Enhancing Two Standard Privacy Preserving to Improve the Security Policy in Cloud Environment

Komarasamy G & Vivek V
Department of Computer Science and Engineering
School of Engineering and Technology
JGI Global Campus, Jain University, Bangalore, Karnataka, India
Email: vivek544@hotmail.com

***Abstract* - Cloud computing is emerging computing model where the data owners are outsourcing their data into the cloud storage. By outsourcing the data files into the cloud, it gives many benefits to the large enterprises as well as individual users for accessing database security. In data base Storage management systems to cloud it still faces a number of fundamental and critical challenges, among which storage space and security is the top concern. We consider the problem of processing range query search over a confidential numeric attribute K in an outsourced setting of cloud computing. To ensure the correctness of user and user's data in the cloud, we propose a multilevel round random key policy third party authentication system in crypto policy standard. In addition to simplified data storage and secure data acquisition. Also, we consider processing range query search over a confidential numeric attribute with two main challenges. First, the confidentiality requires hiding the value and the relative order of the attribute in records from the cloud server. Finally, we will perform security and performance analysis which shows that the proposed scheme is highly efficient for maintaining secure data storage and acquisition.**

***Keywords:* Acquisition, cloud, random key, confidentiality, outsourcing.**

I. INTRODUCTION

1.1 Cloud Computing

Cloud computing is a rising processing model in which assets of the registering interchanges are given as administrations over the Internet. This paper proposed a few administrations for information security and access control when clients outsource delicate information for sharing on cloud servers. This paper tends to this testing open issue by, on one hand, characterizing and upholding access arrangements in light of information properties, and, then again, enabling the information proprietor to relegate the greaterpart of the calculation errands engaged with fine grained information get to control to un-trusted cloud servers without unveiling the fundamental information substance. Broad examination demonstrates that our proposed conspire is very effective and likely secures under existing security models. So as to address this new issue and further accomplish a protected and tried and true distributed storage benefit. The web is usually imagined as mists henceforth the expression "distributed computing" for calculation done through the web. With distributed computing clients can get to database assets by means of the web from anyplace, for whatever length of time that they require, without stressing over any support or administration of genuine assets. Plus, databases in cloud are extremely powerful and adaptable. Distributed computing is dissimilar to matrix figuring, utility registering, or autonomic processing. Truth be told, it is an exceptionally free stage as far as figuring.

1.2 Types of Cloud and Services

Private cloud: In this model, the cloud supplier gives cloud foundation to a solitary association that has numerous shoppers. This framework is to be utilized solely for their utilization and need. The proprietor, supervisor, and administrator of this cloud could be simply the association, an outsider, or the association and outsider together. This private cloud could be on premises or off premises.

Community Cloud: In this model, the cloud supplier gives cloud foundation to a solitary association that has numerous shoppers. This framework is to be utilized solely for their utilization and need. The proprietor, supervisor, and administrator of this cloud could be simply the association, an outsider, or the association and outsider together. This private cloud could be on premises or off premises.

Public Cloud: This model contrasts from the past model in that it is open for general society it isn't private and not only for group. In this model, an open cloud can be provisioned for open to utilize it to fulfill their necessities. The proprietor, administrator, and administrator of this cloud could be an administration, private association, a business or scholastic association, and in some cases a considerable lot of them can be in one cloud and get the administration from a similar supplier.

Hybrid Cloud: This model involves at least two organization models (private, group, or open). The cloud foundation can be mix of those models. Server farm inside an association, private cloud, and open cloud can be consolidated keeping in mind the

IJSMS

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

end goal to get administrations and information from both so as to make an all-around oversaw and bound together registering.

1.3 Cloud Data Storage

In cloud information stockpiling framework, clients store their information in the cloud and never again have the information locally. In this way, the rightness and accessibility of the information documents being put away on the circulated cloud servers must be ensured. One of the key issues is to successfully identify any unapproved information change and defilement, conceivably because of server trade off as well as irregular Byzantine disappointments. Additionally, in the circulated situation when such irregularities are effectively identified, to discover which server the information mistake lies in is likewise of incredible criticalness, since it can be the initial step to quick recuperate the capacity blunders. To address these issues, our fundamental plan for guaranteeing cloud information stockpiling is introduced in this segment. The initial segment of the segment is committed to a survey of fundamental apparatuses from coding hypothesis that is required in our plan for record conveyance crosswise over cloud servers. At that point, the homomorphism token is presented.

