Enhanced Load Balanced Security Solution in Cloud Computing

Kumud Gupta[1], Anuradha Panjeta[2]

[1]M.Tech Research Scholar ,HOD of [2]M.Tech CSE

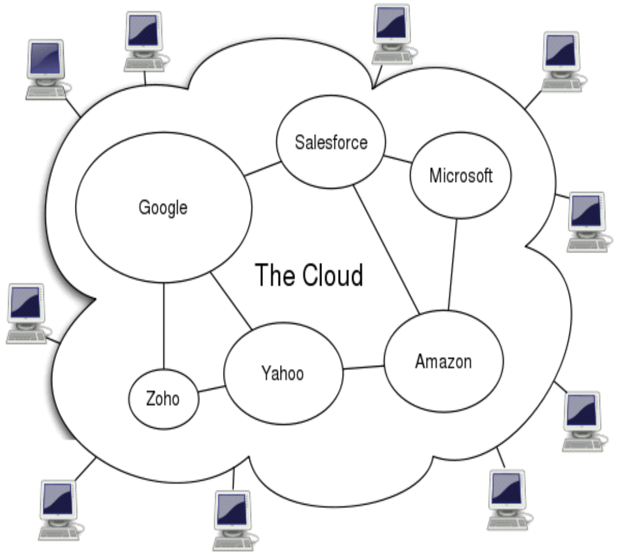
Abstract - With the advancement in technology and lot of upcoming security issues,one wonders how to keep the cloud environment secure and safe.The use of FHE and Homomorphic encryption for this has helped in improving the overall security in cloyd computing environments.The use of Min-Min tasks cheduling has helped in improving the task scheduling.The makespan has been reduced using the Virtual machine migration and load balancing has been improved. In our thesis we have proposed a task scheduling algorithm to achieve the minimum makespan of tasks.We have used the cloud sim 3.1 environment and netbeans as a platform to apply load balanced min-min task scheduling algorithm for static meta task scheduling and the advancement of it is enhanced load balanced min-min task scheduling in which there are two rounds,in first round the load balanced min-min scheduling is applied and in second round enhanced load balanced min-min task scheduling algorithm is applied over smaller tasks in cloud environment.Both these algorithms are applied to improve the maespan time of metatasks and improve the load balancing in cloud environment for faster execution of tasks.Also in our proposed work we have applied the security in cloud computing using the homomorphic encryption and avoided the attacks on source and destination nodes using the variation of homomorphic encryption i.e. full homomorphic encryption.The security applied using full homomorphic encryption uses the concept of router o send and direct the encrypted data to destination.

1. INTRODUCTION

Cloud computing is newest effort in delivering computing resources as a service. It represent a shift from computing as a product that is bought, to computing as a service that is delivered to consumers over the internet from large-scale data centres – or “clouds”.

Cloud computing has acquired popularity and developed to a major trend in IT. As industry has been pushing the Cloud research agenda at lofty pace, academia has only recently joined, as can be seen through the sharp rise in workshops and conference focussing on Cloud Computing. Cloud computing delivers IT as a service, cloud researchers can also learn from service oriented architecture (SOA). Described PaaS as an artefact of combining communications provisioning with the principles of SaaS and SOA.

Cloud computing is an on demand service in which pooled resources, information, software and other devices are provided according to the clients requirement at precise time. It’s a term which is in general used in case of Internet. The whole Internet can be seen as a cloud. Capital and operational costs can be cut using cloud computing. In case of Cloud computing services can be used from varied and pervasive resources, rather than remote servers or local machines. There is no model definition of Cloud computing. By and large it consists of a bunch of distributed servers known as masters, providing asked services and resources to different clients known as clients in a network with scalability and reliability of data centre.



.

