6.1: Introduction

The security issues are paramount impediment in the adaptation and development of cloud computing. The principal concern of any client accessing the services and application of cloud is security and the risk [93] [94]. Where the application and datum security of cloud environment implemented in distributed, virtualized and dynamic architecture depends upon the paradigmatic principle of “CIA” i.e. Confidentiality, Integrity and Availability. In cloud environment and its process “Threats and vulnerabilities are also major concern along with the compliance which leads to hindrance in the security”. The major difference between the two lies w.r.t to the environment and user as explained:

**Vulnerability:** Weakness of the computing environment that can be exploited by the attacker. vulnerabilities of the environments are used by clients to architect parameters, that bypasses the standard security measures and access privileged data of other tenants hosted on same machine or in network

**Threat:** Probable error or attack by malicious user or computing environment condition.

When migrating applications and services in cloud environment, numerous vulnerabilities (Session riding, insecure cryptography, and portability) and threats (Malicious insider, shared technology use and insecure APIs) are need to be considered.

![Figure 6.1: Threats and Vulnerabilities](image-url)
In our study, we have discovered that several vulnerabilities and threats as mentioned in figure 6.1 effects the entire cloud environment and its operation (Load balancing). In order to migrate virtual machines and resources successfully prior knowledge of these threats and vulnerabilities is a welcome option. Enterprise should also avoid relying completely on the cloud provider to overcome the issues related to security [101] [102]. In this chapter, we have proposed the embedment of an efficient security technique based on the privacy homomorphism CDAP (Concealed Data Aggregation) which achieves efficient data concealment by using end to end encryption process during the mechanism of suboptimal Load balancing in our framework. Also we have contemplated only a theoretical way to secure the proposed load balancing framework.

6.2 Security Architecture:

With the defining characteristics and technologies employed for the realization of cloud system, the cloud presents different security issues in comparison to traditional computing environment. Where the security in cloud environment is divided into two broad categories: governance and operations “the governance domains are broad and address strategic and policy issues within a cloud computing environment (Compliance and Audit, Information Lifecycle Management, Portability and Interoperability)” on other hand “the operational domain focus on more tactical security concerns and implementation within the architecture. (Traditional Security, Business Continuity and Disaster Recovery, Data Center Operations, Incident Response, Notification and Remediation, Application Security, Encryption and Key Management, Identity and Access Management, Virtualization)”.

Barring the above pointed reason in our study, we have found that the security measures applied in cloud environment are for the most part is not different in comparison to the traditional computing environment but with the transition to cloud computing, the traditional ways adopted for securing data are challenged by cloud-based architectures. The security controls in cloud architecture are generally implemented independently in a layer or at more levels ranging from the physical, platform and up to the level of information and applications.

Predominately the cloud services are categorized and compared with respect to the cloud reference architecture, which had led to mapping and finding gaps of its security architecture, regulatory and other compliance requirement against it. The CSA model mentioned in figure 6.2 determines the security and risk posture of a service and in what way it would relate to an asset’s assurance and protection requirements. In below model the security issues due to cloud features and the measures adopted to overcome with them have been extensively addressed.
Due to the hierarchical architecture, the security risks, analogous of cloud computing services is also inherited between different layers. Below is the brief analysis of security concerns and level in accordance to delivery model.
The management process and security capabilities of end clients increases down the layer which is one of the critical property in cloud security [102] [103] Also, being a multidomain environment, different security measures can be applied at independent domains of cloud making it critical to analyze the security issues.

### 6.3: Security objective

According to DACS (Data and analysis center for Software) the properties to be executed for security is:

- **Dependability**: Predictability of the application in accordance to various conditions.
- **Trustworthiness**: Minimal or less vulnerabilities.
- **Survivability**: Resistant to attacks and ability to recover as soon as possible.

With various benefits and property cloud environment is hindered with different security risks. Security requirements of cloud computing includes:

- Confidentiality
- Integrity
- Availability
Issues: Besides the cloud architecture and its loop hole, there are other huge security pain points within the cloud environment. As per the anatomization in chapter 2, The traditional network security measures do not properly address the security issues of dynamic cloud environment. Even being one of the fundamental technologies of cloud, the security hindrance of any operation is more because of the vulnerabilities introduced by the virtualization and migration of load (at time of load balancing) per CSA [94] [101]. Different cloud platform has applied different security measures like strong cryptographically Secure Shell (SSH) keys (are used by Amazon), Synchronous cookies and connection limiting for mitigation of Distributed Denial of Service (DDoS) (by Microsoft) etc. [95] [98] [99].

At the time of load balancing in cloud environment, the threats can be directly on Virtual Machines (VMs) or indirectly on hosted Hyper-visors through virtual machines or due to dynamic migration of VMs from one Cloud site to another in cloud network as per Krutz et.al [102] [103]. Since load balancing is composed of various set of process (Load estimation, selection, migration) and policies as discussed in chapter 3, a thorough study has shown that the process suffers from threats (Inter VMs attacks, covert channel communication, vendor lock in hypervisor risk), at each and every level. Also “The need of mechanisms to ensure strong isolation, mediated sharing, and secure communications between VMs is to be properly addressed because of the inherent non-quantitative nature of the issues like trusting the VM image, hardening hosts, and securing inter-host communication are critical areas in IaaS security, privacy, and trust” [100] [104].

The encountered threats degrade the performance of entire cloud system and its operations. The embedment of specific security mechanism during the balancing and allocation process will not only enhance the entire cloud system performance but also improves the system stability.

