Secure Data Storage in Cloud by Using AES

K.Nikitha[1], Gade Swathi[2]

[1]M.Tech Student, Bharat Institute of Technology & Science for Women
Mangalpally(V), Ibrahimpatnam(M),R.R Dist-501510
, A.P, India

[2]Assistant Professor, Bharat Institute of Technology & Science for Women
Mangalpally(V), Ibrahimpatnam(M),R.R Dist-501510
, A.P, India

Abstract: Cloud computing technology makes it straightforward to store the big quantity of information. For observation the user Associate in Nursing entity whose information to be keep within the cloud and depends on the cloud for information storage and computation, server is Associate in Nursing entity which might be managed by cloud service supplier to supply information storage service Associate in Nursing has vital space for storing and computation resources and third party is an ex gratia TPA World Health Organization has experience and capabilities that users might not have is trustworthy to access and expose risk of cloud storage services on behalf of the users upon request. Our projected work relies on cloud computing design, for analysis is cloud information storage a user stores his information through a CSP into set of cloud servers that square measure running during a coincident co-operated and distributed. The info redundancy is used with technique of erasure correcting code to more tolerate faults. The comparative study represents the protection problems in cloud computing design that have the simplest potency or the simplest learning.

Keywords:-Third Party, Redundancy, Cloud Computing, TPA

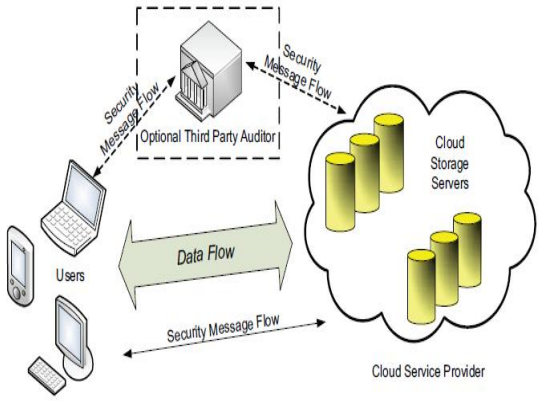
INTRODUCTION:

The Cloud computing is one in all the delivery of computing as a service instead of the merchandise, whereby the shared resources, the package, and data is provided to computers and alternative devices as a metered service over a network. The Cloud computing provides the computation, software, information access, and storage resources while not requiring cloud Users to understand the placement and alternative details of the computing infrastructure. The tip user's access cloud primarily based applications through a browser or a light-weight weight desktop or mobile app whereas the businesses of package and information ar keep on servers at an overseas location. The Cloud application suppliers try to present a similar or higher service and performance as if the package programs were put in regionally on end-user computers. SAAR computing design, reworking Information centres into pools of computing service on a large scale. The increasing network information measure and reliable however versatile network connections create it even potential that users will currently subscribe prime quality services from information and package that reside only on remote information centres.

In order to realize the assurances of the cloud information integrity and convenience and enforce the standard of cloud storage service, economical strategies that area unit modify on-demand information correctness verification on behalf of cloud users ought to be designed. However, the actual fact that during which users now not have physical possession of information within the cloud prohibits the direct adoption of ancient crypto logical primitives for the aim of information integrity protection. Hence, that the verification of cloud storage correctness should be conducted

while not specific information of the entire information files. It's the foremost blessings for individual users to store their information redundantly across multiple physical servers thus on cut back the info integrity and convenience threats. Thus, the distributed protocols for storage correctness assurance are of most importance in achieving sturdy and secure cloud storage systems. during this paper as a complementary approach, we have a tendency to projected distributed protocols.

ARCHITECTURE:



2. LITERATURE REVIEW

CLOUD COMPUTING: ONE SOLUTION TO INFORMATION SUPPORT SYSTEMS (ISS):

Information Support Systems (ISS) are computer technology/network support systems that interactively support the information processing mechanisms for individuals and groups in the life, public, and private organizations, and other entities. Over some decades in the past, organizations have put efforts to be at the forefront of the development and application of computer-based Information Support Systems for collecting, analyze and process the data and generate information to support decisions. The various computing paradigms have been employed for the purpose and needs have emerged for enormous infrastructure, an unlimited system accessibility, cost effectiveness, increased storage, increased automation, flexibility, system mobility and shift of the IT focus. This paper presents a brief evaluation on how Cloud Computing paradigm can be used to meet the increasing demands of the Information Support Systems and how Cloud Computing paradigm can prove to be future solution for such systems.