The token calculation work we are thinking about has a place with a group of all-inclusive hash work, saved the homomorphic properties, which can be flawlessly incorporated with the confirmation of eradication coded information. Therefore, it is additionally demonstrated to determine a test reaction convention for checking the capacity rightness and in addition recognizing getting rowdy servers. At long last, the strategy for document recovery and mistake recuperation in light of deletion redressing code is illustrated.

1.4 Cloud Security Issues

Indeed, even with these numerous advantages of distributed computing, beforehand said, clients are hesitant to embrace this innovation and move from traditional processing to distributed computing. In distributed computing, security is a wide point. It is a blend of advancements, controls to defend the information, and strategies to ensure the information, administrations, and foundation. This blend is an objective of conceivable assaults. In this way, there are new security prerequisites in the cloud contrasted with customary conditions. Conventional security engineering is broken in light of the fact that the client does not claim the framework any more. Likewise, the general security cloud-based framework is equivalent to the security of the weakest substance.

By outsourcing, clients lose their physical control over information when it is put away in a remote server and they assign their control to an untrusted cloud supplier or gathering. In spite of capable and dependable server contrasted with customer handling force and unwavering quality, there are numerous dangers confronting the cloud from an outcast as well as from an insider which can use cloud vulnerabilities to do hurt. These dangers may imperil information classification, information respectability, and information accessibility. Some untrusted suppliers could conceal information breaks to spare their notorieties or free some space by erasing the less utilized or got to information.

1.5 Security Consideration in Cloud Data Storage

1.5.1 Data Loss

Organizations are outsourcing their whole information to cloud specialist organizations. In view of the minimal effort rate that the cloud offers, the clients should make a point not to uncover their vital information to dangers due to the numerous approaches to bargain their information. In distributed computing, the dangers are going up in light of the fact that there are dangers that is recently confronting the cloud and did not occur to customary processing, and difficulties going for broke. There are numerous conceivable outcomes of losing information because of a pernicious assault and in some cases because of server crashes or unexpected erasure by the supplier without having reinforcements.

Disastrous occasions like a quake and fire could be the reasons for misfortune. Likewise, any occasion that prompts hurting the encryption keys could prompt information misfortune. Keeping in mind the end goal to abstain from losing the information, there are numerous arrangements proposed.

1.5.2 Malicious Insiders

Malevolent insiders are the general population who are approved to deal with the information, for example, database managers or workers of the organization offering cloud administrations, accomplices, and temporary workers who approach the information. Those individuals can take or degenerate the information whether they are getting paid by different organizations or to simply hurt an organization. Indeed, even the cloud suppliers may not know about that as a result of their failure in dealing with their representatives.

1.5.3 Privacy Design Goals

Design Goals to enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantees.

1. *Public audit ability*: to enable TPA to check the accuracy of the cloud information on request without recovering a duplicate of the entire information or acquainting extra online weight with the cloud clients.
2. *Storage correctness*: to guarantee that there exists no conning cloud server that can pass the TPA's review without for sure putting away clients' information in place.
3. *Privacy-preserving*: to guarantee that the TPA can't get clients information content from the data gathered amid the inspecting procedure.

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

4. *Batch auditing*: to empower TPA with secure and effective examining ability to adapt to various reviewing appointments from conceivably vast number of various clients at the same time.
5. *Lightweight*: to enable TPA to perform evaluating with least correspondence and calculation overhead.

The gigantic measure of outsourced information, alongside the CU's constrained assets, can introduce an overwhelming test for inspectors while looking at a cloud benefit. One answer for this issue is to keep up a low level of distributed storage overhead utilizing insignificant information recovery activities. Despite the fact that we confront these difficulties, it is still of most extreme significance to create trust between the CUs and CSPs.