Figure 1.1: General architecture in cloud computing environment

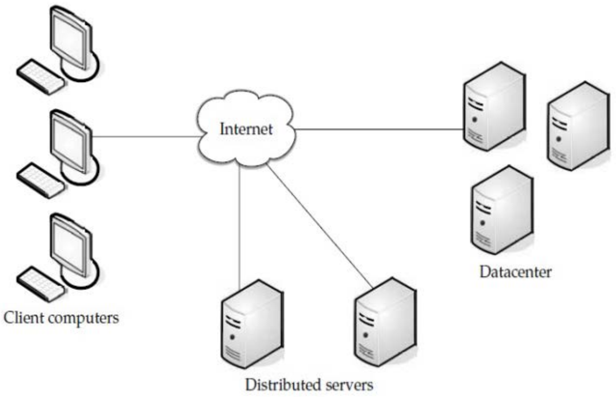


Fig. 1.2: Three components make up a cloud computing solution [41]

Cloud Components

A Cloud system consists of three foremost components such as clients, datacenter, and distributed servers. Each element has a definite purpose and plays a specific role.

Clients

End users interrelate with the clients to manage information related to the cloud. Clients normally fall into three categories as given in :

- Mobile: Windows Mobile Smartphone, Smartphone's, like a Blackberry, or an iPhone.
- Thin: No computation work is performed by them. They only display the information. Servers do all the works for them. Thin clients don't have any internal memory.
- Thick: These use different browsers like IE or Mozilla Firefox or Google Chrome to connect to the Internet cloud.

Datacenter

Datacenter is a collection of servers hosting diverse applications. An end user connects to the datacenter to give to different applications. A datacenter may exist at a large distance from the clients. Currently a concept called virtualization is used to install software that allows multiple instances of virtual server applications.

Distributed Servers

Distributed servers are the parts of a cloud which are present all over the Internet hosting dissimilar applications. But while using the application as of the cloud, the user will feel that he is using this application from its own machine.

Challenges in Cloud Systems

As cloud computing is in its evolving stage, so there are many problems prevalent in cloud computing including :

- Ensuring proper access control (authentication, authorization, and auditing)
- Network level migration, so that it requires minimum cost and time to move a job
- To provide proper security to the data in transit and to the data at rest.
- Data availability issues in cloud
- Legal quagmire and transitive trust issues
- Data lineage, data provenance and inadvertent disclosure of sensitive information is possible

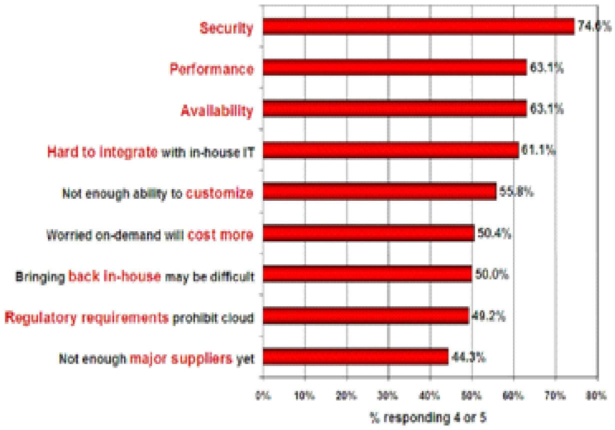


Figure 1.3: Most Prevalent challenges in cloud computing, IDC Survey

Essential Characteristics:

- *On Demand Self-service:*

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

- *Broad Network Access:*

Capabilities are accessible over the network and access through standard mechanisms that promote use by varied, thin or thick client platforms (e.g. mobile phones, tablets, laptops, and workstations).

- *Resource pooling:*

The provider's computing resources are pooled to serve several consumers using a multi-tenant model, with different physical and virtual resources enthusiastically assigned and reassigned according to consumer demand. There is a sense of location in reliance in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to stipulate location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

- *Rapid elasticity:*

Capabilities can be elastically provisioned and unconfined in some cases robotically, to scale rapidly outward and inward proportionate with demand. To the consumer, the capabilities available for provisioning often appear to be boundless and can be appropriated in any magnitude at any time.