PROOFS OF THE RETRIEVABILITY: THEORY AND IMPLEMENTATION

A proof of retrievability (POR) is a compact proof by a file system (prover) to a client (verifier) that a target file *F* is intact, in the sense that the client can fully recover it. As PORs incur lower communication complexity than transmission of *F* itself, they are an attractive building block for high-assurance remote storage systems. In this paper, we proposed a theoretical framework for the design of PORs. Our framework improves the previously proposed POR constructions of Juels-Kaliski and Shacham-Waters, and also sheds light on the conceptual limitations of previous theoretical models for PORs. It supports a fully Byzantine adversarial model, carrying only the restriction fundamental to all PORs that the adversary's error rate *to* be bounded when the client seeks to extract *F*. Our techniques support efficient protocols across the full possible range of, up to non-negligibly close to 1. We propose a new variant on the Juels Kaliski protocol and describe a prototype implementation. We demonstrate practical encoding even for files *F* whose size exceeds that of client main memory.

DYNAMIC PROVABLE DATA POSSESSION

As storage-outsourcing services and resource-sharing networks have became popular, the problem of efficiently proving the integrity of data stored at untrusted servers has received increased attention. In the provable data possession (PDP) model, the client preprocesses the data and then

sends it to an untrusted server for storage, while by keeping a small amount of meta-data. This client later asks the server to prove that the stored data has not been tampered with or deleted (without downloading the actual data). However, then the original PDP scheme applies only to static (or append-only) files. The price of dynamic updates is a performance change from O (1) to O (log n) (or O (nọ log n)), for a file consisting of n blocks, while maintaining the same (or better, respectively) probability of misbehavior detection. Our experiments show that this slowdown is very low in practice (e.g., 415KB proof size and 30ms computational overhead for a 1GB file). We also show how to apply our DPDP scheme to outsourced file systems and version control systems (e.g., CVS).

PRIVACY-PRESERVING PUBLIC AUDITING FOR THE SECURE CLOUD STORAGE

Using Cloud Storage, users can remotely Store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable the computing resources, without the burden of all local data storage and maintenance. Thus, the enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. By securely introduce an effective TPA, then the auditing process should bring in no new vulnerabilities towards user data privacy, and it introduce no additional online burden to user. In this paper, we have proposed a secure cloud storage system supporting privacy-preserving public auditing. Further we extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. The extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

3. RELATED WORK

***Problems in existing system*:**

User: an entity, whose data to be stored in the cloud and relies on the cloud for data storage and computation, can be either enterprise or individual customers.

- The data redundancy can be employed with a technique of erasure correcting code to further tolerate faults or server crash as user's data grow in size and importance.
- In the existing system user to audit the cloud storage for very high communication and cost.
- To easily attack the cloud data using different intrusion attacks such as,
  - Malicious attack.
  - Data modification attack.
  - Server clouding attack.

Disadvantages:

- Less control comes with handling over your data and information.
- Dependence on a third party to ensure security and confidentiality of data and information.
- Long-term dependence on cloud host for maintenance of your information.

***Our proposed approach*:**

The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost.

- The proposed design further supports secure and efficient dynamic operations on outsourced data, including the managed control such as,
  - Block modification.

- Deletion.
- Append.

- The cloud data to securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy.

Advantages:

- Access your data at all times – not just while in the office.
- The physical storage centre is no longer needed.
- Cloud storage cost is low, and then most have any pay structure that only calls for payment when used.
- Relieves burden on IT professionals and frees up their time in the office.
- Easily scalable so that the companies can add or subtract resources based on their own needs.

4. RESULTS:

User Registration and Control:

This module can be also used to register users for custom modules that support personalization and user specific handling. If the users wish to create their own user accounts, i.e. register, then registration checks for the username availability and assign unique ID. User Control means controlling the login with referring the username and password which are given during the registration process.

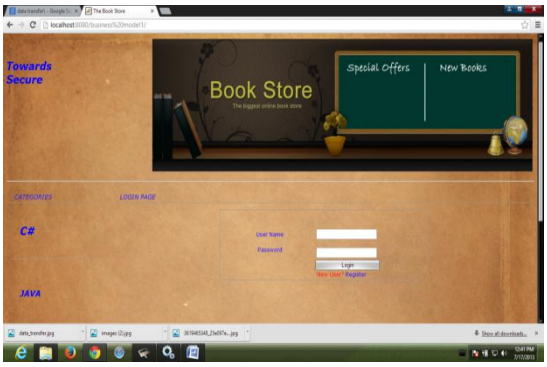


Fig: 4.1 Login page

After login, the user can encrypts the original data and stored it in database, and the user can retrieve the original data which gets decrypted after checking the unique ID and searched data. Based on their logins, they have rights to view, or edit or update or delete the contents of resources. Part of the stored data are confidential, but when these institutions store the data to equipment afforded by cloud computing service provider, priority accessing to the data is not the owner, but it is cloud computing service provider.

Fig: 4.2 Application page

Therefore, there is a possibility that stored confidential data cannot rule out being leaked. Also there is no possibility to track the original data for the hackers.