6.4: Proposed solution

In accordance to above discussion and the review presented in chapter 2, A proper security mechanism during the load balancing is the demand of hour. And with dynamic encryption policies taking centerstage in cloud environment, the adoption of cryptographic approaches will be a measurable task to avoid security. The proposed privacy homomorphism solution aims to guarantee secure load balancing process by adopting encryption mechanism at the participating machines of the proposed framework of chapter 5. Our proposed mechanism of load balancing was based on the idea to migrate consolidated virtual and physical resource from one cloud site to other at dispersed locations by the use of “Incremental tree approach” which was an optimal
way to balance the load. Also where the underloaded nodes, overloaded nodes, aggregator node and enroute nodes had described the entire framework. The migration of VMs during the load balancing process, not contributes to the efficient distribution of the workload across the cloud sites but resulted into security issues too.

6.4.1: Types of encryption process

In the distributed environment like cloud the encryption technique are applied from one cloud site to another or in the same network cluster. The basic types of encryption process adopted are:

**End to end encryption:** It ensures data privacy and security from one data center to another.

**Hop by hop:** Data is encrypted at the aggregator node.

In order to achieve efficient data concealment by using end to end encryption process, in our proposed load balancing framework we are embedding the features of privacy homomorphism CDAP (Concealed Data Aggregation) [110].

The inclusion of the homomorphism on the suboptimal load balancing framework makes the direct operation on cipher texts at time of aggregation and migration process possible. The process of aggregation and migration are key process of our framework. Though being a simple mechanism, this security technique is suitable for a virtual environment like cloud. It not only facilitates the aggregation process along with the enhancement of security but the proposed homomorphism, obtains safe end to end transmission between the overloaded and underloaded machines in the cloud system. Being an encryption transformation mechanism direct calculations on cipher text is possible with symmetric or asymmetric encryption. Either of the technique can be applied to obtain cipher texts. In our work, we are using privacy homomorphism based on symmetric keys because of induced vulnerabilities and disadvantage of asymmetric key in distributed and virtualized environment.

We have assumed that entire operations is performed iteratively on a set of nodes called TNodes (The underloaded nodes, overloaded nodes and enroute nodes which also consist of aggregator node of our framework), where the privacy homomorphic encryption occurs. The TNodes can be of same datacenter or datacenter of different cloud site.
6.4.2: Procedure

The process to attain security during the load balancing consist of following phase:

• **Assignment of public key**: The assignment of public key issued by Overloaded nodes to the TNODEs followed by resources deployment.

• **Key sharing**: The process of Key sharing (Pair-wise) between the TNODEs of different datacenters or in same datacenters.

• **Encryption**: An encryption of data occurs at overloaded nodes by using the symmetric encryption algorithm (RC5) [104] [105] and after which the cipher text is communicated to any of its closest TNODE in the already established path.

• **Decryption**: Cipher text are decrypted at TNodes. Two cases occur during the decryption process is defined according to two conditions: First if the node is aggregator node of the enrooted node then after the decryption of cipher texts, aggregation function is applied and again the text is encrypted and deployed to the underloaded nodes of the TNodes. In second case if node is not the aggregator node then cipher text is directly decrypted at the underloaded node of the TNodes.

6.4.3: Algorithm

**(Homomorphism technique)**

The following transformation encryption mechanism (CDAP) at the nodes are used for attainment of secure load balancing process.

Assumptions:

Let E be the encryption function and D the decryption function.

+ and * respectively indicates the addition and the multiplication functions on the data set R.

`Key_{pr}` =private

`Key_{pu}` =public keys possessed by nodes then the **transformation encryption is** -

Additively homomorphic if:

`m+n = (DKey_{pr}(Ekey_{pu}(m)+Ekey_{pu}(n)))` where `m, n` belong to `R`.

else

Multiplicatively homomorphic if:

`m*n = (DKey_{pr}(Ekey_{pu}(m)*Ekey_{pu}(n)))` where `m, n` belong to `R`. 
In the process the cipher text which can be of a virtual machines files or resources are migrated at as required for load balancing. Any enroute node of TNODEs (which act as aggregator) aggregate incrementally the cipher text during the migration depending upon the condition discussed in chapter 5. The underloaded nodes can decrypt the aggregated data after the migration using its shared private key.

The proposed security mechanism though being a simple technique, but embedding it with the load balancing framework further strengthens the Cloud operations. The flow chart 7.1 described below explains the entire process of embedding.

Flowchart 7.1: Process of embedment

CDAP is dedicated to heterogeneous environment and enhances the security, if aggregation mechanism is adopted. The network performance shows tremendous improvement in energy and the bandwidth consumption once migration is secured. Even though the degree of security is to
be increased along with the performance, the use of our security mechanism can be hindered by restricted number of allowed aggregation functions.

Also, the limited capacity of overloaded machines can make encryption mechanism non-tolerable to some nodes. Though this problem can be addressed by the feature of overcommit exhibited by the machines. Application of advance security technique during load balancing may increase the overhead causing performance degradation because of which we have therefore adopted simple mechanism of concealment during the balancing process in order to achieve security.

6.5: Summary

The chapter provides an insight into the cloud security and vulnerabilities and mechanism to overcome the security issues at the time of load balancing. Embedding of security features in load balancing framework is discussed in this chapter. Though we have suggested and adopted a very simple mechanism when compare with other, but the contemplated mechanism guarantees a secure load balancing process which will add only a stepping stone in order to increase the overall security of cloud. And also, the main objective for the security embedment in load balancing mechanism was that “if cloud is secure at operation level then only the application hosted and deployed on it will we secure resulting into overall cloud environment security”.