- *Measured service:*

Cloud systems robotically control and optimize resource use by leveraging a metering capability at some level of generalization apposite to the type of service (e.g, storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing lucidity for both the provider and consumer of the utilized service.

Service Models

- *Software as a Service (SAAS):*

The competence provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are available from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. The consumer does not manage or have power over the primary cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exemption of limited user precise application configuration settings.

- *Platform as a Service (PAAS):*

The capability provided to the consumer is to position onto the cloud infrastructure consumer created or acquire application created using programming. Typically this is done on a pay-per-use or charge-per-use basis. A cloud infrastructure is the anthology of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are essential to support the cloud services being provided, and characteristically includes server, storage and network components. The abstraction layer consists of the software deployed athwart the physical layer, which manifest the essential cloud description. Conceptually the abstraction layer sits above the physical layer, Languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the causal cloud communications including network, servers, operating systems, or storage, but has control over the deployed applications and probably configuration settings for the application hosting environment.

- *Infrastructure as a Service (IAAS):*

The wherewithal provided to the consumer is to provision processing, storage, networks, and other elemental computing resources where the consumer is able to deploy and run arbitrary software, which can embrace operating systems and applications. The consumer does not manage or control the primary cloud infrastructure but has control over operating systems, storage, and deployed applications and possibly controlled control of select networking components (e.g., host firewalls). The datacenter hardware and software is what we will call a Cloud. When a Cloud is made obtainable in a pay as you go manner to the general public, we call it a Public Cloud, the service being sold is Utility Computing. We use the term Private Cloud to refer to internal datacenters of a business or other association, not made available to the general public.

Cloud Deployment Models:

- *Private Cloud:*

The cloud communications is provisioned for restricted use by a single organization comprise multiple consumers (e.g., business units). It is owned, manage and operated by the group, a third party, or some amalgamation of them, and it may exist on or off site.

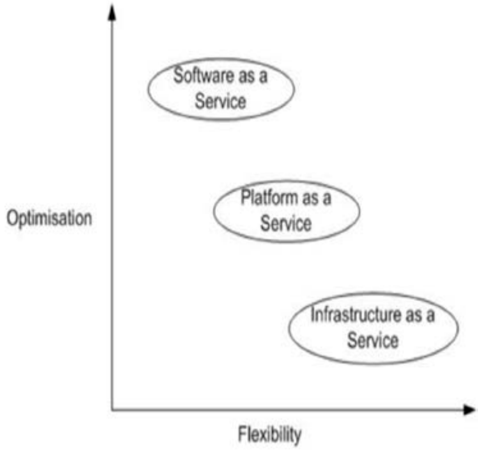


Figure 1.4 – Software, Platform and Infrastructure Services

- *Community Cloud:*

The cloud communications is provisioned for restricted use by a unambiguous community of consumers from organization that have joint concerns (e.g., mission, security requirements, policy, and observance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party, or some amalgamation of them, and it may exist on or off site.

- *Public cloud:*

The cloud communications is provisioned for unbolt use by the universal public. It may be owned, managed, and operated by a business, academic, or government organization, or some amalgamation of them. It exists on the grounds of the cloud provider.

- *Hybrid cloud:*

The cloud communications is a work of two or more divergent cloud infrastructures (private, community, or public) that remain idiosyncratic entities, but are bound together by harmonized or proprietary technology that enables data and application portability (e.g., cloud convulsive for load balancing between clouds).

Advantages Of Cloud Computing[41]

• Low start-up costs

• Payment according to need/use

• Great suppleness in relation to fast up-and downscaling of resource needs

• Short term of agreements.

• likelihood of ”thin clients”

• Possibility of full service with maintenance and SLA in an in general service.

