

# Secure Public Cloud Using DES Algorithm

**B. Ramya, M.S.Kokila, S.Hemalatha. ,**

Assistant Professors, Department of Computer Applications,  
Kongu Arts and Science College, Erode, India<sup>1</sup>.

**Abstract— Abstract- In this paper, an effective and flexible distributed scheme is proposed with explicit dynamic data support to ensure the correctness of users' data in the cloud. Some part of the data is encrypted in the cloud storage with a symmetric key encryption. For example, the day to day transaction database records. Their aggregated values are encrypted in data owner storage which is less in size. The database in cloud storage may be redundant and can be accessed by more number of users. To check the data in cloud storage is safe, the sample data can be fetched from cloud storage and decrypted. The aggregated data is also decrypted so that the data from cloud produce the same aggregated data. This ensures the data in the cloud storage is unaffected by users. The storage correctness verification is made in the above manner. In addition, each and every user is provided with a strong authentication mechanism so that the data owner, user, cloud provider is able to access with more trusted mechanism. A policy is induced and checked periodically to check the data is not violated.**

**Index Terms— Cloud Computing, Public Enterprise, DES.**

## I. INTRODUCTION

Cloud computing portends a major change in how we store information and run applications. Instead of running programs and data on an individual desktop computer, everything is hosted in the “cloud”—a nebulous assemblage of computers and servers accessed via the Internet. Cloud computing lets you access all your applications and documents from anywhere in the world, freeing you from the confines of the desktop and making it easier for group members in different locations to collaborate.

Cloud Computing Technology is perceived by many as a new asset of Information technology for the IT companies, educational institutions, government sectors, etc. In the ever fast growing economy apart from the challenges faced due to recession, the educational institutes find this a big hurdle as to how to provide necessary Information technology support for educational activities and research areas. Cloud Computing, the latest buzzword in IT sector, may come to the rescue, as it can provide an easy and inexpensive access to the state of the art IT technology, software and its applications. Cloud computing is a recent concept that is still evolving across the information technology industry and academia.

Cloud computing is Internet (cloud) based development and use of computer technology whereby dynamically scalable and often virtualized resources are

provided as a service over the Internet. This research process aims at studying the factors which affect the adoption of Cloud Computing Technology in an educational institution, case study of a Delhi based renowned public school. Questionnaire was used a data collection tool and the results were analyzed by SPSS program for statistical analysis.

## II.SERVICE UNDER LOAD BALANCING ENVIRONMENT

Cloud computing contains many content like virtualization, distributed computing, networking, advance version to grid computing, software and web services, etc. A cloud consists of components like Cloud controller, cluster controller, nodes, datacenters and servers. It composed of fault tolerance, high availability, scalability, flexibility, reduced cost of ownership, reduced overhead for users, less maintainability, on demand services. Addressing to this issue needs the foundation of efficient load balancing algorithm.

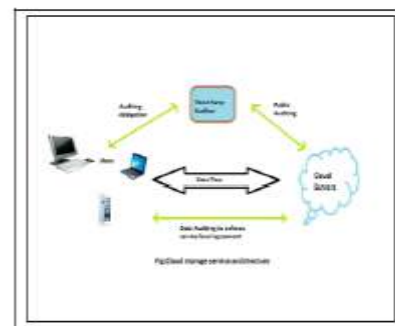


Fig-1 Cloud Computing Basic Storage Structure

The load can be CPU load, memory capacity, delay or network load. Load balancing is the process of distributing the load among various nodes of a distributed system to improve both resource utilization and job response time while also avoiding a situation where some of the nodes are heavily loaded while other nodes are idle or doing very little work. Load balancing ensures that all the processor in the system or every node in the network does approximately the equal amount of work at any instant of time. Various types of cloud system

- **Platform as a Service (PaaS):** Users create and run their own software applications while relying on the cloud

provider for software development tools as well as the underlying infrastructure and operating system.

• **Software as a Service (SaaS):** Under this layer applications are delivered through the medium of the internet as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management. The cloud provider hosts a single application which offers complete application functionality.

• **Infrastructure as a Service (IaaS):** Users rent computing power – either actual hardware or virtualized machines – to deploy and run their own operating systems and software applications. Simply, the backend systems that deliver cloud services are generally deployed in one of four ways.

• **Public Cloud:** Customers access cloud services are store documents in large documenters Equipped with hundreds of virtualized servers that house data from multiple organizations.

