International Engineering Journal For Research & Development

Vol.4
Issue 2

E-ISSN NO:-2349-0721

Impact factor : 6.03

DEPENDABILITY OF THE USERS IN CLOUD ENVIRONMENT USINGLOAD BALANCING AND INTEGRITY OF DATA

Ms. Sandhiya R[1], Mrs. D. Radhika [2], Mrs. G. Sasikala [3]

[1] PG Student, Department of CSE, Vivekanandha College of Engineering for women (Autonomous), Tiruchengode, India, [2] Assistant Professor Department of CSE, Vivekanandha College of Engineering for women (Autonomous), Tiruchengode, India, [3] Assistant Professor Department of CSE, Vivekanandha College of Engineering for women (Autonomous), Tiruchengode, India

[1]sandhiyageniune@gmail.com, [2]radhikadeva@gmail.com ,[3]sasimecse2013@gmail.com

ABSTRACT

A cloud Computing is one of the most impressive service offered via internet which creates a platform to store and retrieve data Since user's personal data is being stored in an unencrypted format on a remote machine operated by third party vendors who provide various services, the impact of user's identity and unauthorized access or disclosure of files are very high. In this proposed system is using Dependability of the Users,Privacy and Integrity of Data (DPI) algorithms using improve the Performance evaluation of Cloud Computing infrastructures is required to predict and quantify the cost-benefit of a strategy portfolio and the corresponding Quality of Service (QoS) experienced by users. Thus, focusing on Load balancing in the cloud computing environment has an important impact on the performance. This paper takes care of multi objective resource provisioning scheme for handling multiple task classes for various workload facility. In this proposal, project is using a Best Partition Searching for distributing a file system to another cloud environment. This approach provides a security in terms of user authentication for "authorization" to enter the network which is made via Image Sequencing password to prove that the identity is original user, RSA algorithm to encrypt the data to provide data integrity, a highly parallel distributed data management service that enables to read /write and append huge data sets that are fragmented and distributed at a large scale. Thus this approach provides an overall security to the client's personal data and the issue of concurrency, volume of data can be resolved with these techniques.

KEYWORDS: Integrity of Data, Dependability of the Users, Quality of Service, Load balancing

INTRODUCTION

Today, this propose have an ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud

computing. In this new world of computing, users are universally required to accept the underlying premise of trust. Within the cloud computing world, the virtual environment lets users' access computing power that exceeds that contained within their own physical worlds. Cloud computing is the process of providing computer facilities via internet. And it's provided us better and efficient way to access information in timely manner and also increases storage of capacity for user in.

Cloud computing enables a new business model that supports on-demand, pay for-use, and economies-of-scale IT services over the Internet. The Internet cloud works as a service factory built around virtualized data centers.1 Cloud platforms are dynamically built through virtualization with provisioned hardware, software, networks, and datasets. The idea is to migrate desktop computing to a service-oriented platform using virtual server clusters at data centers. However, a lack of trust between cloud users and providers has hindered the universal acceptance of clouds as outsourced computing services. To promote multi-energy, this propose must design the cloud ecosystem to be secure, rust worthy, and dependable. In reality, trust is a social problem, not a purely technical issue. However, we believe that technology can enhance trust, justice, reputation, credibility, and assurance in Internet applications. To increase the adoption of Web and cloud services, cloud service providers (CSPs) must first establish trust and security to alleviate the worries of a large number of users.

Cloud users are anxious about whether data-center owners will misuse the system by arbitrarily using private datasets or releasing sensitive data to a third party Without permission. Cloud security is deployed to provide full of protection between data owner and service provider. To address these issues, this propose a reputation-based trust-management scheme augmented with data coloring and software watermarking.

The Cloud Security Alliance 5 has identified a few critical issues for trusted cloud computing, and several recent works discuss general issues on cloud security and privacy. Public and private clouds demand different levels of security enforcement. This propose can distinguish among different service-level agreements (SLAs) by their variable degree of shared responsibility between cloud providers and users. Critical security issues include data integrity, user confidentiality, and trust among providers, individual users, and user groups. The three most popular cloud service models have varying security demands; the infrastructure-as-a-service (IaaS) model sits at the innermost implementation layer, which is extended to form the platform-as-a-service (PaaS) layer by adding OS and middleware support. PaaS further extends to the software as-a-service (SaaS) model by creating applications on data, content, and metadata using special APIs. This implies that SaaS demands all protection functions at all levels. At the other extreme, IaaS demands protection mainly at the networking, trusted computing, and compute storage levels, whereas PaaS embodies the IaaS support plus additional protection at the resource-management level.