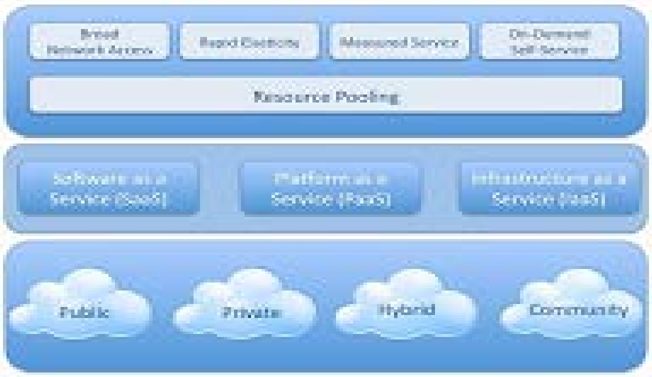


figure 1.5: general cloud computing model

•Possibility of access to supplier’s economies of scale by use of server capacity.

• Easier (and cheaper) admittance to new software versions.

• Other common outsourcing advantages (security for uptime, availability, contingency arrangements, reduced costs of investment in own data centre).

•Environmental advantages considerable CO2 reductions when servers are aggregated in large data centres, or when servers are grouped virtually to a joint server capacity (enables a far more efficient utilisation).

Privacy in Cloud Computing

When a user stores some astute information in a cloud, the confidentiality of this sensitive information is of nervousness to the user. Without any shield on this sensitive information, e.g., personal financial information, health records, a user won’t have assurance in storing his/her astute information in cloud. Likewise, when a company stores some business documents, e.g., business plans, in a cloud, the company also cares about the discretion and hopes only the germane personnel can admission these documents after they are authorized. Besides the privacy of these sensitive information, the user’s identity privacy, a fundamental right to privacy, is also likely in cloud computing. If the access to a cloud disclose a user’s real identity, the user could still be reluctant to accept this paradigm. Due to this reason, the user authentication without identifying the real identity, also called anonymous authentication, is desirable in cloud computing. Although unidentified authentication can provide user uniqueness privacy, it is a two-edged sword to provide complete dignified access in cloud computing. For example, when a group of users are authorized to some financial computing or data-intensive scientific collaborations in a cloud, if an important data modified by someone is disputed, it is hard to track the real user due to complete anonymous authentication. Therefore, on the way to tackle this dilemma, cloud computing should also provide provenance to testimony ownership and process history of data objects in cloud in order for wide acceptance to the public. Secure provenance should at least satisfy the following basic requirements:

- *Unforgeability:* A genuine origin record in cloud computing can effectively attest the ownership and process history of data objects stored in a cloud, any antagonist cannot forge a valid attribution records, i.e., modifying an item in a existing record or directly introducing a innovative forged record without being detected.
- *Conditional privacy preservation:* To ensure information confidentiality and unidentified authentication in cloud computing, a genuine provenance record should also be conditional privacy preserving That is, only a trustworthy authority has the

ability to reveal the real identity recorded in the derivation, while anyone else cannot.

Secure provenance is fundamental to the success of data forensics in cloud computing, yet it is still a challenging issue today. s

2. PREVIOUS WORK

Ning Cao† et.al,(2011), describes that the problem of privacy preserving graph query can be smoothly solved in cloud computing (PPGQ). To reduce the times of inspection of subgraph isomorphism, the principle of "filtering and verification" is utilised to remove as many negative data graphs as possible prior to verification.[11]

Boyang Wang et.al,(2012), describes Oruta as a new privacy preserving public auditing mechanism for data shared in an untrusted cloud. Oruta utilises ring signatures to construct homomorphic authenticators so that the third party auditor is able to confirm the integrity of shared data for a group of users without retrieving the entire data . It can also be used to support batch auditing, which can audit multiple shared data concurrently in a single auditing task. It supports dynamic operations. The dynamic operation means an insert, delete or update operation on a single block in shared data. [8]