This is the place TPAs could help with ensuring the CU's information security. Through a reasonable and fair-minded reviewing process and additionally the protection of the CU's computational assets, a higher standard could be set for confide in cloud administrations. This evaluating procedure could likewise help in enhancing the gave by cloud-based stages and assets. In the field of information security and protection, the likelihood of an insider risk can't be kept away from. This raises the worry that a TPA could be malignant. The TPA will have free and open access to the CU's information and the cloud administrations, which leaves the CU helpless against assaults. Along these lines, to dodge potential monetary misfortunes or insider dangers, a strict check and adjust process over the TPA execution should exist.

1.6 Scope of the Paper

Out in the open distributed computing, the customers store their gigantic information in the remote open cloud servers. Propose a multilevel round arbitrary key arrangement outsider verification for secured information stockpiling in cloud. Since the put away information is outside of the control of the customers, it involves the security chances regarding secrecy, trustworthiness and accessibility of information and administration. Remote information honesty checking is a crude which can be utilized to persuade the cloud customers that their information are kept in place. In some extraordinary cases, the information proprietor might be limited to get to general society cloud server, the information proprietor will assign the errand of information preparing and transferring to the outsider, for instance the intermediary.

1.6.1 Motivation of the Project

We propel people in general reviewing arrangement of information stockpiling security in Cloud Computing and give a protection safeguarding examining convention, i.e., our plan empowers an outer inspector to review client's outsourced information in the cloud without taking in the information content. To the best of our insight, our plan is the first to help adaptable and productive open inspecting in the Cloud Computing. In particular, our plan accomplishes bunch inspecting where numerous designated reviewing errands from various clients can be performed at the same time by the TPA.

In public cloud environment, most clients upload their data to PCS and check their remote data's integrity by Internet. When the client is an individual manager, some practical problems will happen. If the manager is suspected of being involved into the commercial fraud, he will be taken away by the police.

II. LITERATURE SURVEY

2.1 "Above The Clouds: A View Of Cloud Computing", Michael Armbrust, Armando Fox, 2010

Cloud computing alludes to both the applications conveyed as administrations over the Internet and the equipment and frameworks programming in the datacenters that give those administrations. The administrations themselves have for some time been alluded to as Software as a Service. The datacenter equipment and programming is the thing that we will call out loud. One of the troublesome difficulties in Cloud Computing is including blunders in these expansive scale scattered frameworks. A typical event is that these bugs can't be imitated in littler designs, so the troubleshooting must happen at scale in the generation server farms. One break might be the dependence on virtual machines in Cloud Computing.

2.2 "Toward Secure And Dependable Storage Services In Cloud Computing", Kui Ren, 2012

So as to address this new issue and further accomplish a safe and tried and true distributed storage benefit, we past in this paper an adaptable appropriated stockpiling uprightness inspecting system, using the homomorphic token and dispersed eradication coded information. The past plan enables clients to review the distributed storage with exceptionally lightweight correspondence and calculation cost. The examining result guarantees solid distributed storage accuracy ensure, as well as all the while accomplishes quick information blunder confinement, i.e., the ID of getting out of hand server. Considering the cloud information are dynamic in nature, the past plan additionally bolsters secure and productive dynamic activities on outsourced information, including piece change, erasure, and affix. Examination demonstrates the past plan is exceedingly productive and versatile against Byzantine disappointment, vindictive information alteration assault, and significantly server conniving assaults. Information excess can be utilized with a method of deletion remedying code to additionally endure shortcomings or server crash as client's information develop in size and significance.

2.3 "A Dynamic Secure Group Sharing Frameworkin Public Cloud Computing",Kaiping Xue,2014

The cloud supplier can't be dealt with as a trusted outsider due to its semi-confide in nature, and along these lines the

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

conventional security models can't be clearly summed up into cloud based gathering sharing systems. In this earlier a novel secure gathering sharing system for open cloud, which can successfully exploit the Cloud Servers' assistance however have no touchy information being presented to aggressors and the cloud supplier? The system joins intermediary signature, upgraded TGDH and intermediary re-encryption together into a convention. By applying the intermediary signature system, the gathering pioneer can adequately allow the benefit of gathering administration to at least one picked amass individuals. The improved TGDH conspire empowers the gathering to arrange and refresh the gathering key sets with the assistance of Cloud Servers, which does not require the greater part of the gathering individuals been online constantly.