Virtual Trust Difficulty in Cloud Services:

The cloud security grouping has identified a few vital issues for trusted cloud computing, and several recent works discuss general issues on cloud security and privacy. Public and private clouds order different levels of security enforcement. This propose can differentiate among different service-level agreements (SLAs) by their variable degree of shared responsibility of Security concerns which contains data integrity, user confidentiality, and trust among providers, individual users, and user groups. The three security demands should be varied from the three cloud service models that are described in below the infrastructure-as-a-service model sits at the innermost implementation layer, which is expanded to form the platform-as-a service (PaaS) layer by adding OS and middleware support. Pass further extends to the software-as-a-service (SaaS) model by creating applications on data, content, and meta-data using special A PIs. This implies that SaaS demands all protection functions at all levels.

Securing transportation as a service

The Iaas model is works to compute networking and data storage, other resources in a virtualized environment. Amazon's Elastic Compute cloud is one of good example of Iaas, at the cloud infrastructure level, CSP can implement network security with intrusion-detection systems, firewalls, antivirus programs, distributed denial-of-service suspicion and so on. Securing policy as a service. Cloud platforms built in Iaas with system integration and virtualization middle-ware. And these platforms can be used to users for implementing user-built software applications onto the cloud infrastructure using provider-supported programming languages and software tools like Java, Python and Dot net.

Cloud Suppliers and Reported Services

Hardware and software features are presents in cloud security. Three main security requirements is used in cloud computing demands such as confidentiality, integrity and availability. Report is the process of maintaining user communicated details on database. And these details are viewed only by an authenticated user in cloud environments

Data reliability and confidentiality Protection

Data integrity is the ability of cloud provider keep data safe from unauthorized person or hackers. Confidentiality is essentially the way the cloud provider insures that the data is secured from unauthorized access. The measures that the cloud provider uses to insure that this goal is met include physical isolation and cryptology. Cloud computing is a public network, which brings a set of complicated challenges for the provider to produce isolation for the customer. Physical isolation is accomplished by using virtual local area networks and middle boxes. The second method the provider uses is cryptology, which essentially encrypts the data before it is placed into the cloud. These two methods are standard measures that are used to secure data in the cloud.

Many tools are available for constructing cloud applications on large datasets and it's provided by cloud software environment to desired users. Let's following features are presents in security and privacy such as. Fine-grained access control to conserve data integrity and deter intruders or hackers a method to stop ISPs or CSPs from attacking user privacy. CSPs that struggle against spyware and web bug. We can improve some of these features with cloud reputation systems and more efficient identity management systems some features are Cloud resource can access security protocol like http and secure socket layer. Fine grained access control to protect data integrity and data attacker.

Trusted Cloud Computing over Data Centers

Security aware cloud architecture and this used to identify the protection mechanisms needed. Intruder detection action is should be implemented by using these architectures.

Cloud protection Infrastructure

Trusted and dependable cloud architecture helps protect network attack by launching trusted operational sectors for different cloud applications. The difficulties in security agreement that CSPs protect all data canter servers and storage areas. Our architecture protects MACHINE checking from software-based attacks and upholder data and information from robbery, fraud and natural failures. It provides strong authentication and authorized access to sensitive data and on-demand services. This propose had several design objectives for a trusted and dependable cloud when creating our architecture.

RELATED WORKS

Load balancing is an efficient part of cloud computing environment which confirms that all procedures work similar amount of work in particular time period. The different types of algorithms for load balancing over cloud environment have been implemented with the main goal to develop cloud resources accessible to the end users with easy and accessibility. The main load balancing problem is the run time overload owed to the change of load data amongst CPUs, selection of processes for decision making and transfers the job from processor to processor. The proposed approach analyzes the conditions and divides the load balancing approach in multiple layers [1].Recent promising developments in quantum computing seem ideal for performing this overhead work. As a step towards this goal, this paper proposes a host resource usage prediction approach, based on a complex-valued neural network. The algorithm can be further modified in the future to be applicable to quantum computing environments. A proof-of-concept is evaluated on real world load traces from a grid. The algorithm is compared against some current state-of-the-art host-load prediction algorithms to demonstrate its accuracy [2].