Marten van Dijk et.al,(2012), describes Cryptography or traditional cryptography lags a certain prospect of protection and hence to achieve that lag we introduce FHE (FULLY HOMORPHIC ENCRYPTION) to ensure complete security of data over cloud environments.[12]

Ronald Petrlic et.al,(2012) ,describes the use of DRM (DIGITAL RIGHTS MANAGEMENT) concept for cloud computing to show how license management for software in the cloud can be achieved in a privacy friendly manner.[7]

Dr. Ali Ahammed et.al,(2014),describes that Cloud computing provides services to user through network. Cloud computing allow users to use applications or functions devoid of installating any application at any computer with internet. Since data precaution and purity is the major trouble of various users who place the data in cloud .The problem of empowering the integrity and security of data storage in Cloud Computing is solved in this. Users can store their data using cloud storage and enjoy the services through a shared pool of computing resources, without the difficulty of limited data storage and maintenance. Thus, liberal public auditability for cloud data storage security is of critical concern so that users can resort to a third party auditor to check the integrity of redistribution of data when needed. Third Party Auditor should be able to efficiently audit the cloud data storage without asking the local copy of data, and should not create new liability to the user data confidentiality.[13].

Nareshkumar R.M et.al,describes**,** that with cloud storage services, it is usual for data to be not only stored in the cloud, but also shared by multiple users. However, public auditing for such shared data while preserving identity privacy remains to be an open challenge. The first privacy-preserving mechanism that allows public auditing on shared data stored in the cloud is discussed in this approach . In particular, exploiting the ring signatures to compute the verification information needed to audit the integrity of shared data. With this mechanism, the identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to widely verify the integrity of shared data without retrieving the entire file. The experimental results demonstrate the effectiveness and efficiency of our proposed mechanism when auditing shared data.[14]

Krati Mehto et.al,(2015**)**,describes**,** Cloud computing is a novel computational manner for rewarding the need of new generation computing and the storage solutions. That offers scalable computing performance as well as storage solution therefore more than one cloud service providers are collaborating together for offering the scalable solutions. In addition the data outsourcing techniques are developed to reduce the overhead of maintenance and reducing the computational cost. But data hosting on third party servers is always untrusted. Therefore keep preserve the data on third party servers in secure manner need a cryptographic solution for data storage the similar direction the proposed work is provide the solution for enhancing cryptographic storage solution, authentication process and the data negotiation or retrieval techniques. In order to achieve the efficient solution for cryptographic cloud storage on third party server the MD5 and AES algorithms are used develop a hybrid cryptographic technique. For improving the authentication mechanism an authentication process is involved through the authentication server. Finally for providingease in data retrieval technique the feature selection and keyword based efficient search technique is proposed. The proposed keyword based search technique implements the KNN (k-nearest neighbour) algorithm for retrieving the documents from the storage. The functioning of the proposed technique is performed using JSP (java server pages). Additionally for exploitation of the given implementation a public cloud namely Open Shift services are used. After implementation and testing the performance of the implemented system is evaluated in terms of precision, recall and f measures for finding the query relevance of the data retrieval. Additionally for finding the cryptographic performance the time and space complexity is evaluated. The obtained experimental results demonstrate the effective and efficient computing technique, which is adoptable for third party data storage and retrieval processes.[15]

3. PROPOSED METHODOLOGY

Homomorphic Encryption

Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.This is sometimes a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services. For example, a chain of different services from different companies could calculate 1) the tax 2) the currency exchange rate 3) shipping, on a transaction without exposing the unencrypted data to each of those services.[1] Homomorphic encryption schemes are malleable by design. This enables their use in cloud computing environment for ensuring the confidentiality of processed data. In addition the homomorphic property of various cryptosystems can be used to create many other secure systems, for example secure voting systems, collision-resistant hash functions, private information retrieval schemes, and many more.There are several partially homomorphic crypto-systems, and also a number of fully homomorphic crypto-systems. Although a crypto-system which is unintentionally malleable can be subject to attacks on this basis, if treated carefully homomorphism can also be used to perform computations securely.

