacities, for example, compression and compression manage the cost of capacity suppliers better usage of their stockpiling back finishes and the capacity to serve more clients with a similar foundation. Information compression is the procedure by which a capacity supplier just stores a solitary duplicate of a record claimed by a few of its clients. There are four diverse compression systems, contingent upon whether compression occurs by the customer part (i.e. formerly the transfer) or then again at the server side, and whether compression occurs on a piece stageotherwiseon a record stage. Compression is most remunerating when it is activated at the customer side, as it likewise spares transfer data transmission [25]. Consequently, compression is a basic empowering agent for various famous and fruitful stockpiling administrations that offer shoddy, remote stockpiling to the expansive open by performing customer side compression, along these lines sparing both the system data transmission and capacity costs.The objective of the framework is to ensure information privacy without losing the benefit of pressure. Privacy must be ensured for all documents, including the anticipated ones. The security of the entire framework ought not depend on the security of a solitary segment (single purpose of disappointment), and the security level ought not crumple when a solitary segment is traded off. We think about the server as a put stock in segment regarding client confirmation, get to control and extra encryption [26]. The server isn't trusted as for the privacy of information put away at the distributed storage supplier. Subsequently, the server can't perform disconnected word reference assaults. Any individual who approaches the capacity is considered as a potential assailant, including representatives at the distributed storage supplier and the distributed storage supplier itself. In our risk demonstrate, the distributed storage supplier is straightforward however inquisitive, implying that it completes its errands yet may endeavor to decode information put away by clients.And also implement back up recover scheme to recover data at the time of infrequent access. Admin can be sent alert to every 3 days, one week, two weeks and three weeks. If the users not login to the system means, automatically recover the data and forward to alternate storage with mobile intimation.

4.1 Block encryption algorithm

In cryptography, a piece figure is a deterministic count taking a shot at settled length social occasions of bits, called blocks, with an unvarying change that is demonstrated by a symmetric key. Square figures fill in as basic essential parts in the planof various cryptographic traditions, and are for the most part used to execute encryption of mass data. Iterated thing figures finish encryption in different rounds, each one of which uses a substitute subkey got from the primary key. One sweeping execution of such figures, named a Feistel arrange after Horst Feistel, is prominently actualized in the DES figure. Numerous different acknowledge of square figures, for example, the AES, are named substitution-change systems. The production of the DES figure by the Unified States National Agency of Benchmarks (along these lines the U.S. National Establishment of Models and Innovation, NIST) in 1977 was principal in the overall population appreciation of present day piece figure layout. It in like manner influenced the educational progression of cryptanalytic attacks. Both differential and straight cryptanalysis rose out of focuses on the DES plot. Beginning at 2016 there is a palette of strike frameworks against which a square figure must be secure, despite being overwhelming against creature control attacks. To be sure, even a protected piece figure is sensible only for the encryption of a singular square under a settled key. A colossal number of techniques for assignment have been proposed to allow their reiterated utilize secury, as a rule to achieve the security goals of protection and legitimacy. In any case, square figures may likewise include as building-obstructs in other cryptographic traditions, for instance, far reaching hash limits and pseudo-subjective number generators.

One essential kind of iterated square figure identified as a substitution-change arrange (SPN) takes a piece of the plaintext and the key as data sources, and smears a few rotating rings comprising of a substitution organize took after by a step organize—to create each piece of figure content yield.The non-straight substitution organize mixes the key bits with those of the plaintext, making Shannon's perplexity. The direct change organize then disseminates

redundancies, making dispersion. A substitution box (S-box) substitutes somewhat square of data bits with another bit of yield bits. This substitution must be facilitated, to ensure invertibility (accordingly unscrambling). An ensured S-box will have the property that changing one data bit will change about bit of the yield bits by and large, showing what is known as the heavy slide affect—i.e. it has the property that each yield bit will depend upon every information bit.