Cloud Computing is becoming a viable computing solution for services-oriented computing. Several open-source cloud solutions are available to these supports. Open-source software stacks offer a huge amount of customizability without huge licensing fees. As a result, open source software are widely used for

designing cloud, and private clouds are being built increasingly in the open source way. Numerous contributions have been made by the open-source community related to private-IaaS-cloud. Open Nebula - a cloud platform is one of the popular private cloud management software [3]. In this mathode the time series of daily maximum load is partitioned into two parts, historical dataset and current tendency dataset, backward cloud algorithm is applied to the two datasets to form the historical cloud and the current cloud, and the corresponding rule sets are mined. Then the historical cloud and current cloud is integrated to created predictive cloud through synthesized cloud. Finally, via cloud reasoning, the forecast result can be obtained. This predictive method effectively integrates quasi-periodical regularity and current tendency of time-series data, and has a simple computing model. The case study shows that the proposed method is accurate and practical [4].

Nowadays handling of big data transfer among thousands of interconnected servers plays a vital role on cloud computing environment. Big data is nothing but collection of relational data, unstructured data (human readable format), and semi-structured data, streaming data such as machines, sensors, Web applications, and social media. In existing system this concept enhances by fixing some optimal to overcome the bottlenecks occurs while data transfer on scientific cloud application. The parameters are pipelining, parallelism, and concurrency [5].Researchers used many approaches (i.e. Ant colony, Honey Bee, Genetic, Static, and Dynamic) but still need improvement. Virtual Machines (VMs) migration system plays the vital role in load management. Our focus in this research is maximizing the utilization of VMs CPU capacity. Proposed research approach is based on Dynamic Weighted Live Migration (DWLM) to manage load imbalance problem. The proposed mechanism results outcomes compared with Migration time, Scalability, Throughput and Availability factor from Equally Spread Current Execution load balancing algorithm (ESCEL) and Push Pull algorithm. This paper also focuses on others load balancing strategies and future research scope in Load management mechanism [6].

Facing load imbalance problem; that is, the file chunks are not assigning correctly among all the nodes. For that purpose, the load rebalancing technique comes into picture, load rebalancing has the more efficiency that makes system more efficient. For load imbalance we use a secure load rebalancing algorithm that merges with the MD5 with DES encryption algorithm. The result shows perform the system in terms of security parameters message overhead and the movement cost for our proposed scheme. For this work we are implementing in distributed file system of the EC2 [7]. Scheduling of computational load and actual processing is an important problem to be considered from the perspectives of time and consumed energy for execution ın the scale of data centers. In this paper, time-series analysis of the arrivals of the workloads have been done by applying auto regression (AR), moving average (MA), auto regression and moving average (ARMA), and Holt-Winters approaches. Performances of the four methods was evaluated and compared for Google

workload logs that is publicly available in the Internet [8].

Cloud computing is an emerging computing paradigm in which shared resources are provided according to the customer request at specific time. Load balancing is the process of distributing workload among various nodes of the computing system. The load can be CPU load, memory capacity, or network load. An efficient load balancing avoids a situation where some of the nodes are heavily loaded while other nodes are idle or doing very little work. When Virtual Machine (VM) is overloaded with multiple tasks, these tasks are removed and migrated to the under loaded VMs of the same or different datacenter [9]. The main objective of this paper was to propose cloud supporter framework to support cloud for processing multiple tasks. Because of multiple tasks on cloud server, it works slower and sometimes gets failed. In this situation distributing or scheduling of tasks on the distributed computing system is the only solution to reduce workload on server. Computing capability of smart phones CPU can compete with the CPU of the computers. Smart phones are energy-efficient and cost-effective alternative to running certain tasks of traditional servers. Distributing tasks for computations must utilize all the resources equally, no resource should be under or over utilize this problem leads to focus on the load balancing technique to support the cloud for processing tasks [10].