Homomorphic Encryption H is a set of four functions:

H = {Key Generation, Encryption, Decryption, Evaluation }

1. Key generation: client will generate pair of keys public key pk and secret key sk for encryption of plaintext.

2. Encryption: Using secret key sk client encrypt the plain text PT and generate Esk(PT) and along with public key pk this cipher text CT will be sent to the server.

3. Evaluation: Server has a function f for doing evaluation of cipher text CT and performed this as per the required function using pk.

4. Decryption: Generated Eval(f(PT)) will be decrypted by client using its sk and it gets the original result.[45]

Fully Homomorphic Encryption

A. Principle of fully homomorphic encryption

Craig Gentry construct homomorphism encryption scheme including 4 methods. They are the key generation algorithm, encryption algorithm, decryption algorithm and additional Evaluation algorithm.

Fully homomorphic encryption includes two basic homomorphism types. They are the multiply homomorphic encryption algorithm and additively homomorphic encryption algorithm .The multiplication and addition with Homomorphic properties. Homomorphic encryption algorithm supports only addition homomorphism and multiplication homomorphism before 2009. Fully homomorphic encryption is to find an encryption algorithm, which can be any number of addition algorithm and multiplication algorithm in the encrypted data. For simply, this paper uses a symmetrical fully encryption homomorphic algorithm proposed by Craig Gentry **.**

4. SIMULATION/EXPERIMENTAL RESULTS

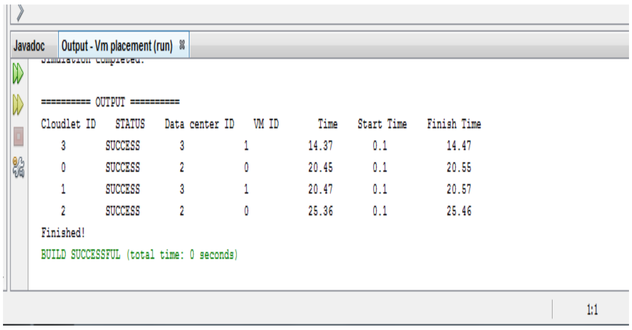
Theoretical Comparison and Analysis

The task scheduling algorithm used in our research is MIN-MIN scheduling algorithm,its used to reduce the makespan time of the various tasks using the VM concept.The strategy used is Load balancing.Assume that the task scheduler has meta tasks and resources as given below. Table 6.1 represents the volume of instructions and data of tasks T1 to T4.Instruction volume is specified in M1(million instructions)unit and Data volume is specified in Mb.

Table 4.1 Task Specification

TASK	INSTRUCTION VOLUME (MI)	DATA VOLUME (Mb)
T1	8178	137
T2	11295	258
T3	12109	182
T4	6107	137

Table 6.2 Demonstrates calculated execution time of various tasks on various resources. Data in table 6.2 will be updated after all tasks are allocated. Load Balanced MIN-MIN strategy on meta-tasks achieves makespan equals to 90.22 seconds and Enhanced Load Balanced MIN-MIN which achieves makespan equals 84.31 seconds and our approach FHE AND MIN-MIN TASK SCHEDULING together achieves a makespan of 80.65 seconds.



```
Simulation completed.

========== OUTPUT ==========
Cloudlet ID    STATUS    Data center ID    VM ID      Time    Start Time    Finish Time
    3         SUCCESS        3               1        14.37      0.1           14.47
    0         SUCCESS        2               0        20.45      0.1           20.55
    1         SUCCESS        3               1        20.47      0.1           20.57
    2         SUCCESS        2               0        25.36      0.1           25.46
Finished!
BUILD SUCCESSFUL (total time: 0 seconds)
```

Figure 4.1 Execution Time Of Min-Min Scheduling Using Virtual Machine Migration.

