SECURE AND EFFICIENT DATA OUTSOURCING IN CLOUD USING SESSION KEY ALGORITHM

Sridharan S[1], Kaviya K[2], Nanthini A[3], Deepika K [4]

[1]*Assistant Professor & Head, University college of Engineering, Thirukkuvalai, Tamilnadu, India*
[2,3,4] *Student , University college of Engineering, Thirukkuvalai, Tamilnadu, India*

---***---

Abstract - In the present scenario businesses and people are outsourcing database to accomplish helpful administrations and minimal effort applications. These are buried in the cloud server, which is outside the ability to control of the data proprietor The SQL Queries require a few secure database schemes for its indisputable functioning, yet this at elongated previous prompts privacy spillage to the cloud server. For numerical range inquiry (>, <, and so forth.) these neglect to give adequate security insurance. A portion of the difficulties faced are privacy leakage of statistical attributes, access patterns and so on. Likewise increased number of queries will release more information to the cloud server. Thus regarding these issues numerous works have been done by various researchers. We have studied some of these research works and analyzed the best possible ways to come to the desired level of privacy preservation in the case of cloud computing.

Keywords: Index Terms—database, range query, privacy preserving, cloud computing.

INTRODUCTION

The increasing industry of cloud has provide a service paradigm of storage/computation outsourcing helps to reduce users' burden of IT infrastructure maintenance, and reduce the cost for both the enterprises and individual users. However, due to the privacy concerns that the cloud service provider is assumed semi-trust (honest-but curious.), it becomes a critical issue to put sensitive service into the cloud, so encryption or obfuscation are wanted prior to outsource sensitive information - such as database scheme - to cloud.

The privacy challenge of outsourced database is two-hold. 1) Sensitive data is stored in cloud, the corresponding private information may be exposed to cloud servers; 2) Besides data privacy, clients' frequent queries will inevitably and gradually reveal some private information on data statistic properties. Thus, data and queries of the outsourced database should be protected against the cloud service provider.

One straightforward approach to mitigate the security risk of privacy leakage is to encrypt the private data and hide the query/access patterns. Unfortunately, as far as we know, few academia researches satisfy both properties so far.

The main contribution of this paper can be summarized as follows: 1)In the propose a two non-colluding cloud architecture to conduct a secure database service, in which the data is stored in one cloud, while the knowledge of query pattern is well partitioned into two parts, and knowing only one cannot reveal any private information; 2) In the present a series of intersection protocols to provide numeric-related SQL range query with privacy preservation, and especially, such protocols will not expose order-related information to any of the two non-colluding clouds.

The two clouds work together to respond each query request from the client/authorized users (availability). For privacy concerns, these two clouds are assumed to be non-colluding with each other, and they will follow the intersection protocols to preserve privacy of data and queries (privacy).

RELATED WORKS

In [1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph et al presents Cloud Computing, the long-held nightmare of subtract as a utility, has the probable to transform a huge part of the IT industry, making software even more striking as a service and determining the system IT hardware is designed and purchased. Developers with imaginative thoughts for pioneering Internet armed forces no longer necessitate the great resources outlay in hardware to deploy their service or the being expense to operate it. They need not be concerned about over-provisioning for a overhaul whose reputation does not meet their predictions, thus murder expensive resources, or under-provisioning for one that become wildly conventional, thus absent potential customers and proceeds. Moreover, company with immense batch-oriented odd jobs can acquire cost as speedily as their agenda can degree, since by 1000 servers for one hour costs no added than using one server for 1000 hours.

In [2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou et al presents Cloud storage enable users to distantly ensue their data and take happiness in the on-demand high advantage cloud application lacking the burden of cramped hardware and software government. Though the recompense are apparent, such a overhaul is also relinquish users' corporeal possession of their outsourced information, which unavoidably poses new security risks toward the correctness of the data in cloud. In order to tackle this novel predicament and additional attain a secure and dependable cloud storage service, we recommend in this term paper a reproduction disseminated storage integrity auditing mechanism, utilize the homomorphism coupon and distributed erasure-coded information. The proposed design allows users to review the cloud storage with incredibly frivolous communiqué and computation cost. The auditing products not only ensure brawny cloud storage exactness promise, but also alongside attain speedy information error localization, i.e., the classification of disobedient server.

In [3] K. Xue and P. Hong et al The reputation of collection information allocation in public obscure computing, the solitude and safety of group sharing data have become two major issues. The cloud provider cannot be treated as a trusted third party because of its semi-trust nature, and thus the traditional security models cannot be straightforwardly generalized into cloud based group sharing frameworks. In this document, we suggest a narrative protected assembly allocation framework for public cloud, which can effectively take advantage of the Cloud Servers' assist but have no sensitive data being exposed to attackers and the cloud provider. The framework combines proxy signature, enhanced *TGDH* and proxy re-encryption together into a protocol. By applying the proxy signature technique, the group leader can effectively grant the privilege of group management to one or more chosen group members.