Cloud computing is offering on demand services by providing virtualize and storage environment. Due to the sharing of resources in cloud, there is a chance of resource wastage which creates need for load balancing. To address this problem, this work proposes an adaptive solution which enhances the performance of the distributed systems and provides scalability desired in internet based computing environments. The proposed algorithm has been implemented and compared with the results of existing mechanisms and results of our proposed mechanism has been found promising [11]. In Cloud based Storage every server clusters completely handles a particular kind of information service and receives the client's request dynamically in different time steps. It is a research challenge to design an efficient load balancing algorithm which can assign the multimedia message jobs with minimum cost between server clusters and clients while not overloading the server clusters. Differing from previous works, this paper takes into account a more practical dynamic services scenario in which each server clusters handles only a particular type of multimedia task and each client request different type of multimedia services at different time. Such scenario can be handled as an integer linear programming problem which is computationally in feasible in general. In this paper an attempt to solve the problem by an efficient GA in immigrant scheme Simulation results exhibit that the proposed genetic algorithm can efficiently cope with dynamic multi-service load balancing in CMS [12].

Numerous huge cloud organizations, alike as Amazon, Yahoo, Google, offer many cloud-services and have many users. Cloud-computing is an Internet-based computing approach, where the software, resources and the applications are shared between many-to-many computing

devices. Cloud Load-balancing (CLB) takes the wealth of the cloud's scalability and the physically to meet rerouted workload and to improve overall availability. In the addition of tasks goods and traffic distribution, CLB technology provides fitness checks to the cloud applications. We used GA approach to handling the LB in cloud-computing. Our proposed work is more appropriate than the current techniques work, as we executed the cloudlets in less time and performing the load-balancing in more profitability [13].

Cloud computing is one of the fast-growing fields in high performance computing. The demand for cloud computing services is increasing due to its availability anywhere anytime. As the users for cloud computing service increases rapidly, the load on individual nodes increases. This situation triggers the need for load balancing. Load balancing is a method by which the user requests are equally distributed among the available virtual machines in the data center to achieve maximum throughput, processing time and response time. In our work, we are incorporating Weighted Round Robin algorithm in Honeybee algorithm in order to achieve minimum data center processing time and response time [14]. Users can use these resources and services as they want on pay per use concept. In cloud computing architecture load balancing is a very important issue. There are many algorithms for load balancing in cloud computing. All algorithms work different ways. We proposed a Improved Max-Min Ant colony Algorithm. Improved Max-Min used the concept of original Max-Min. Improved Max-Min is based on the execution time not on completion time as a selection basis. The main motive of our work is to balance the total load of cloud system. We try to minimizing the total makespan. We simulated results using the CloudSim toolkit. Results show the comparison between improved max min and new hybrid improved Max-Min ant approach. It mainly focuses on total processing time and processing cost [15].

METHODS AND MPLEMENTATIONS

Current available cloud vendors provide huge amounts of storage space and computing resources access the user data from Cloud storage privacy and security problems are major concern that need to be solved we must use new method for cloud storage security enhancement. By implementing Cloud storage many business related security issues and problems and threats will be resolved. To understand the security issues related with cloudStorage. To provide high quality services to the users.To provide high data security in cloud basedEnvironment using steganography, encryption andDecryption.To minimizing the data uploading and downloadingTime on cloud storage. In this proposed system is using Dependability of the Users,Privacy and Integrity of Data (DPI)algorithm depend upon In cloud based environment there are many security issues such as authentication, integrity, privacy, virtualization, confidentiality, large amount data processing, scalability, access control etc. Traditional security approaches are no longer suitable for data and application in cloud.

Cloud Computing have scalable and location independence features so application and data stored in cloud have no fixed limitations. In security breaches it is quite difficult to resolve a particular node in which threats occurred. Due to the openness of cloud environment data may be accessed by unauthorized users. In cloud the issue of verifying correctness of cloud data storage becomes more challenging. Cloud computing poses several security threats due to number of reasons. Data Breaches is also major security concern in cloud storage. User stored large data sets in the cloud so there is a chance that malicious user may entered in the cloud storage system. There is high possibility of attack and threats. In cloud storage data integrity must be kept effectively to avoid data loss. In cloud storage data is stored over the remote server so it is necessary to preserve confidentiality. Security policies should be followed strictly