4.1.2 Pseudo code for Block Cipher algorithm:

Step 1: Fractioning of the text into 64-bit (8 octet) blocks;

Step 2: Initial permutation of blocks;

Step 3: Breakdown of the blocks into two parts: left and right, named *L* and *R*;

Step 4: Permutation and substitution steps repeated 16 times (called rounds);

Step 5: Re-joining of the left and right parts then inverse initial permutation.

4.2 Block level data chunk similarity

Block compression requires more handling power than the document pressure, since the quantity of identifiers that should be prepared increments enormously. Correspondingly, its file for following the individual cycles gets likewise substantially bigger. Utilizing of variable length pieces is much more source-escalated. Also, some of the time a similar hash number might be produced for two unique information parts, which is called hash impacts. In the event that that happens, the framework won't spare the new information as it sees that the hash number as of now exists in the file.he algorithm steps as follows
BlockTag(FileBlock) - It figures hash of the Record hinder as document piece Tag;

DupCheckReq(Token) - It asks for the Breaking point Server for Copy Check of the record square.

FileUploadReq(FileBlockID, FileBlock, Token) – It trades the Record Information As far as possible Server if the file piece is Imperative and resuscitates the report square Token set away.

FileBlock Encrypt(Fileblock) - It scrambles the document destroy with Joined Encryption, where the mixed key is from similitude checking of the record piece;
TokenGen(File Square, UserID) – the strategy stacks the related advantage keys of the customer and make token.

FileBlockStore(FileBlockID, FileBlock, Token) - It stores the FileBlock on Plate and updates the Mapping.

4.2.2 Psuedo code for secure information pressure:

Step 1: Client profiling: Customer enlistment and sign in

Step 2: Session secret word: Token age and check

Step 3: Customer starts document exchange (transfer/download).

Step 4: Document transfer: check for copy

Step 5: If copy at any of document name and record content, make document pointer and store in CSP

Step 6: If no copy discovered, store scrambled document in CSP.

Step 7: Record download: Information proprietor to unscramble and download document.

Step 8: Server match up with customer and finishes document transfer/download process
Step 9: Check Login time of user after 3 days, 1 week, 2 week and 3 Weeks
Step 10: If no login means, send mobile intimation to user
Step 11: Recover the files and forward to alternative mail
The proposed architecture is shown in fig 2.

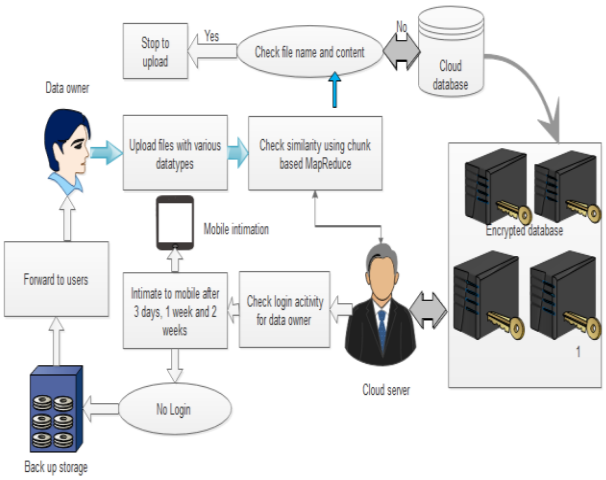

Fig 2: Proposed framework

4.3 ADVANTAGES:

- Dynamic updation can be implemented in cloud storage. File and file content analyzed
- Security is high and to provide data integrity to all data owners

V. EXPERIMENTAL RESULTS

The proposed algorithm is analyzed in terms of storage preserving and implemented in real time environments. We can illustrate the results using PHP framework as front end and SQL SERVER as Back end.