In [4] D. Zissis and D. Lekkas et al presents the relevant form of cloud computing has fundamentally distorted everyone's alertness of transportation architectures, software delivery and development models. Extrapolative as an evolutionary footstep, consequent the changeover from processor computers to client/server deployment models, cloud computing encompasses elements from grid computing, utility computing and autonomic compute, into an imaginative exploitation construction. This be set to modification towards the vapors, has fuel nervousness on a sober issue for the achievement of information systems, communication and information security. From a security perception, figures of unchartered risks and challenge have been introduced from this rearrangement to the clouds, decline much of the efficiency of conventional protection mechanisms. As an ending the happening of this text is twofold; firstly to estimate cloud haven by identifying unique security necessities and secondly to effort to there a viable clarification that eliminate these potential threats.

In [5] H. T. Dinh , C. Lee, D. Niyato, and P. Wang et al presents An unbalanced mellowness of the impermanent application and endowed of cloud computing thought, mobile cloud computing (MCC) has been introduce to be a potential expertise for mobile services. MCC integrates the cloud computing into the mobile environment and overcomes obstacles related to the performance (e.g., battery life, storage, and bandwidth), environment (e.g., heterogeneity, scalability, and availability), and security (e.g., reliability and privacy) discuss in mobile computing. This paper gives a survey of MCC, which helps universal readers have an overview of the MCC counting the definition, architecture, and applications. The issue, presented solution, and draw near are obtainable. In totaling, the prospect investigate directions of MCC are discussed. Mobile devices (e.g., Smartphone and capsule PC) are ever more attractive an essential part of human life as the nearly all successful and opportune statement utensils not restricted by time and place.

PROPOSED SYSTEM

In the proposed system design and implementation of a cloud-based storage scheme that has the following features: It allows a data owner to outsource the data to a CSP, and perform full dynamic operations at the block-level, i.e., it supports operations such as block modification, insertion, deletion, and append. It ensures the newness property, i.e., the authorized users receive the most recent version of the outsourced data. It establishes indirect mutual trust between the data owner and the CSP since each party resides in a different trust. It enforces the access control for the outsourced data.CSP------Cloud Service Providers.

MODULE SPECIFICATION

- ❖ Picture Selection Phase
- ❖ File encryption
- ❖ File upload to Service Providers
- ❖ Dynamic Operations on the Outsourced Data
- ❖ Data Access and Cheating Detection
- ❖ File decryption

Picture Selection Phase

In picture selection phase user select any image as passwords and consist of a sequence of click-points on a given image. Users may select any pixels in the image as click-points for their password. During password formation, the majority of the image is dim excluding for a minute sight haven area that is randomly positioned on the image. Users must select a click-point within the view port. If they are incapable or disinclined to choose a summit in the current view port, they may press the Shuffle button to randomly reposition the view port.

File encryption

The first module in this project is file encryption module. This module is designed for encrypt the file before outsourcing the file into cloud service providers. The encryption process done by the dynamic data owner to prevent their data from the unauthorized users. During the encryption time the secret key for the file to decrypt the file is produced. The owner has to keep the secret key. When they are retrieving the data from the cloud service providers the data will be in encrypted form. So this module plays an important role in our project.

File upload to Service Providers

The data owner can not directly upload their files into the cloud service providers. The data owner first has to upload their files into the Trusted Third Party. The TTP in our project is a trusted intermediate between the cloud service providers and the data owner. The TTP first receives the data from the data owner and forward the file to the cloud service providers, when the file is receives at cloud service providers from the TTP then it sends a confirmation mail that the file is uploaded at the cloud service providers to the data owner.

Dynamic Operations on the Outsourced Data

The data owner can modify their file after uploading their file into the cloud service providers. They can do the operations dynamically on the data. So the authorized users can access recently updated version of the outsourced data. Only the data owner can change the data dynamically. The data can be deleted, updated or edited by the data owner.

Data Access and Cheating Detection

An authorized user sends a data-access request to both the CSP and the TTP to access the outsourced file. The outsourced data can be only retrieved by the authorized users. The TTP has to check whether the users are authorized persons or not. To check the authorization the CSP and the TTP check the secret key of the particular file which has the data request by the users. If the secret key matches with the database then only they can download the file and decrypt it. if there any unauthorized users try to access the data the notification will send to the TTP.

File decryption

The last module in this project is file decryption. In this module the encrypted file will return back into its original form. For the decryption process the algorithm need the key which created at the time of encryption. The data owner keeps the key generated at encryption process. After enter the key the algorithm will decrypt the file and returns the data in a readable manner.