2.4 "Addressing Cloud Computing Security Issues",Dimitrios Zissis, Dimitrios Lekkas, 2012

Cloud computing incorporates components from network processing, utility registering and autonomic figuring, into an imaginative organization engineering. This quick progress towards the mists, has fuelled worries on a basic issue for the achievement of data frameworks, correspondence and data security. From a security point of view, various unchartered dangers and difficulties have been acquainted from this movement with the mists, breaking down a great part of the adequacy of customary insurance components. Accordingly the point of this paper is twofold; right off the bat to assess cloud security by recognizing one of a kind security prerequisites and besides to endeavor to show a suitable arrangement that disposes of these potential dangers. This paper proposes presenting a Trusted Third Party, entrusted with guaranteeing particular security qualities inside a cloud situation.

2.5 "Relational Cloud: A Databases Service For The Cloud",Carlo Curino, Evan P. C. Jones, 2011

A SaaS guarantees to move a significant part of the operational weight of provisioning, design, scaling, execution tuning, reinforcement, protection, and access control from the database clients to the administration administrator, offering lower general expenses to clients. Early SaaS endeavors incorporate Amazon RDS and Microsoft SQL Azure, which are promising as far as setting up the market requirement for such an administration, however which don't address three essential difficulties: productive multi-tenure, versatile adaptability, and database protection. We contend that these three difficulties must be overcome before outsourcing database programming and administration winds up alluring to numerous clients, and financially savvy foodservice suppliers.

III. EXISTING SYSTEM

Ventures and people outsource database to acknowledge helpful and ease applications and administrations. So as to give adequate usefulness to SQL inquiries, numerous safe database plans have been proposed. Be that as it may, such plans are powerless against protection spillage to cloud server. The principle reason is that database is facilitated and handled in cloud server, which is outside the ability to control of information proprietors. For the numerical range inquiry (">", "<", and so forth.), those plans can't give adequate security insurance against viable difficulties, e.g., protection spillage of factual properties, get to design. Moreover, expanded number of inquiries will definitely release more data to the cloud server. In earlier proposition a two-cloud design for secure database, with a progression of crossing point conventions that give protection safeguarding to different numeric-related range inquiries. Security examination demonstrates that security of numerical data is unequivocally ensured against cloud suppliers in past plan.

The two mists cooperate to react each question ask for from the customer/approved clients (accessibility). For protection concerns, these two mists are thought to be non-intriguing with each other, and they will take after the crossing point conventions to save security of information and inquiries (privacy).In our plan, the learning of put away database and questions is divided into two sections, separately put away in one cloud. The system ensures that knowing both of these two sections can't acquire any valuable protection data to direct a safe database, information are encoded and outsourced to be put away in one (Cloud An), and the private keys are put away in the other one (Cloud B).

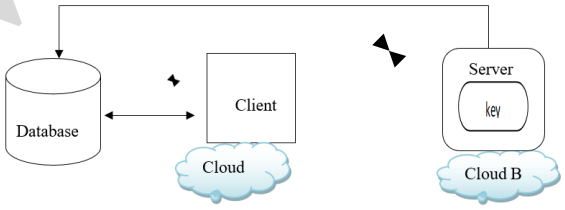


Fig 5.1 Knowledge Partition of Stored Data

3.1 Disadvantages

- *User:* clients, who have information to be put away in the cloud and depend on the cloud for information calculation, comprise of both individual shoppers and associations.
- *Cloud Service Provider*: a CSP, who has huge assets and aptitude in building and overseeing disseminated distributed storage servers, claims and works live Cloud Computing frameworks.
- *Third Party Auditor*: a discretionary TPA, who has ability and capacities that clients might not have, is trusted to evaluate and uncover danger of distributed storage benefits for the clients upon ask.

IJSMS

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

- Focus on security safeguarding mining on vertically apportioned databases not have an information protection in Data Owner.
- The resource consumption at the data owner end is very low.