• **Private Cloud:** A single organization uses a dedicated cloud infrastructure. Community cloud: A private cloud is shared by a group of organizations with common missions, interests, or concerns.

• **Hybrid cloud:** Two or more cloud types are linked to enable data and applications to flow between them in a controlled way.

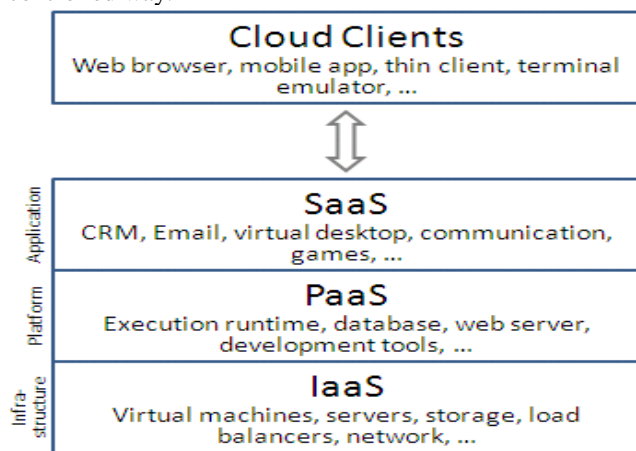


Fig-2 Cloud Computing Basic Types Structure

### III.PROBLEM IDENTIFIED

Recently the importance of ensuring the remote data integrity has been highlighted by the some research works. These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations.

As a complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers to peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.

However, while providing efficient cross server storage verification and data availability insurance, these schemes are all focusing on static or archival data. As a result, their capabilities of handling dynamic data remains unclear, which inevitably limits their full applicability in cloud storage scenarios.

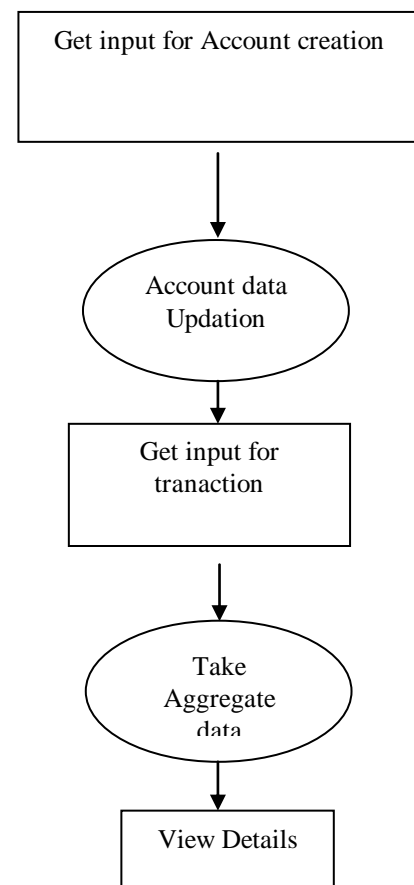
#### Demerits Of System in DES Algorithm

The following drawbacks are present in the system.

- Cannot address all the security threats in cloud data storage.
- Do not consider dynamic data operations.
- Security aspects in data managed by third party cloud providers are risk.
- Traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing
- Verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data.

### IV.SYSTEM MODEL

A large public cloud will include many nodes and the nodes in different geographical locations. Cloud partitioning is used to manage this large cloud. A cloud partition is a subarea of the public cloud with divisions based on the geographic locations. The load balancing strategy is based on the cloud partitioning concept. After creating the cloud partitions, the load balancing then starts: when a job arrives. Typical cloud partitioning the system, with the main controller deciding which cloud partition should receive the job. The partition load balancer then decides how to assign the jobs to the nodes. When the load status of a cloud partition is normal, this partitioning can be accomplished locally. If the cloud partition load status is not normal, this job should be transferred to another partition.



box and button controls are used to get the input from the console. Tab control is used to move between the account holder details to the reference holder details. The save button performs the operation that it saves the details in the accounts table. The delete button performs the operation that deletes the data according to the account number.

### 3. Account data Updation

In the data such as account no, date of transaction, amount and type of transaction of accounts can be given. It uses the textbox control and combo box control to get the input from the user. And then the details can be stored in the database. The save button performs the operation that saves the accounts transaction details into the AccountTrans table.