ARCHITECTURE DIAGRAM

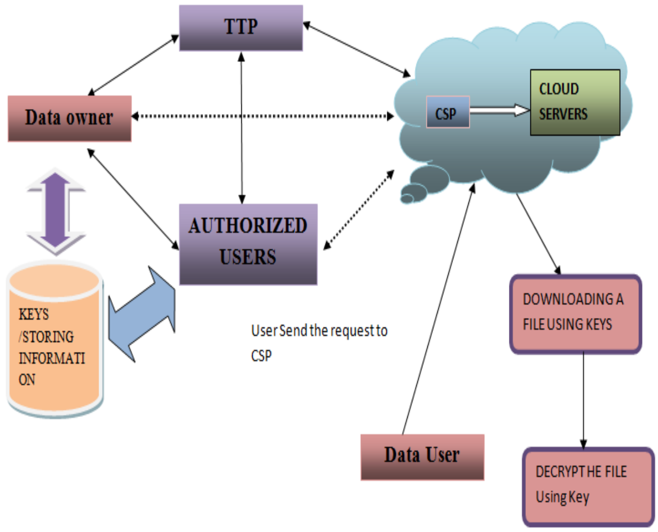
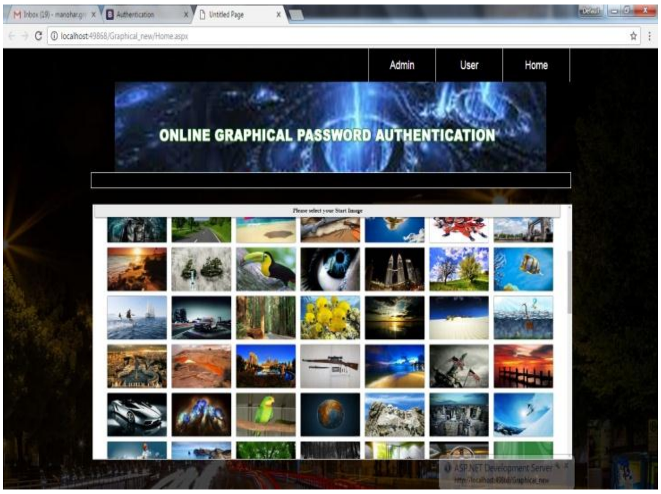
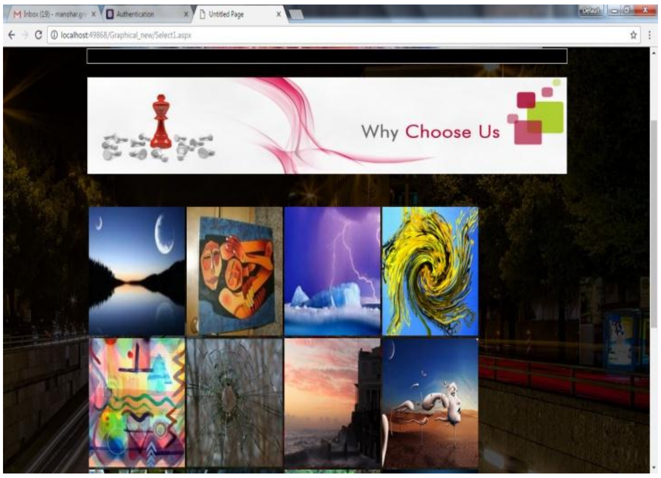

TTP
Data owner
CSP
CLOUD SERVERS
KEYS /STORING INFORMATI ON
AUTHORIZED USERS
User Send the request to CSP
DOWNLOADING A FILE USING KEYS
Data User
DECRYPT HE FILE Using Key

Fig -1: Architecture Diagram

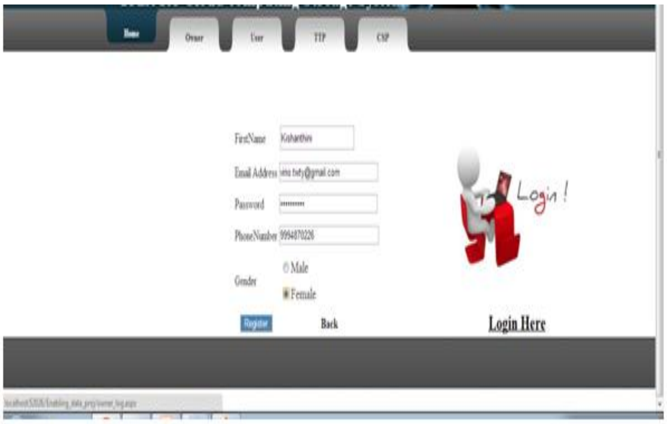
OUTPUT RESULTS


Inbox (19) - manohar.gr
Authentication
Untitled Page
localhost:49868/Graphical_new/Home.aspx
Admin
User
Home
ONLINE GRAPHICAL PASSWORD AUTHENTICATION
Please select your Start Image
ASP.NET Development Server