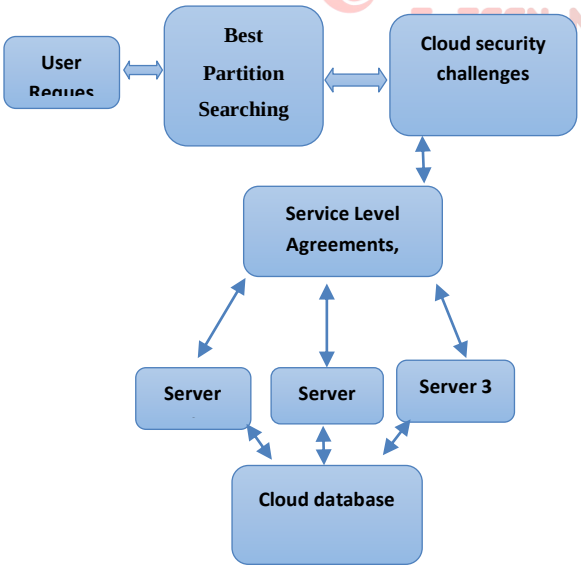

Fig: Dependability of the Users,Privacy and Integrity

Data access provides user access to data storage. Data should be shared only between authorized users so it is required to provide privileged user access. Reliability is also an important issue in cloud storage because data is stored in virtual machines. Multi-tenancy is an important characteristic of cloud computing technique. Multitenancy permits multiple users to access and store data on cloud servers.so there is a risk of data intrusion. By injecting client code data can be intruded.

Identity management & access control

In registration module user will register themselves by user name, password, contact number and email id. User generate random verification code by using Random frequency. User get the verification code on his email address after that user verify the code and redirect to home page. If verification code field remain blank or user entered wrong verification code then redirect to login page. Login is the procedure by which individual get access to the data by identifying and authenticating through the credentials provided by the user. User has logout when access is no longer required.

Service Level Agreements

In this suggested system file is scattered at three locations. First one is at our application and next two where second and third files are stored. We developed setting page that will be used for uploading and downloading file from table. Insert FTP details into table. In other words splitted files get saved to different cloud server. We created a method where user can share files to other users, for that we have designed a page in which user can simply enter the id of person whom to

transfer the files and file gets uploaded to cloud server and name of the files get saved to SQL server table. The receiver will get a notification that somebody has shared a file with you. If user clicks on the download button all the splitted files get merged and saved to receiver local system. Now the receiver party gets the encrypted and compressed file it is the time that user has to decrypt and decompressed the received file.

Data Privacy and Integrity

In Suggested system, we are splitting the data file, image file or video in different parts with some extension (.part in our case).After splitting we stored splatted file in our local system with extension .part. In this proposed system, encrypt each and every splitted file which is of .part extension with public key so that it cannot be easily readable by any unauthorized access or hacker.

Encryption technique like DES, AES, and RSA is developed before storing it on cloud. In this proposed system, splitted files get compressed with GZIPSTREAM algorithm so that the size of splitted files gets reduced, and it can easily be transferred to cloud server. Zip is based on the deflate algorithm.

Super Key Assessment Algorithm

Step 1:

Cipher(no of byte in[6*TNb] and No of byte out [TNb*(TNr+1)],

Start

Byteformal [6, TNb], Formal = in

Step 2:

If (TNr=in TNb)

{

AddRoundKey(formal, w[0, Nb-1])

For pattern Cipher key= 1 step 1 to TNr–1

Split Sub Bytes (formal)

Data Rows Shift (formal)

Mix data columns and rows (formal)

Addpattern CipherKey(formal,

W [pattern Cipher Key *TNb, (pattern Cipher Key +1)*TNb-1])

End for

Addpattern Cipher Key (formal, w [TNr*Nb,

(TNr+1)*TNb-1])

}

Else

{

Out = formal

}

Step 3:

End

The cipher text message contains all the information of the plaintext message, but is not in a format Readable by a human or computer without the proper mechanism to decrypt it; it should resemble random gibberish to those not intended to read it. The encrypting procedure is varied depending on the key which changes the detailed operation of the algorithm. Without the key, the cipher cannot be used to encrypt or decrypt.

