Performance Analysis of Trust-Based Secured Cloud Storage Processing for Virtualized Green Cloud

(IJCSNT) International Journal of Communication Systems and Network Technologies
ISSN Number: 2053-6283
Volume 2, Issue No. 3, 121–134

https://journals.mirlabs.in/index.php/ijcsnt
DOI- 10.18486/ijcsnt/2.3.027
IJCSNT

Shaji D.S[1], E. Baburaj[2]

Abstract

In cloud computing, prototype is emerged as an energy efficient approach that facilitates ubiquitous, on-demand network access to a shared pool of flexibly reconfigurable sources. The CyberGuarder is designed to address the key security issues faced by the conventional green cloud computing scenarios. The advantage of virtual-based cloud computing provides with the development of energy efficient, highly scalable network software applications (NetApp) by way of providing maximum utility of available resources. CyberGuarder is integrated into internet-oriented virtual computing infrastructure that creates a virtual machine resource management towards resource utilization. To permit the public auditability and data dynamic, a distinctive paradigm that brings the issues related to storage security in cloud poses many new security challenges. Moreover, as the data processing in cloud is distributed, the major hindrance in cloud is the accountability, where the users fears of losing control of their own data. This in turn results in distributed accountability becoming a significant barrier to the wide adoption of cloud services. At the same time, in order to overcome the problem of e-waste with integrating the old and mid-range processors with modern processors, the care regarding the resource efficiency is less. CyberGuarder has laid the foundation for providing solutions in demonstrating its important security assurance role towards the security operation. The Cloud Service Provider (SCP) is one of the important storage pools that helps with users to store their data and provides with the resources to maintain the client data. The optimal resource allocation technique in the green cloud computing provides with the utilization of two types of resources namely, processing capability and bandwidth which are being assigned simultaneously over a period of time. In this paper, various schemes for virtual computing are discussed in detail.

Keywords

CyberGuarder, Cloud Service Provider, ORAT, Public Audibility and Data Dynamics.

Received: 10 August 2013; **Revised:** 29 November 2013; **Accepted:** 05 December 2013; **Published:** 31 December 2013;

[1]Research Scholar, Computer Information Tech, Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India.
[2]Professor, Computer Science and Engg, Sun College of Engineering and Tech, Nagercoil, India.

Corresponding author:
Email: Shajids2004@gmail.com

Introduction

The journey to the cloud computing makes a great provisioning in the IT industry. Cloud Computing is one of the emerging platform for both the industrial and scientific community. The cloud computing is the exploit of computing resources that are distributed as a service above a network. The cloud shaped symbolizes as an abstraction for the complex infrastructure. The cloud data storage provides with significant service towards cloud computing and provides with three different types of services (i) Software as a Service (SaaS), (ii) Platform as a Service (PaaS) and (iii) Infrastructure as a Service (IaaS).

Cloud computing also referred to as the internet-based computing with resources, software and information being shared amount the users, computer and other devices on demand. Cloud computing is a usual calculation of virtualization technologies that facilitate scalable management of virtual machines over an excess of physically connected systems.

Cloud Computing suggest users a transparent level of access to computing and data property from Data Centers. The increasing reputation of Cloud Computing has resulted in the deployment of large scale Data Centers for developing different applications including economy, manageability, and operational efficiency. Cloud computing is more related to a specific method than widely referred to as the technology.

Cloud scenario analyses the entire security challenges through conventional green cloud computing environments. The virtualization security assurance architecture provides with the key for the above mentioned problems related to cloud computing in virtual environment. CyberGuarder, virtualization security assistance architecture is designed to provide mechanisms to address the numerous key security problems within the green cloud computing context. Subsequently, CyberGuarder gives solutions to three different types of services. The three ranges of services provided in CyberGuarder includes security service related to virtual machine, security service in virtual network and a trust-based management service related to fixation of policy.

The expandable cloud resources and enormous datasets processed are subject to security breaches, privacy abuses, and copyright violations. The new approaches to integrate virtual clusters with security-reinforced data centers, and trusted data accesses guided by reputation systems are the key to cloud computing environment. Different types of security countermeasures are recommended to defend cloud service models as IaaS, PaaS, and SaaS, and are currently implemented respectively.

The extensive use of Internet connected systems and distributed applications have triggered a revolt towards the adoption of pervasive and cloud computing environments everywhere in wide manner. These environments allow the users and clients to obtain computing power according to their specific requirements, and accordingly elastically adapting to different performance needs while providing higher availability. The widespread use of Internet connected to numerous systems and distributed application has triggered a rebellion towards the acceptance of pervasive and ubiquitous cloud computing environments. These internet-based and distributed environments provides with the users and clients to make availability of computing power according to their specific requirement of the user, at the same time adopting to varied performance needs while maximizing higher availability.