3.2 Proposed System

We aim to build a secure system that can fend off both external and internal attackers. Much previous work deal with issues related to external attackers. Our system combines many existing techniques which we explain in the following sections. We summarize the interaction roles of the system in multilevel round random key policy third party authentication. Data availability has a very high priority in any company operations. In our system, all data are stored encrypted. The backup of the database is performed regularly by the cloud service, in addition we require a backup of the Encryption Proxies with the corresponding decryption keys for the system integrity. A privacy-preserving outsourced frequent data for vertically partitioned databases. This allows the data owners to outsource mining task on their joint data in a privacy-preserving manner.

Based on this solution, we built a privacy-preserving multilevel round random key policy third party authentication solution for vertically partitioned databases. Our solutions protect data owner's raw data from other data owners and the cloud. Our solutions also ensure the privacy of the mining results from the cloud. Compared with most existing solutions, our solutions leak less information about the data owners raw data analysis techniques, are generally used for discovering frequently co-occurring data and interesting association relationships between data respectively in large transaction databases.

Focus on privacy preserving mining on vertically partitioned databases. In such a scenario, data owners wish to learn the key exposure data polices from rule sets from a collective dataset, and disclose as little information about their (sensitive) raw data as possible to other data owners and third parties. To ensure data privacy, we design an efficient homomorphism encryption scheme and a secure comparison scheme.

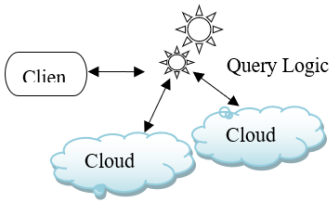


Fig 5.2 Knowledge Partition of Query Logic

3.4 Advantages of Proposed System

- Our evaluation has also demonstrated that our solutions are very efficient.
- An efficient homomorphism encryption scheme and a secure outsourced comparison scheme were presented.
- Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.
- Unlike most prior works for ensuring remote data integrity, the new scheme
- supports secure and efficient dynamic operations on data blocks, including: update, delete and append.

IV. SYSTEM IMPLEMENTATION

Microsoft SQL Server is a relational database management system developed by Microsoft. As a database, it is a software product whose primary function is to store and retrieve data as requested by other software applications, be it those on the same computer or those running on another computer across a network (including the Internet). There are at least a dozen different editions of Microsoft SQL Server aimed at different audiences and for workloads ranging from small single-machine applications to large Internet-facing applications with many concurrent users. Its primary query languages are T-SQL and ANSI SQL. Fig 5.3 System Flow diagram shows how the data is encrypted and stored in the cloud and sent to the another user.

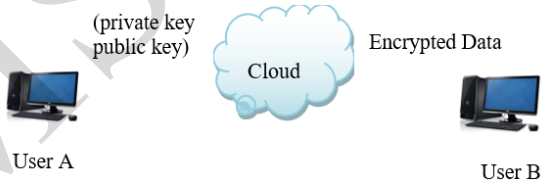


Fig 5.3 System flow Diagram

5.1 Modules

In this section, we outline the substitution cipher, crypto-graphic hash function and homomorphic encryption, which serve as the building blocks in our privacy-preserving data mining solutions.

1. Substitution Cipher and Frequency Analysis
2. Cryptographic Hash Function
3. Homomorphic Encryption

5.1.1 Substitution Cipher and Frequency Analysis

A substitution cipher encrypts a message by substituting the units of the message with cipher text units according to a substitution alphabet. Substitution cipher has been used in outsourced association rule mining and frequent item set mining. In such use cases, the message units are the items in a transaction database. Let Σ be the plaintext alphabet including all unique items appearing in a database. Every item in Σ has a corresponding unique cipher text. A substitution To encrypt the database, all items in the database are replaced with their corresponding cipher texts.

IJSMS

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

- *Homophonic substitution:* Utilization of homophones — a few contrasting options to the most widely recognized letters in generally mono alphabetic substitution figures. For instance, for English, both X and Y figure content may mean plaintext E.
- *Polyalphabetic substitution:* The use of several alphabets chosen in assorted, more or less devious.
- *Polygraphic substitution:* Plans where sets or triplets of plaintext letters are dealt with as units for substitution, as opposed to single letters, for instance, the Play reasonable figure imagined by Charles Wheatstone in the mid-nineteenth century.