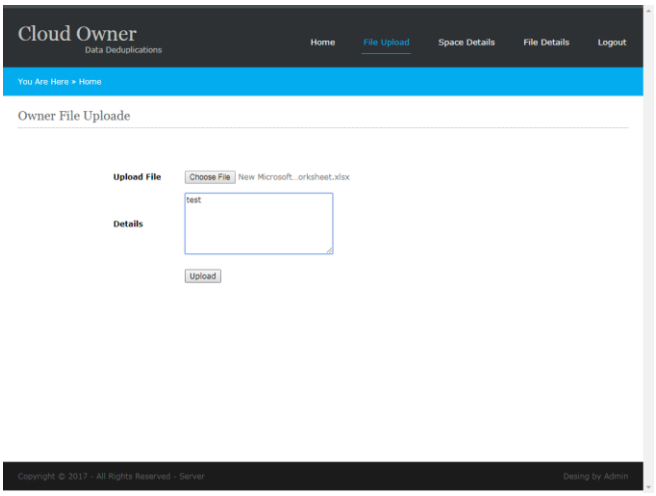

Fig 3: Cloud Framework

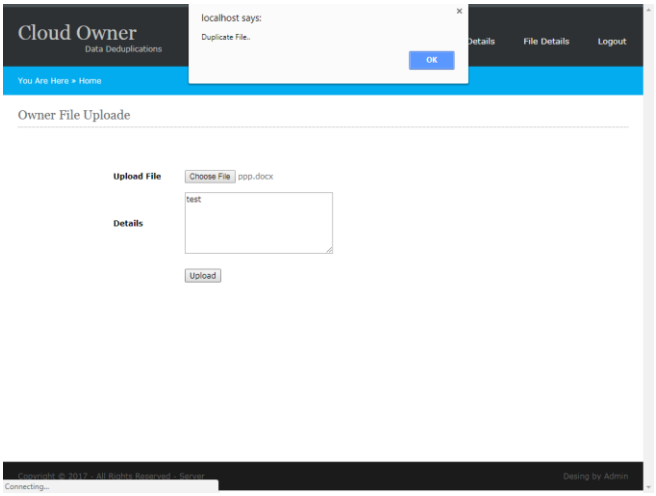

Fig 4: Duplication checking

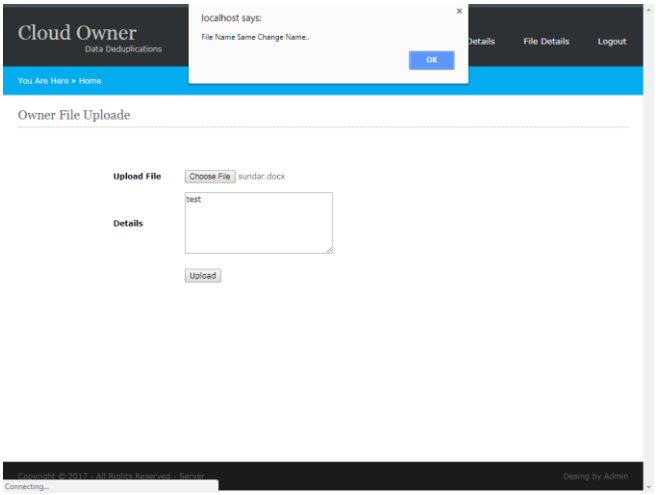

Fig 5: Notification system

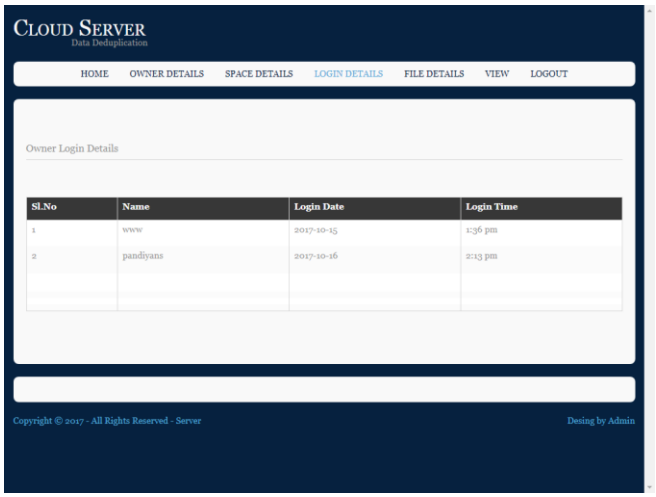

Fig 6: Login details

From the above figure 6 provide alert about user login status using Time to live properties. The proposed system preserves the storage with security and also recovered the backup.