Literature Review

Several works have been conducted to provide mechanisms for cloud using the privacy preservation. One of the several methods for privacy-preserving is Homomorphic cryptography and Zero-Knowledge Proof that is based on privacy-preserving method for cloud publish service. The author in[1] with homomorphic

cryptography and zero-knowledge proof used to attain three main contributions comprising of (a) professional privacy-preserving verification, (b) data integrity and (c) publish-subscribe confidentiality.

Although all advertise encircle the cloud, enterprise customers are still indisposed to deploy their business in the cloud. One of the main problems related to cloud computing is security that condenses the growth of cloud computing. The next difficulty in cloud arena is related to data privacy and data protection that continue to afflict the market. In [2] the service delivery model required for the cloud service users has discussed about the thorough understanding of the risks of data contravene in the new environment. The author presents the method to protect the data confidentiality for guest virtual machines. To improve the data privacy of virtual machines in cloud computing was the main area of discussion provided in [3]. Here the cloud computing service supplier can not access the private data of their clients. The accessibility is only ensured through the trusted third party provider present in the cloud environment.

The cloud computing poses challenging and incompetent solution for daily routines related to cloud computing. The established difficulty connected with cloud computing is the cloud security and the suitable implementation of cloud over the network was provided in [4] using RSA encryption structure. The main objective of providing security in cloud using RSA encryption mechanism was to explore into the problems related to the cloud computing security problem. Moreover, it also aims to explore and establish a secure channel for the single information owner to communicate with the other multi corporate information owner. At the same time, the cloud service provider maintains the trust and the confidentiality of the data of user at different level of operations. The intention of the work in [5] was to provide with analyzing different protocols and suggest the best method keeping in mind the requirement of the security property of the user in cloud environment. Moreover, the confidentially of the data was also maintained along the line of security in cloud computing environment (CCE).

In order to build an expectation computing environment for cloud computing system which directly integrates the trusted computing stage into cloud computing system, a model system was designed in [6] where the cloud computing system shared the information system is with trusted computing platform using trusted platform module. Here the major task of cloud provider is to establish the key management and cloud key management (CKMI) with the users. Creation and subsequent adoption force decrease the difficulty of encryption management. In [7] to enable support for interoperability inside cloud cryptographic clients and cloud management servers, cloud key management decrease connections costs and the risks involved in the designing of key for users in cloud.

The work of providing privacy for virtualization machines where the mass administrator cannot be trusted, ideas has to be created to identify and determine the forward thoughts to defend the privacy of virtualization machines. Using virtualization environment, threat model was identified in [8] and subsequently a series of security prospects were evolved which are of real-world concerns. Measures were also taken to leverage the trusted computing technologies and probable explanation in these security threats were detailed in [8].

Providing security in cloud computing is the main hindrance. Several measures have been followed and adapted towards it. To recognize and encrypt all functionally encryptable data, responsive data that can be encrypted without preventive the functionality of the application on the cloud, the work of [9] provided measures to accumulate the data on the cloud only in an encrypted form, which was again available and accessible only to users with the correct keys. The web technology has provided with the users to provide their data and consume any form of data from the cloud in an easy manner. It has called for a model change in the computing architecture and huge level data processing mechanisms. This pattern

shift paradigm from the location of this transportation to the network to reduce the costs associated with the management of hardware and software resources related to data management approaches in cloud were discussed in [10].

To make sure the integrity of data storage in cloud computing is obtained and processed at all level from the point of user and cloud, the task of permitting a third party auditor (TPA) was provided in various studies. Based on the information provided by the user to the cloud, the integrity of dynamic data is ensured from both the user and cloud. Subsequently, the introduction of third party auditor in [11] ensures and at the same time eliminates the connection of the client during the audit of whether his data stored in the cloud data.

The initialization of third party auditor has been indeed intact that are significant in terms of economy of scale for cloud computing. In [12] efforts were made to provide an analysis of energy consumption in cloud computing. The analysis gives a detailed study of energy consumption required in both public and private clouds and at the same time in switching and broadcast as well as data processing and data storage. The analysis of the key security hindrances faced in the modern green cloud computing environments and gives measures towards virtualization security assurance architecture. CyberGuarder is intended to address some key securities in green cloud computing context.