Table 4.2 Execution Time Of Various Strategies

LOAD BALANCED MIN-MIN STRATEGY (TIME)	ENHANCED LOAD BALANCED MIN-MIN (TIME)	MIN-MIN using virtual machine migration strategy (TIME)
90.22 SECONDS	84.31 SECONDS	80.65 SECONDS

Using data in table 4.1 and 4.2, to calculate expected execution time of tasks on each resource.

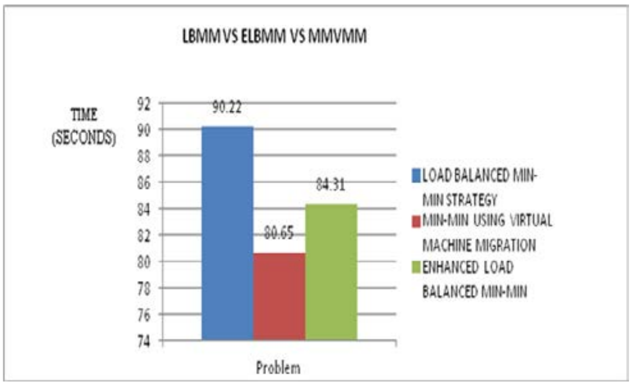


Figure 5.2 Graph Showing Comparisons

Security Aspect In Cloud Computing Implementation

In this we have used three modules:

- *Server:*-Its the module for selecting the file to be encrypted.In this we browse the file and select it to be sent to the destination. It acts as the source to the destination.
- *Destination:*-In this we receive the file sent by the server/source through the router.
- *Router:*-Its the module to receive the file sent by the server and redirect it to the destination providing full security and avoiding attacks on the source file.

To provide the security we have used FHE and there are some source files that needs to be encrypted. To allow this we have used the following steps:

5. CONCLUSION

This paper have concluded that the concept of Virtual Machine migration has been implemented using the CloudSim version 3.1 and we have compared it with Enhanced Load Balanced Min-Min algorithm for Static Meta task scheduling in Cloud Computing, in which we have reduced the Makespan using the Min-Min task scheduling algorithm and plotted the graphs accordingly.Also we have introduced the security aspect in our Cloud environment and avoided any kind of attacks on our cloud environment Using Homomorphic encryption.The Homomorphic emcryption can further be subdivided into Full Homomorphic Encryption and it is a better approach than the partial homomorphic encryption and cryptography.The attacks are avoided by using a router in between the source and destination nodes.It has helped in covering the security to a great extent.

6. FUTURE SCOPES

In future the study has to be done to improve the security level. By applying various attacks we can check the various security levels by the Homomorphic Encryption.We can extend our work in future to understand how homomorphic encryption works and how much security it provides.We can evaluate the security provided by the Homomorphic encryption.The security and various attacks can be applied and worked upon in varied domains of passive attacks and active attacks.

REFERENCES

[1] Anthony T.Velte, Toby J.Velte, Robert Elsenpeter, Cloud Computing A Practical Approach, TATA McGraw-HILL Edition 2010, pp. 3-11.

[2] Randles M., Lamb D., Taleb-Bendiab A.,"A Comparative Study into Distributed Load Balancing Algorithms for Cloud Computing", 2010, IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, pp. 551-556.

[3] Jhawar R., Piuri V., Santambrogio M. "Fault Tolerance Management in Cloud Computing: A System level Perspective", Systems Journal, IEEE, Volume-7, Issue-2, June, 2013, pp. 288-297.

[4] Jhawar R., Piuri V., Santambrogio M. "Fault Tolerance Management in Cloud Computing: A System level

Perspective", Systems Journal, IEEE, Volume-7, Issue-2, June, 2013, pp. 288-297.