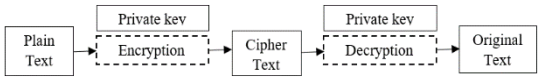


Fig 5.4 Process of Data Encryption

5.1.2 Cryptographic Hash Function

Aggressors with some information of the frequencies of message units or unit gatherings can recoup some plaintext through recurrence examination. For instance, if an aggressor realizes that bread and drain are the most and second most successive things in an exchange database, the assailant can construe that the most and second most incessant figure content units in the encoded database compare to bread and drain, individually. To counter recurrence investigation assault, invented things or exchanges can be added to shroud thing recurrence.

A cryptographic hash work is an uncommon class of hash work that has certain properties which make it appropriate for use in cryptography. It is a numerical calculation that maps information of subjective size to a bit string of a settled size (a hash) and is intended to be a restricted capacity, that is, a capacity which is infeasible to rearrange. The best way to reproduce the info information from a perfect cryptographic hash capacity's yield is to endeavor a savage power hunt of conceivable contributions to check whether they create a match, or utilize a rainbow table of coordinated hashes. Bruce Schneierhas called one-way hash works "the workhorses of present day cryptography. The info information is frequently called the message, and the yield (the hash esteem or hash) is regularly called the message process or just the process.

Cryptographic hash capacities have numerous data security applications, strikingly in computerized marks, message validation codes (MACs), and different types of confirmation. They can likewise be utilized as customary hash capacities, to list information in hash tables, for fingerprinting, to distinguish copy information or extraordinarily recognize documents, and as check aggregates to identify inadvertent information defilement. For sure, in data security settings, cryptographic hash esteems are some of the time called (computerized) fingerprints, checksums, or simply hash esteems, despite the fact that every one of these terms remain for more broad capacities with rather unique properties and purposes.

5.1.3 Homomorphic Encryption

Homomorphism encryption conspire permits at least one plain-content tasks (e.g expansion and duplication) to be done on the figure writings. On the off chance that the expansion activity is permitted, at that point the plan is known as added substance homomorphism encryption. On the off chance that the duplication task is permitted, at that point the plan is known as multiplicative homomorphic encryption.

The motivation behind homomorphic encryption is to permit calculation on encoded information. Distributed computing stages can perform troublesome calculations on homomorphically encoded information while never approaching the decoded information. Homomorphic encryption can likewise be utilized to safely chain together extraordinary administrations without uncovering touchy information. For instance, administrations from various organizations can figure the expense, the money conversion scale, shipping, on an exchange without uncovering the decoded information to every one of those administrations. Homomorphic encryption can likewise be utilized to make other secure frameworks, for example, secure voting frameworks, crash safe hash capacities, and private data recovery plans. Homomorphic encryption plans are naturally pliant. As far as flexibility, homomorphic encryption plans have weaker security properties than non-homomorphic plans.

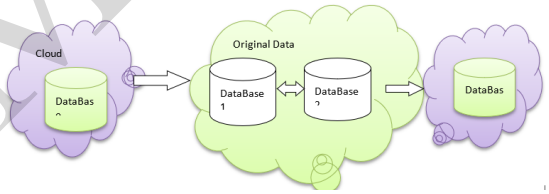


Fig 5.5 Data Flow Diagram

The above fig shows how data is stored and accessed from the cloud. The keys are stored in one database and information are stored in another database.

V. RESULTS OF EXPERIMENTS

Step 1:

The Server is logged in and the same way the owner is also logged in and the new owner can register their id.

IJSMS

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

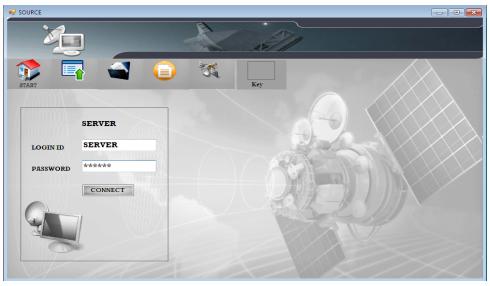


Fig 6.1 Login Page

Step 2:

The files are uploaded and the nodes are selected for the data processing.