Methodology

Different analysis involved in "Trust-based Secured Cloud Storage Processing for Virtualized Green Cloud" is

CyberGuarder: Virtualization Security Assistance Architecture

Virtualization is considered to be one of the predominant techniques in current computing scenarios. The deployment of virtualization in cloud computing results in cost reduction towards hardware and minimize the maintenance costs by method of consolidating the usage of servers. At the same time, green computing results in reducing the power consumption and forms a basis for cloud computing by providing of greater range of virtual supercomputers and networks. To connect the individual computing power and storage devices, the iVIC in [13], an internet-based virtual computing infrastructure is a network computing platform that support on a distributed virtual resource container. As a result of this, iVIC provide certain virtualized entities comprising of VMs or vDisks.

The virtual machines are organized and attach into virtual networks. Users also assign their own virtual cluster in iVIC to maintain hardware as a service (vHaaS) and software as a service (vSaaS). Through iVIC the software and hardware property are controlled in respective resource pools. Using iVIC as the base, the software assigned from software pool are easily downloaded and installed and further configured into VMs in a hardware pool on-demand made by the corresponding users with four key issues discussed in [13]. The four key issues related to VM, the virtual machine security support, VMM based software integrity verification, multi-granularity NetApp sandbox mechanism and virtual network security service is designed.

Virtual Machine Security Support The virtual machine security support in [13] not only provide trust loading approach towards VMM-based NetApp but also ensures a multilevel security in an isolated manner for the virtual machine in cloud setting.

VMM based software integrity verification This system calls interception approach to provide load-time and run-time reliability defense mechanisms for a NetApp. First CyberGuarder VMInsight, identifies and determines the series of system call made in order to control and analyze the loading of software that comprises of user-defined applications, libraries shared between the users and kernel specific modules. The second set of action to be performed is system call that establishes the relationship between different calls made by VM simultaneously. Finally the third set of action performed by VMInsight in [13] is to monitor the different types of jobs performed by NetApp processes in order to differentiate between the malicious attacking patterns. The VM system also maintains its correctness and security through the protection mechanism in VMM level even though if the guest OS kernel has been comprised. The VMInsight system in [13] provide with certain level of legacy and hence requires no more changes performed to the guest OS.

Multi-granularity NetApp sandbox mechanism The availability and securitizing of applications deployed in virtual environmental scenario can be further improved based on the isolation metric, and at the same time is far superior to certain kind of applications running in a conventional or non-virtualized system. Even though the virtual machines share the physical resources of a computer, they are completely isolated from each other of the computers as if they were in different physical machines. In [13], the virtual network level isolation was performed with CyberGuarder.

Virtual Network Security Service In [13], an adaptive security service model was designed for virtual network environments. The principle behind the virtual network security service is that the conventional network security service is encapsulated into virtual security system and adaptively implemented into virtual networks to protect the applications that are run in virtual networks. A dynamic mechanism is also designed in [13] based on fuzzy control theory. The working of fuzzy control in virtual network is designed in a way such that is based on the varied network traffic where the resource is assigned continuously for the purpose of virtual security appliance by satisfying energy consumption requirements.

Public Auditability and Data Dynamics in Cloud Computing

In [11], to achieve data dynamics the conventional storage models are modified in such a way that efficient multi handling tasks are achieved using classic Merkle Hash tree. The objective of [11] was to provide auditability that allows anyone to verify the correctness of data that are stored in cloud, allows clients to provide block operations and at the same time it also ensures that no possibility of retrieval by the verifier is made during the process of verification.

Public Auditability In [11], public auditability is achieved using the homomorphic authenticator technique. Homomorphic authenticators are one form of unforgeable metadata that are generated from single data blocks. The homomorphic authenticators are securely aggregated in such a way to assure with a verifier such that linear combination of data blocks is evaluated by making sure that only the aggregated authenticator acts as the verifier. The work of [11] uses PKC-based homomorphic authentication method to help with the verification protocol to provide with public auditability.

Dynamic Data Operation with Integrity Assurance The default integrity verification in [11] makes the third party auditor verify the integrity of data by way of providing a challenge to the server. Before proceeding with the process of challenge, the third party auditor uses a key to verify the signature. Based

on the results of the verificaiton process, the proceedings continue with the process of several dynamic data operations. It includes data modification, data insertion and data deletion from cloud environment.

Provisioning of block operations One of the advantages related to cloud environment as discussed in [11], is its ability to handle multiple verification sessions from numerous clients given with N signatures on N distinct data files from N clients. It is of high advantage to combine all these signatures into a single form and verify it at one at a time. In order to achieve this goal, the scheme is extended to allow for provable data updates and verification is performed in a multi-client system in [11] by way of using the bilinear aggregate signature scheme. The advantage of bilinear aggregation signature scheme in [11] is it supports the combination of multiple signatures, by different signers on different form of messages into single short signature.