Data Distribution

Data distribution is a critical task distribution should maximize transfer rates and minimize information redundancy. VMs algorithm to reduce the burden in virtual machine. Set of heuristics that prevent burden in the system effectively while saving energy used. The second component is a central data repository which has the files to be deployed onto all the VMs.

Algorithm JSQ ()

{

Scheduler initializes the VM allocation table.

While (there is a task received by JSQ scheduler)

{

Scheduler forwards the task towards that VM

Whose queue length is smallest & update

VM allocation table.

If (any virtual machine completes the task)

Then

{

Update the VM allocation table

Accordingly.

}

}

}

Steps of proposed algorithm

Step 1: Through scheduler table choose the scheduler whose idle queue length is largest, assign the task to idle virtual machine through the selected scheduler and update the scheduler table accordingly.

Step 2: If idle queue of all scheduler is empty then Scheduler access the VM table and select that virtual machine whose queue length is shortest and assign the task to that virtual machine.

Step 3: On completion of task, VM update the VM table. If any VM gets idle then it adds itself to the idle queue of that scheduler whose queue length is shortest. Scheduler updates the scheduler table accordingly.

Key Expansions—Round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

Particle Swarm Optimization

The specified number of VMs are created and started within the selected cloud provider. This function performs the actual deployment of the virtual infrastructure, installation, and configuration of the software installed in the VMs in our specific case it is our VMs and the peers for distributing the partitioned file. Automatic Deployment Layer using the configuration parameters taken from the user. In this scenario one of the VMs is randomly chosen to be the master and the others become slaves of the application.

RESULT AND DISCUSSION

Analysis of time complexity

The time complexity parameter has been calculated by using database and the request queries are input of the listed algorithm based on the number of users and the execution time of the individual algorithms are represented below: Time represented by T, Data analytics by DA, Trust Accuracy represented by TA

$$T = \frac{DA + TA}{\text{No databas e access } + \text{no of user}}$$

The figure given below shows the Time complexity by different comparisons as follows

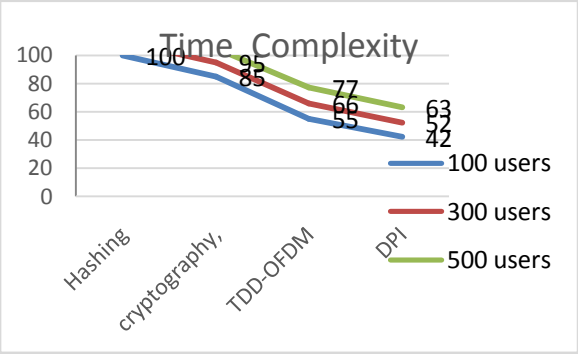

Figure 6.1.2: Comparison of time complexity

Figure 4.10, shows the comparative result on time complexity produced by various methods and shows clearly that the proposed SKA has produced less time complexity.

Users	Hashing	Cipher key	SKA	DPI
100 Users	100	85	55	42
300 Users	110	95	66	52
500 Users	125	105	77	63

Table 6.1.2 Processed data, UN Processed data and Efficiency of packet processing

Table 4.4 represents the throughput ratio of the different algorithmsDPI 73 %, Cipher Key 68 %, SKA 57 % and Hashing 42 % and the overall the proposed DPI technique have the high throughput ratio as compared with other techniques.

The resultant algorithm has been implemented and evaluated for its performance using the dataset being considered with previous clarification. The method has produced efficient results in all the factors considered.

Analysis of Integrity to security provision

The figure given below shows the false ratio accuracy by different comparisons as follows

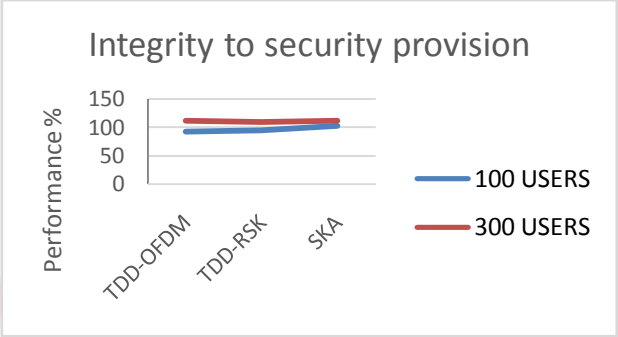

Figure 6.1.4 various dissimilar in Integrity to security provision

Figure 4.2.9 shows the comparative result on intent security produced by different methods. The proposed TDD-RSK method has produced high performance in integrity to security dissimilar than other methods. They represent the Integrity in security performance of the algorithms, SKA algorithm 90% TDD-OFDM 72% and TDD-RSK technique 75% and the overall the proposed SKA technique have the high Integrity Security as compared with other techniques.