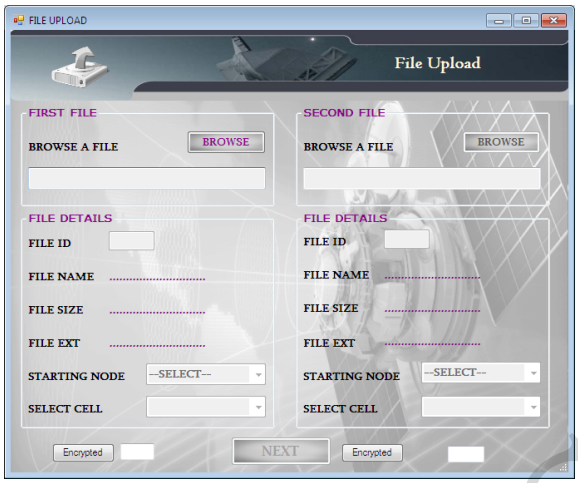


Fig 6.2 Uploading a file

Step 3:

The uploaded files are viewed here and requests to the file are given here.

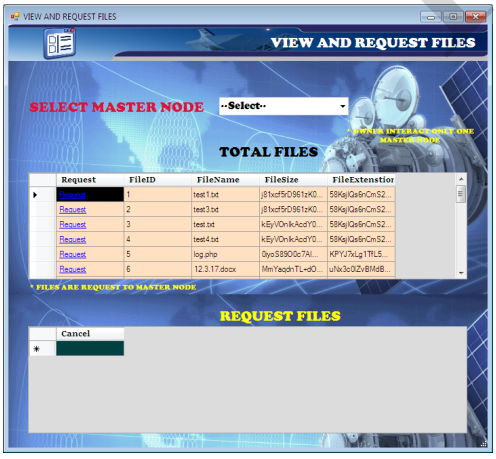


Fig 6.3 Viewing and requesting the files

Step 4:

Finally the transactions for the files are done here. The requested files can be downloaded by giving correct id and key.



Fig 6.4 Transaction page

VI. CONCLUSION AND FUTURE WORK

In this proposal, we intent a privacy-preserving outsourced multi-level round random key policy third party authentication to the partitioned databases. This allows the data owners to outsource privacy task on their joint data in a privacy-preserving manner. Based on this solution, we built a privacy-preserving round random crypto policy to secure the two cloud databases. Our solutions protect data owner's raw data from other data owners and the cloud.

In the future work, we will implement client side uploading, reducing time complexity and further increasing of security to the data.

REFERENCES

1. Kaiping Xue, Shaohua Li, Jianan Hong, Yingjie Xue, Nenghai Yu and Peilin Hong, "Two-Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving", IEEE Transactions on Information Forensics and Security, 2017.
2. ANSI, X3-135, "American national standard for information systems: Database language SQL," American National Standards Institute, NY, 1986.
3. C.Wang, Q.Wang, K.Ren, N.Cao, and W.Lou, "Toward secure anddependable storage services in cloud computing," IEEE Transactions onServices Computing, vol. 5, no. 2, pp. 220–232, 2012.
4. C.Curino, E.P.Jones, R.A.Popa, N.Malviya et al., "Relational cloud:A database-as-a-service for the cloud," 2011, http://hdl.handle.net/1721.1/62241.
5. D.Zissis and D.Lekkas, "Addressing cloud computing security issues,"Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)