VI. CONCLUSION

The thought of approved information de-duplication method is particular information pressure strategy which dispenses with excess information and also enhances stockpiling and data transfer capacity usage. Symmetric encryption strategy is proposed to uphold secrecy amidde-duplication, which encode data before outsourcing. Security examination shows that the plans are secure in regards to insider and untouchable strikes. To better ensure the information reinforcement, we display session time examination of client alongside TTL property, to address issue of information blockages progressively cloud conditions.

REFERENCES

[1]. X. Zhang, C. Liu, S. Nepal and J. Chen, "An Efficient Quasiidentifier Index based Approach for Privacy Preservation over Incremental Data Sets on Cloud," Journal of Computer and System Sciences (JCSS), 79(5): 542-555, 2013.

[2]. X. Zhang, T. Yang, C. Liu and J. Chen, "A Scalable Two-Phase Top-Down Specialization Approach for Data Anonymization using Systems, in MapReduce on Cloud," IEEE Transactions on Parallel and Distributed, 25(2): 363-373, 2014.

[3]. N. Laptev, K. Zeng and C. Zaniolo, "Very fast estimation for result and accuracy of big data analytics: The EARL system," Proceedings of the 29th IEEE International Conference on Data Engineering (ICDE), pp. 1296-1299, 2013.

[4]. T. Condie, P. Mineiro, N. Polyzotis and M. Weimer, "Machine learning on Big Data," Proceedings of the 29th IEEE International Conference on Data Engineering (ICDE), pp. 1242-1244, 2013.

[5]. Aboulnaga and S. Babu, "Workload management for Big Data analytics," Proceedings of the 29th IEEE International Conference on Data Engineering (ICDE), pp. 1249, 2013

[6]. M. Abadi, D. Boneh, I. Mironov, A. Raghunathan, and G. Segev,"Message-locked encryption for lock-dependent messages," in Advancesin Cryptology - CRYPTO 2013 - 33rd Annual