CRM Service:

This module is customer relationship management, where the user can interact with the application. CRM is concerned with the creation, the development and enhancement of individualised customer relationships with carefully targeted customers and customer groups resulting in maximizing their total customer life-time value. CRM is a business strategy that aims to understand, the anticipate and manage the needs of an organisation's current and potential customers. It has a comprehensive approach which provides

seamless integration of every area of business that touches the customer- namely the marketing, sales, customer services and field support through the integration of the people, technology and the process.

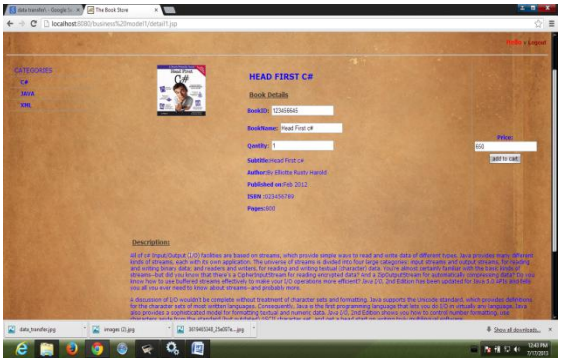


Fig: 4.3 Book details

CRM is a shift from traditional marketing as it focuses on the retention of customers in addition to the acquisition of new customers. The expression of Customer Relationship Management (CRM) is becoming standard terminology, replacing which is widely perceived to be a misleadingly narrow term, relationship marketing (RM). The main purpose of CRM is: The focus [of CRM] is on creating value for the customer and the company over the longer term.

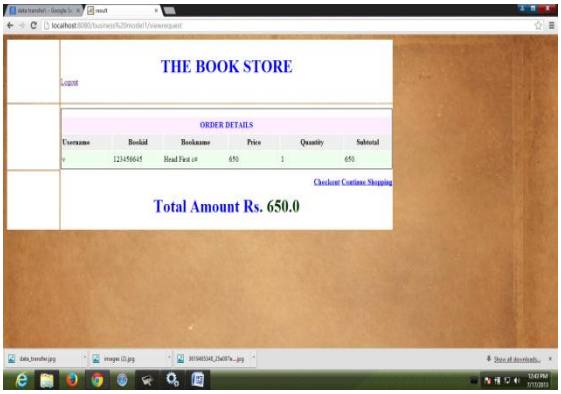


Fig: 4.4 View request

- When customers value the customer service that they receive from suppliers, they are very less likely to look to alternative suppliers for their needs.
- CRM enables organisations to gain 'competitive advantage' over competitors that supply similar products or services.

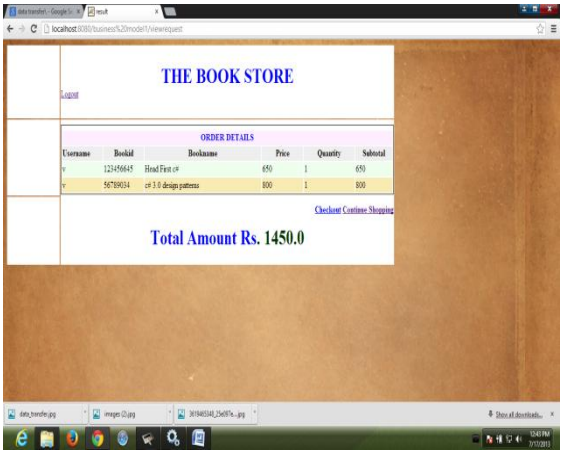


Fig: 4.5 Order details

CRM consists of index page, registration page, login page, etc. Through this, the user can register with the user details, after registration the user can send the original data, which gets encrypted and stored in database; also the user can retrieve the original data which they stored only after decrypting the encrypted data by giving the decryption key.

Encryption/Decryption Service:

This module describes about the encryption and decryption process for the original data. The encryption process is needed while storing the data, and the data decryption is needed while retrieving the data.

After the user's login has been successfully completed, if the CRM Service System requires client information from the user, it sends a request the information (for encryption and decryption) to the Storage Service System.

Fig: 4.6 Data encryption

Encryption: In this (data storage service) the CRM Service System transmits the user ID to the Storage Service System where it searches for the user's data. This original data, once found, a request must be sent to the Encryption/Decryption Service System along with the user ID.

It shows the Storage Service System executing the transmission of client data and the user ID to the Encryption/Decryption Service System. Here, the user sends the original data and it gets encrypted and stored in storage service as per the user request. That data cannot be hacked by unauthorized one that is more confidential and encrypted.