### 4. Aggregated data Updation

In this process, the date of transaction is given, so that the aggregated data stored in the database. It uses controls such as combo box and button. This is stored in the bank database. On clicking the add button the date is selected in the date of transaction field. Then by clicking the save button, the aggregate value saved in the aggregate table.

### 5. View Accounts List

In this process, the accounting information of the customers can be viewed. The accounting information such as account number, address, phone number, nationality, sex, type of account, creation date, father name and mother name and so on details can be viewed, and then the reference holder details can also be viewed.. It uses grid view control to view the account list.

### 6. View Accounts Transaction List

In this process, the transaction information of the customers can be viewed. In the amount transaction list can be viewed. The list contains the amount credited or debited and the date on which the transaction can be made. It uses the grid view control to view the details.

### 7. View Aggregate data

In this process, the aggregate data can be viewed. The encrypted aggregate data can be viewed. It uses the grid view control to view the data.

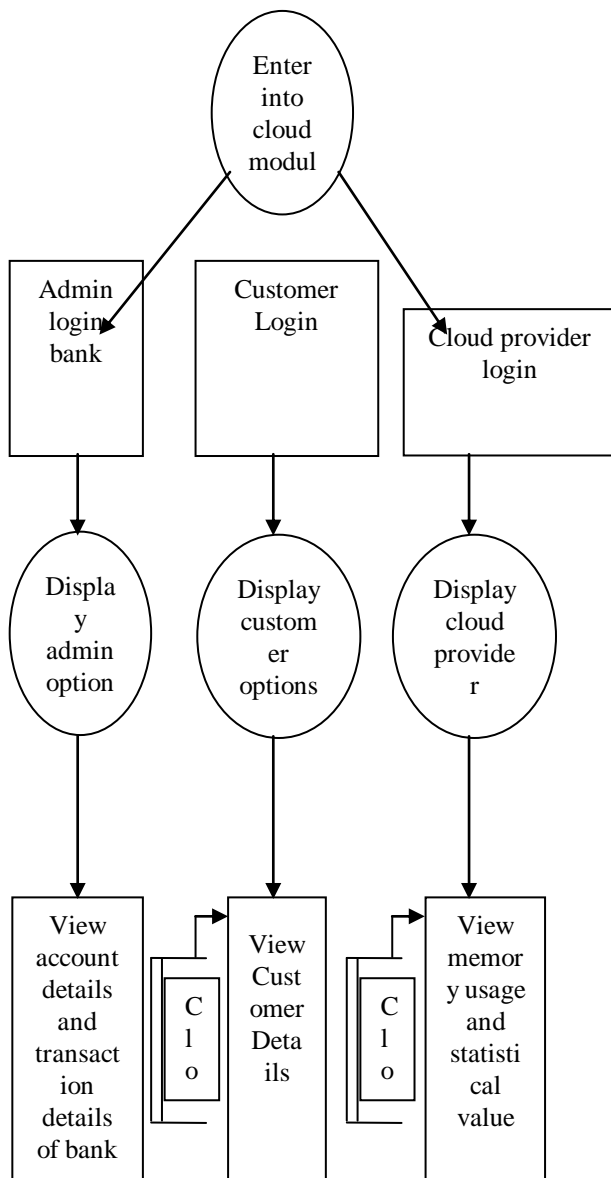
### 8. View Account Transaction Encrypted

In this process, the encrypted data can be viewed. All the transaction details can be viewed in the encrypted processat. Gridview control is used to view the encrypted transaction list.

## V. CONCLUSION

In this process companies entering the cloud should take steps to ensure they can trust the companies providing them with services, as well as the entities they are transacting with inside the cloud. Enterprises must have the ability to safeguard proprietary information on virtual servers and storage while giving cloud administrators the access and privileges needed to do their jobs.

All of cloud issues relate to establishing trust relationships, which process the conceptual foundations for cloud security. Many of the time-tested practices and technologies for managing trust relationships in traditional



### 1. Administrator login

The administrator logs in to the windows application uses the given username and password using this process. It uses the text box control to get input from the console. This process is used is used for the security purpose. On clicking the login button, it checks for username and the password, then if it matches means, then it logs in to the main process.