[5] Sureshbabu G.N.K, Srivatsa S.K.," A Review of Load Balancing Algorithms for Cloud Computing", International Journal of Engineering and Computer Science, Volume-3, Issue-9 September, 2014, pp. 8297-8302.

[6] Shivaramakrishnan Narayan, Martin Gagné and Reihaneh Safavi-Naini Department of Computer Science University of Calgary, Alberta, Canada {snarayan,mgagne,rei}@ucalgary.ca

[7] Ronald Petrlic and Christoph Sorge," Privacy-Preserving DRM for Cloud Computing", 26th International Conference on Advanced Information Networking and Applications Workshops,2012.

[8] Boyang Wang, Baochun Li, *Member*,Hui Li," Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud",IEEE Transactions on Cloud Computing,Volume:2,Issue:1,Issue Date :March 2014,2012

[9] Ronald Petrlic and Christoph Sorge," Privacy-Preserving DRM for Cloud Computing", 26th International Conference on Advanced Information Networking and Applications Workshops,2012.

[10] Ning Cao*y*, Cong Wang*z*, Ming Li*y*, Kui Ren*z*, and Wenjing Lou*y yDepartment* of ECE, Worcester Polytechnic Institute, Email: *f*ncao, mingli, wjlou*g*@ece.wpi.edu *zDepartment* of ECE, Illinois Institute of Technology, Email: *f*cong, kreng@ece.iit.edu

[11] Ning Cao*†*, Zhenyu Yang*†* , Cong Wang*‡*, Kui Ren*‡* , and Wenjing Lou*†*," Privacy-Preserving Query over Encrypted Graph-Structured Data in Cloud Computing",2011.

[12] Marten van Dijk, Ari Juels," On the Impossibility of Cryptography Alone for Privacy Preserving Cloud Computing",2010

[13] Dr. Ali Ahammed, Mukesh kumar B." Secure Cloud Storage Aiding Confidentiality Protecting Public Auditing", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering *(An ISO 3297: 2007 Certified Organization)* Vol. 3, Issue 6, June 2014.

[14] Nareshkumar R.M1, Gayatri Sarag, Pooja Doshi," PRIVACY-PRESERVING PUBLIC AUDITING DATA INTEGRITY FOR SHARED DATA IN THE CLOUD", International Journal of Research In Science & Engineering e-ISSN: 2394-8299 Volume: 1 Issue: 6

[15].KratiMehto, Rahul Moriwal." An Implementation of Privacy Preserving Search on Cryptographic Cloud", International Journal of Innovative Research in Computer and Communication Engineering *(An ISO 3297: 2007 Certified Organization)* Vol. 3, Issue 12, December 2015

[16] Vladimir Boˇzovi´c1, Daniel Socek2?, Rainer Steinwandt1, and Vikt´oria I. Vill´anyi1," Multi-authority attribute based encryption with honest-but-curious central authority".

[17] E Ashwini Kumari, N. Chandra Sekhar Reddy, E Uma shankari," Multi-Cloud Storage Data Possession Based Data Integrity Verfication And Security Cooperative Schedule" *International Journal Of Scientific Research And Education* ||Volume||2||Issue||10||Pages-2019-2026||October-2014|| ISSN (e): 2321-7545 Website**: http://ijsae.in**

[18] Michael Ben, Shafi Goldwassert ,Avi Wigdemon,"completenesss theorems for Non-cryptographic fault tolerant distributed computation".

[19] Ning Cao*†*, Zhenyu Yang*†* , Cong Wang*‡*, Kui Ren*‡* , and Wenjing Lou*†*,"Privacy-Preserving Query over Encrypted Graph-Structured Data in Cloud Computing",2011

[20] Krishna Kumar L1, Deepa P Sivan 2," Preserving Privacy Policy- Preserving public auditing for data in the cloud", International Journal of Engineering Science Invention ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726 www.ijesi.org || Volume 3 Issue 11 || November 2014 || PP.06-09.