6. D.Boneh, D.Gupta, I.Mironov, and A.Sahai, "Hosting services onan untrusted cloud," in Advances in Cryptology-EUROCRYPT 2015.Springer, 2015, pp. 404–436.
7. E. Stefanov and E. Shi, "Multi-cloud oblivious storage," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, 2013, pp. 247–258.
8. E. Stefanov and E. Shi, "Oblivistore: High performance oblivious cloud storage," in Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP'13). IEEE, 2013, pp. 253–267.
9. H.T.Dinh, C.Lee, D.Niyato, and P.Wang, "A survey of mobilecloud computing: architecture, applications, and approaches," WirelessCommunications and Mobile Computing, vol. 13, no. 18, pp. 1587–1611,2013.
10. H.Kadhem, T.Amagasa, and H. Kitagawa, "MV-OPES: Multivaluedorder preserving encryption scheme: A novel scheme for encrypting integer value to many different values," IEICE Transactions on Information and Systems, vol. 93, no. 9, pp. 2520–2533, 2010.
11. ISO9075, "Information processing systems. database language SQL," 1987.
12. J.W.Rittinghouse, J.F.Ransome, Cloud implementation, management and security. CRC press, 2016.
13. J. Katz and Y. Lindell, Introduction to modern cryptography. CRC press, 2014.
14. K.Xue, Y.Xue, J.Hong,W. Li, H.Yue, D.S.Wei, and P.Hong, "RAAC:Robust and auditable access control with multiple attribute authoritiesfor public cloud storage," IEEE Transactions on Information Forensicsand Security, vol. 12, no. 4, pp. 953–967, 2017.
15. K.Xue and P.Hong, "A dynamic secure group sharing frameworkin public cloud computing," IEEE Transactions on Cloud Computing,vol. 2, no. 4, pp. 459–470, 2014.
16. M.Armbrust, A.Fox, R.Griffith, A.D.Joseph et al., "A view of cloudcomputing," Communications of the ACM, vol. 53, no. 4, pp. 50–58,2010.
17. M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "Cloud computing security: from single to multi-clouds," in Proceedings of the 45th Hawaii International Conference on System Science (HICSS2012). IEEE, 2012, pp. 5490–5499.
18. O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious RAMs," Journal of the ACM, vol. 43, no. 3, pp. 431–473, 1996.
19. O. Goldreich, Foundations of cryptography: volume 2, basic applications. Cambridge university press, 2009.
20. P.Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in Cryptology-EUROCRYPT'99. Springer, 1999, pp. 223–238.
21. R.A.Popa, C.Redfield, N.Zeldovich, and H.Balakrishnan, "CryptDB:protecting confidentiality with encrypted query processing," in Proceedingsof the 23rd ACM Symposium on Operating Systems Principles.ACM, 2011, pp. 85–100.
22. R.A.Popa, F.H.Li, and N.Zeldovich, "An ideal-security protocol fororder-preserving encoding," in Proceedings of the 2013 IEEE Symposiumon Security and Privacy (SP'13). IEEE, 2013, pp. 463–477.
23. S.Benabbas, R.Gennaro, and Y.Vahlis, "Verifiable delegation ofcomputation over large datasets," in Annual Cryptology Conference.Springer, 2011, pp. 111–131.
24. S. R. Ganta, S. P. Kasiviswanathan, and A. Smith, "Composition attacks and auxiliary information in data privacy," in Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM, 2008, pp. 265–273.
25. W.Li, K.Xue, Y.Xue, and J.Hong, "TMACS: A robust and verifiablethreshold multi-authority access control system in public cloud storage,"IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 5,pp. 1484–1496, 2016.
26. X.Chen, J.Li, J.Weng, J.Ma, and W.Lou, "Verifiable computation over large database with incremental updates," IEEE Transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016.
27. X. Wu, X. Zhu, G.-Q. Wu, and W. Ding, "Data mining with big data," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 1, pp. 97–107, 2014.
28. Y. Dou, K. C. Zeng, H. Li, Y. Yang, B. Gao, K. Ren, and S. Li, "P 2 - SAS: Privacy-preserving centralized dynamic spectrum access
29. Yang, H. Li, M. Wen, H. Luo, and R. Lu, "Achieving ranked range query in smart grid auction market," in 2014 IEEE International Conference on Communications (ICC2014). IEEE, 2014, pp. 951–956.
30. Z. Liu, X. Chen, J. Yang, C. Jia, and I. You, "New order preserving encryption model for outsourced databases in cloud environments," Journal of Network and Computer Applications, vol. 59, pp. 198–207, 2016.

IJSMS

This is an open access article under the CC BY-SA 4.0 license (https://creativecommons.org/licenses/by-sa/4.0/)