### 2. Accounts Details

In the accounting details, Reference Id holders, and contact details of the customers can be keyed in. All the customer details can be keyed in as input. Details such as name, sex, accno, phone, address, mail id, pan no, and reference holder id personal details can be keyed in as input and stored in the table. The controls such as textbox, combo

enterprise IT environments can be extended to work effectively in both private and public clouds. Those practices include data encryption, strong authentication and fraud detection, etc.

Through this process, the data management process becomes easy. The interface helps bank officials and cloud providers along with customers for accessing the data in the safest way. All the day-to-day activities are assigned to them through browser interface. **The new system eliminates the difficulties in the existing system. It is developed in a user-friendly manner. The system is very fast and any transaction can be viewed or retaken at any level. Error messages are given at each level of input of individual stages.**

The Triple DES algorithm is used to implement the process. It saves the data in the encrypted format, so that data securely saved in the cloud database. For theft analysis, the aggregate value is used and for recovering the data the error recovery algorithm is used. The error recovery algorithm automatically recovers the data from the replicated copy of the cloud database. So the proposed system eliminates the drawback of the existing system. The proposed system is very cost effective. So for implementation it utilizes low cost when compared to the existing system.

## VI. FUTURE SCOPE

The following are to be present in the proposed system.

- The new mechanism is calculating cloud area status at a given refresh period.
- Cloud areas are grouped based on their processing ability.
- If the application is designed as web service, it can be integrated in many web sites.
- SMS can be send to the customer
- Cost is minimized by using more advanced algorithm
- It is developed platform independent, so that use in any operating system
- Dynamic operations can be performed in the cloud space
- All types of access can be provided to the user
- So that the user can be accessed and modify their data in the place where they are
- Nodes inside the cloud area not treated equally. According to their processing and storage power, the partial job is assigned to them.
- One job is assigned to multiple node after the job is split according to the nodes capability.
- Jobs are split into sub tasks and assigned to more cloud nodes.
- Both dependent tasks and independent task scheduling is taken into account.
- Job replication strategy is also considered.
- Decreasing completion time of jobs.

## REFERENCE

- [1] M. Armbrust et al., "Above the Clouds: A Berkeley View of Cloud Computing," technical report, Univ. of California, Berkeley, Feb. 2009.
- [2] L. Siegele, "Let It Rise: A Special Report on Corporate IT," *The Economist*, vol. 389, pp. 3-16, Oct. 2008.
- [3] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the Art of Virtualization," *Proc. ACM Symp. Operating Systems Principles (SOSP '03)*, Oct. 2003.
- [4] "Amazon elastic compute cloud (Amazon EC2)," <http://aws.amazon.com/ec2/>, 2012.
- [5] C. Clark, K. Fraser, S. Hand, J.G. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield, "Live Migration of Virtual Machines," *Proc. Symp. Networked Systems Design and Implementation (NSDI '05)*, May 2005.
- [6] M. Nelson, B.-H. Lim, and G. Hutchins, "Fast Transparent Migration for Virtual Machines," *Proc. USENIX Ann. Technical Conf.*, 2005.
- [7] M. McNett, D. Gupta, A. Vahdat, and G.M. Voelker, "Usher: An Extensible Framework for Managing Clusters of Virtual Machines," *Proc. Large Installation System Administration Conf. (LISA '07)*, Nov. 2007
- [8] T. Wood, P. Shenoy, A. Venkataramani, and M. Yousif, "Black-Box and Gray-Box Strategies for Virtual Machine Migration," *Proc. Symp. Networked Systems Design and Implementation (NSDI '07)*, Apr. 2007.
- [9] C.A. Waldspurger, "Memory Resource Management in VMware ESX Server," *Proc. Symp. Operating Systems Design and Implementation (OSDI '02)*, Aug. 2002.
- [10] G. Chen, H. Wenbo, J. Liu, S. Nath, L. Rigas, L. Xiao, and F. Zhao, "Energy-Aware Server Provisioning and Load Dispatching for Connection-Intensive Internet Services," *Proc. USENIX Symp. Networked Systems Design and Implementation (NSDI '08)*, Apr. 2008.

## BIOGRAPHY

Ms. Ramya B is Part-Time research scholar pursuing her Ph.d in the area of Computer Science in Vellalar College for Women, Erode affiliated by Bharathiyar University. She has also completed her Post Graduation in Computer Technology in Institute Kongu Engineering College in Erode affiliated by Anna University. Her Research areas are Cloud Computing, Grid Computing and Networking.