PICTURE SELECTION

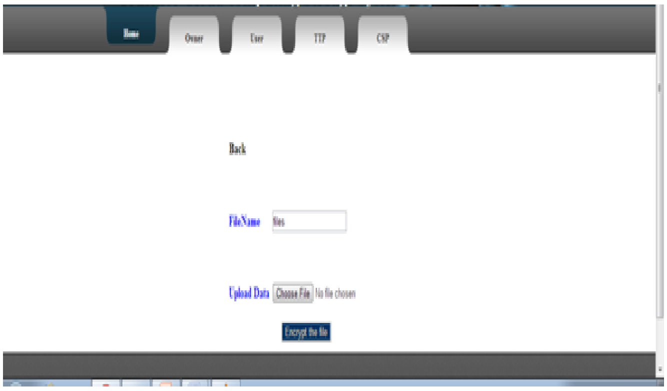


USER REGISTER PROCESS

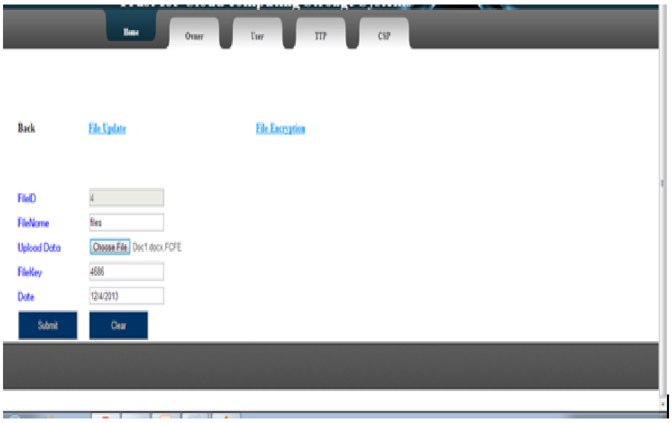


FirstName Kishanthini
Email Address vino.twty@gmail.com
Password ••••••••••
PhoneNumber 9994870226
Gender ○ Male ● Female

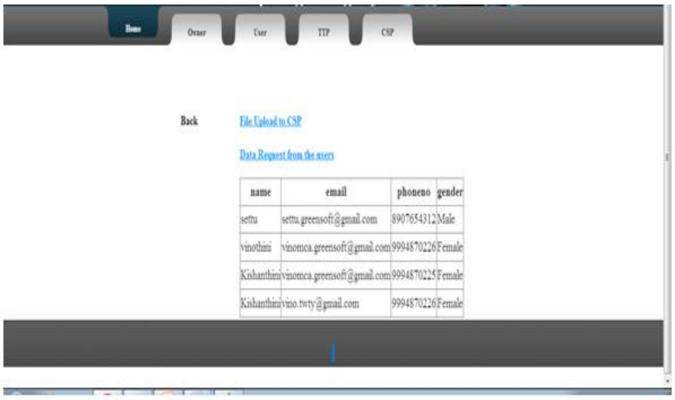
FILE UPLOADING PROCESS



FileName files
Upload Data No file chosen



FileID 4
FileName files
Upload Data Doc1.docx.FCFE
FileKey 4686
Date 12/4/2013



name	email	phoneno	gender
settu	settu.greensoft@gmail.com	8907654312	Male
vinothini	vinomca.greensoft@gmail.com	9994870226	Female
Kishanthini	vinomca.greensoft@gmail.com	9994870225	Female
Kishanthini	vino.twty@gmail.com	9994870226	Female

3. CONCLUSION

In the presented two-cloud architecture with a series of interaction protocols for outsourced database service, which ensures the privacy preservation of data contents, statistical properties and query pattern. At the same time, with the support of range queries, it not only protects the confidentiality of static data, but also addresses potential privacy leakage in statistical properties or after large number of query processes. Security analysis shows that our scheme can meet the privacy-preservation requirements. Furthermore, performance evaluation result shows that our proposed scheme is efficient.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph et al., "A view of cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

[3] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.

[4] J.W. Rittinghouse and J. F. Ransome, Cloud computing: implementation, management, and security. CRC press, 2016.

[5] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.

[6] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wireless Communications and Mobile Computing, vol. 13, no. 18, pp. 1587–1611, 2013.

[7] R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: protecting confidentiality with encrypted query processing," in Proceedings of the 23rd ACM Symposium on Operating Systems Principles. ACM, 2011, pp. 85–100.

[8] 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.

[9] D. Boneh, D. Gupta, I. Mironov, and A. Sahai, "Hosting services on an untrusted cloud," in Advances in Cryptology-