USERS	TDD-OFDM	TDD-RSK	SKA
300 Users	92	95	103
500 Users	112	110	112

Table 6.1.4 Processed Data, UN Processed Data and Efficiency of packet processing.

CONCLUSION:

Cloud storage privacy and security problems are major concern that need to be solved we must use new method for cloud storage security enhancement. By implementing Cloud storage many business related security issues and problems and threats will be resolved. By implementation of this proposed work we can increased cloud storage security using encryption, decryption, compression, sharing technique. The compressive sensing method is replaced by the DPI algorithm. Use of DPI algorithm gives us a compressed data's with high quality. Further the splitting of data into chunks then the sequence of chunks saved into a metadata file and encrypting it using AES gives further security to the data. To open secure file, user must need securely their confidential file in storage in secure manner or user can securely transfer their confidential files across the network. By this key, all data will be in encrypted manner. This approach is quite useful because it enables user to keep away the unauthorized person such that he cannot be able to read user files. A Particle Swarm Optimization approach considers various attributes to schedule the workloads. This artificial intelligent perform an automatic work scheduling. That transparently migrates only the working set of an idle VM and support green computing by optimizing the number of servers in use. We use the maximum precedence algorithm to reduce the burden in virtual machine.

REFERENCES:

[1]Enhanced load balancer with multi-layer processing architecture for heavy load over cloud network Navdeep Singh Randhawa 19-21 Oct. 2017.

[2]Towards Quantum Computing Algorithms for Datacenter Workload Predictions Kashifuddin Qazi , Igor Aizenberg 2-7 July 2018.

[3]An experimental study of load balancing of OpenNebula open-source cloud computing platform A B M Moniruzzaman ; KawserWazedNafi ; Syed Akther Hossain 23-24 May 2014

[4]A Novel Cloud Theory Based Time-series Predictive Method for Middle-term Electric Load Forecasting X.M. Yang, J.S. Yuan, H.N. Mao, J.Y. Yuan 4-6 Oct. 2006

[5]Big data transfers through dynamic and load balanced flow on cloud networks C. Jayashri P. Abitha, S. Subburaj 27-28 Feb. 2017

[6]Dynamic weighted virtual machine live migration mechanism to manages load balancing in cloud computing Pradeep Kumar Tiwari ,Sandeep Joshi 15-17 Dec. 2016

[7]New approach for load rebalancer, scheduler in big data with security mechanism in cloud environment Priyanka A. Dhande, A. J. Kadam 2-3 Dec. 2016

[8]"Cloud work load prediction through different models based on time-series"

İlksencaglar, D. TurgayAltıla 5-8 Oct. 2017

[9]Load Balancing of Tasks in Cloud Computing Environment Based on Bee Colony Algorithm K R RemeshBabu ,Amaya Anna Joy, Philip Samuel 2-4 Sept. 2015

[10]A Load Balancing Framework in Cloud to Support Task Processing Using Smartphone with CWC Anantkumar Vikas Salame, Prof. Pradnya V. Kulkarni 6-8 April 2018.

[11]Adaptive Framework for Load Balancing to Improve the Performance of Cloud Manisha Malhotra, Aarti Singh 13-14 Feb. 2015

[12]Dynamic load balancing in cloud based multimedia system with genetic algorithm K V Kavitha, Vinza V Suthan 26-27 Aug. 2016

[13]Load balancing in cloud computing using genetic algorithm Monika Lagwal, Neha Bhardwaj 15-16 June 2017

[14]Incorporating weighted round robin in honeybee algorithm for enhanced load balancing in cloud environment Nithin K. C. Das, Melvin S. George, P. Jaya 6-8 April 2017

[15]Dynamic combination of improved max-min and ant colony algorithm for load balancing in cloud system Navtej Singh Ghumman, Rajwinder Kaur 13-15 July 2015