Cryptology Conference,Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, PartI, 2013, pp. 374–391.
[7]. L. Wang, J. Zhan, W. Shi and Y. Liang, "In cloud, can scientific communities benefit from the economies of scale?" IEEE Transactions on Parallel and Distributed Systems 23(2): 296-303, 2012.
[8]. B. Li, E. Mazur, Y. Diao, A. McGregor and P. Shenoy, "A platform for scalable one-pass analytics using mapreduce," in: Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD'11), 2011, pp. 985-996.
[9]. R. Kienzler, R. Bruggmann, A. Ranganathan and N. Tatbul, "Stream as you go: The case for incremental data access and processing in the cloud," IEEE ICDE International Workshop on Data Management in the Cloud (DMC'12), 2012
[10]. C. Olston, G. Chiou, L. Chitnis, F. Liu, Y. Han, M. Larsson, A. Neumann, V.B.N. Rao, V. Sankarasubramanian, S. Seth, C. Tian, T. ZiCornell and X. Wang, "Nova: Continuous pig/hadoop workflows," Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD'11), pp. 1081-1090, 2011.
[11]. K.H. Lee, Y.J. Lee, H. Choi, Y.D. Chung and B. Moon, "Parallel data processing with mapreduce: A survey," ACM SIGMOD Record 40(4): 11-20, 2012.
[12]. T. Jiang, X. Chen, Q. Wu, J. Ma, W. Susilo, and W. Lou, "Secure andefficient cloud data Deduplication with randomized tag," IEEE Trans.Information Forensics and Security, vol. PP, no. 99,
[13]. Y. Zhou, D. Feng, W. Xia, M. Fu, F. Huang, Y. Zhang, and C. Li, "Secdep: A user-aware efficient fine-grained secure Deduplication scheme with multi-level key management," in IEEE 31st Symposium on Mass Storage Systems and Technologies, MSST 2015, Santa Clara, CA, USA, May 30 - June 5, 2015, 2015, pp. 1–14.
[14]. Z. Yan, W. Ding, X. Yu, H. Zhu, and R. H. Deng, "Deduplication on encrypted big data in cloud," IEEE Trans. Big Data, vol. 2, no. 2, pp. 138–150, 2016.
[15]. "Prism (surveillance program)," https://www.theguardian.com/us-news/ prism.
[16]. R. Bhaskar, S. Guha, S. Laxman, and P. Naldurg, "Verito: A practical system for transparency and accountability in virtual economies," in 20th Annual Network and Distributed System Security Symposium, NDSS 2013, San Diego, California, USA, February 24-27, 2013, 2013.
[17]. D. Boyd, K. Crawford, S. Shaikh, and V. Ravishankar, "Six provocations for big data," Six-provocations-for-Big-Data1.pdf.
[18]. X. Yang, R. Lu, H. Liang, and X. Tang, "SFPM: A secure and fine-grained privacy-preserving matching protocol for mobile social networking," Big Data Research, vol. 3, pp. 2–9, 2016.
[19]. A. K. Mohan, E. Cutrell, and B. Parthasarathy, "Instituting credibility, accountability and transparency in local service delivery?: helpline and aasthi in karnataka, india," in International conference on information and communication technologies and development, ICTD 2013, Cape Town, South Africa, December 7-10, 2013, Volume 1: Papers, 2013, pp. 238 247.
[20]. S Saravanan, V Venkatachalam, Improving map reduce task scheduling and micro-partitioning mechanism for mobile cloud multimedia services [J]. Int J of AdvIntell Paradigms ***8***(2), 156–167 (2016)
[21]. S Saravanan, V Venkatachalam,"Advance Map Reduce Task Scheduling algorithm using mobile cloud multimedia services architecture" IEEE Digital Explore,pp21-25,2014.
[22]. S.Saravanan, Arivarasan."An efficientranked keyword search for effective utilization of outsourced cloud data" Journal of Global Research in Computer Science, Vol4(4), pp:8-12
[23]. S.Swathi "Preemptive Virtual Machine Scheduling Using CLOUDSIM Tool", International Journal of Advances in Engineering, 2015, 1(3), 323 -327 ISSN: 2394-9260, pp:323-327.
[24]. S Saravanan, V Venkatachalam, Then Malligai "Optimization of SLA violation in cloud computing A artificial bee colony"2015, 1(3), 323 -327 ISSN: 2394-9260, pp:410-414.
[25]. M.Murugesan, A.Kalaiyarasi, "Secure Data Compression Scheme in Cloud Environments With Backup Recovery Scheme", International Journal of Pure and Applied Mathematics, issue Feb. 2018, pp467-471.
[26]. Dr.P.Santhi, "Privacy Preserving and consistency check of Data Store in Cloud using Attribute based Encryption", International Journal of Engineering Development and Research, issue 2017.

Authors Profile

Mr.M.Murugesan received the B.Sc degree in Physics from Madurai Kamaraj University, Salem, Tamil Nadu, India in 2006 and MCA from Anna university,chennai,Tamil Nadu, India in 2009 and ME degree in Computer Science and Engineering from Anna university,Chennai,Tamil Nadu,India in 2016.He is pursuing Ph.D from Anna University,Chennai. Presently Working as a Assistant Professor and Placement Head in the Department of Computer Science and Engineering, at M.Kumarasamy College of Engineering. One among Top 10% faculty members of the college in the Performance Appraisal during the academic year 2014 – 2015.Infosys Recognized as Bronze partner faculty under Inspire – The Campus Faculty Partnership Model through Infosys Campus Connect.He has published 4 papers in reputed international journals. His area of interest is Data Structures and Algorithm and Networks.