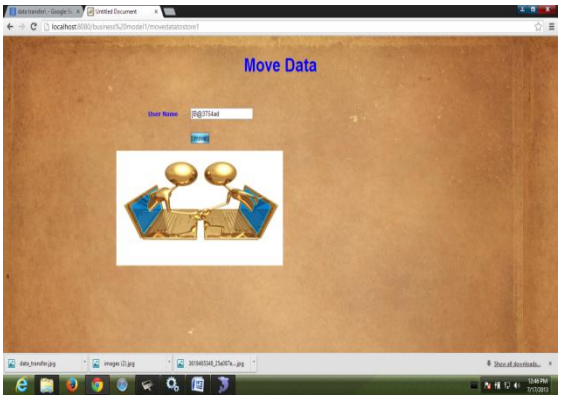


Fig: 4.7 Moving data

Decryption: In this (data retrieval service), if the user request the CRM service to retrieve the data which are stored in Storage service, the CRM sends the user ID and the search data to the Encryption/Decryption Service System.

Fig 4.8 Data decryption

It authenticates whether the user ID and search data are owned by the same user. If authenticated, the encrypted data from the storage service system is send to the Encryption/Decryption Service System for the decryption process. In that process, it checks for decryption key, if it OK, then decrypts the encrypted data and the original data retrieved, and send to the user.

Accessing Storage service

This module describes about how the data gets stored and retrieved from the database. The original data which given by the user gets encrypted and request for the storage, the storage service system store the encrypted data with the user ID for avoiding the misuse of data.

Also during retrieval, the user request for retrieving the data by giving the search data, the storage service system checks for user ID and search data are identical, if so it sends the encrypted data to the Encryption/Decryption Service System for the decryption process, it decrypts the data and sends to the user. The user interacts with the database every time through the CRM service only.

The user's goal in logging into the CRM Service System is possibly to maintain part of the client data, thus the system design must take data maintenance into consideration. Feasible design methods include matching the encrypted client data with the corresponding user ID and client ID, thus allowing for the indexing of the user ID to obtain the corresponding client data. Then the client ID can be used to index the client data the user wishes to maintain. Considering the massive amount of client data, search efficiency could be improved by combining the user ID and client ID to form a combined ID used for searching for a specific client's data.

In the new business model, multiple cloud service operators jointly serve their clients through existing information technologies including various application systems such as ERP, accounting software, portfolio selection and financial operations which may require the user ID to be combined with other IDs for indexing stored or retrieved data. In addition, to this foregoing description of the two systems can use Web Service related technology to achieve operational synergies and data exchange goals.

5. CONCLUSION

In this paper we've enforced information storage that provides a lot of security for data supported cloud. to realize the assurances of cloud information integrity and convenience and enforce the standard of dependable cloud storage service for users, we tend to projected a good and versatile distributed theme with express dynamic information support, together with the block delete, update and append. we tend to place confidence in erasure-correcting code within the file distribution preparation to produce redundancy parity vectors and guarantee the information responsible ness. For utilizing the homomorphism token with distributed verification of erasure coded information, our theme has achieved the combination of storage correctness insurance and information error localization, i.e, whenever the information corruption has been detected throughout the storage correctness verification across by the distributed servers, we will offer nearly guarantee the co-occurring identification of the misbehaving servers.

6. FUTURE ENHANCEMENT

In this paper we've got mentioned regarding 2 secure processes. 1st method is secret writing technique and another method is coding technique. during this paper all we've got enforced 2 levels of security and additionally 2 info's that area unit used as secret writing info and decryption database. In future we are able to use over 2 databases .so that the info movement action is totally different. During this paper we tend to area unit exploitation single time cloud method however in future we tend to can use multi cloud method.

7. REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1-9, July 2009.

[2] Amazon.com, "Amazon Web Services (AWS)," http://aws. amazon.com, 2009.

[3] Sun Microsystems, Inc., "Building Customer Trust in Cloud Computing with Transparent Security," https: //www.sun.com/offers/details/sun_transparency.xml, Nov. 2009.

[4] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[5] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions,"http: //www.techcrunch.com/2006/12/28/gmail-disasterreportsof- mass-email-deletions, Dec. 2006.

[6] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors," http: //www.techcrunch.com/2008/07/10/mediamaxthelinkup-closesits- doors, July 2008.

[7] Amazon.com, "Amazon S3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s320080720.html, July 2008.
[8] S. Wilson, "Appengine Outage," http://www.cio-weblog.com/50226711/ appengine_outage.php, June 2008.
[9] B. Krebs, "Payment Processor Breach May Be Largest Ever,"http: //voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html, Jan. 2009.
[10] A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.

Guide Name: Gade.Swathi
Qualification: M.Tech
Designation: Asst.Professor
Email id: gadeswathi@gmail.com

Student Name: K.Nikitha
Qualification: M.Tech(SE) pursuing
Designation: Student
Email id: knikitha1@gmail.com