Cloud Information Accountability for Data Sharing in the Cloud

In [14], a decentralized information accountability framework was designed in order to keep track of actual users' usage in cloud environment. An object-centered approach was presented in [14] that presented a logging mechanism for the corresponding users' data and policies. At the same time, to strengthen the users' control in cloud distributed auditing mechanisms was also provided. The Cloud Information Accountability framework presented in [14] performs with automated logging mechanism and also conducts distributed auditing of relevant access processed by any user, carried out at any interval of time at any cloud service provider levels with the help of two differing components logger and log harmonizer.

Logger in Cloud Information Accountability The logger in [14] is highly associated with the data provided by the user and has the strong relationship between the data being accessed and data copies by the user. At the same time, the job of logger is to access or handle the particular copy provided by the user. The logger as in [14] requires minimal support from the server side in order to be implemented. The permanent coupling between data and logger, achieves a highly distributed logging system. At the same time, the logger need not be installed on any machine. Finally, the responsibility of the logger is to generate the error correction information for subsequent log record and send it to the log harmonizer. The error correction information is combined with authentication and encryption mechanism that results in robustness and strong reliable mechanism.

Log harmonizer in Cloud Information Accountability The job of log harmonizer in [14] acts as the central component that allows the user access to the specified log files. The log harmonizer also provides with two other auditing policies namely, push and pull. During the process of push, the file is pushed to the owner of specified data in a periodic manner automatically. During the process of pull mode, an approach based on on-demand, the file is obtained by the owner of the data whenever required.

Automated Logging mechanism The automated logging mechanism is performed using JARs. The automated logging mechanism comprises of a nested Java JAR file which periodically stores the user's data items and subsequent log files of the respective users. As shown in figure, the JAR file as in [14] comprises of one outer JAR that are enclosed again with one or more inner JARs. The job of the outer JAR in [14] is to offer authentication of user who want to access the data stored in the form of JAR file. The objective of the outer JAR is also to provide the access control probability in order to give the data owner's requirements. The Java policy mentions the types of permissions that are readily available for

a specific part of code in Java application environment that are in terms of File System Permissions. Anyhow, the owner of the data owner can also provide with the permissions in terms of user-centric than to the conventional code-centric provided by Java, by way of using Java Authentication and Authorization Services.

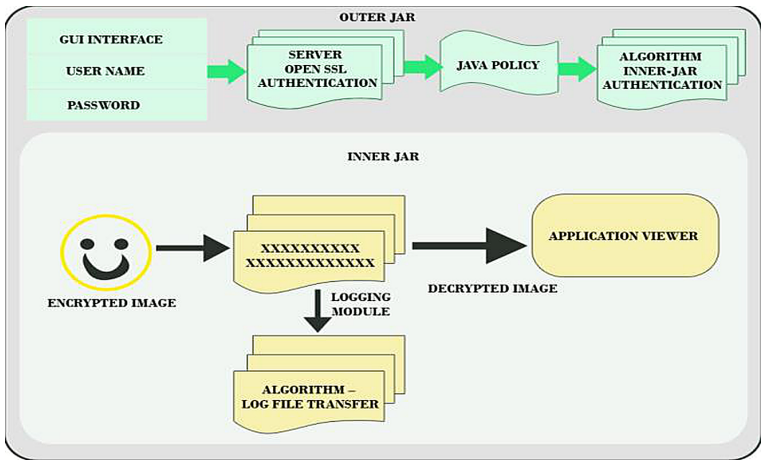

Figure 1. Framework of JAR file

Optimal Resource Allocation Technique (ORAT)

Several researchers have presented the work on optimal resource allocation for cloud environment. In [15], the author designed optimized resource allocation method using the basic design model in such a way that the requisite resource is obtained from a joint resource pool. In addition, to be capable of providing the processing capability and storage power, it is highly required that the bandwidth should be assigned to the respective user at same time interval. In [15], the author proposed an optimal resource allocation method for green cloud computing environments. The ORAT presumes the utilization of two types of resources, namely processing capability and bandwidth. The services in general are divided into two types comprising of a non-delay system and a waiting scheme. The design principle of non-delay system in [15] assigns the addition resource required for the user ahead of the request, and discards the request given by the user if there is no additional capacity. The other service, waiting system assigns the additional capability to the respective users in the series in which their needs are in order, immediately upon the advent of a request. The ORAT in [15] uses the service that sprints as non-delay.

Resource Allocation in Cloud Environment In the cloud computing scenario, the resource allocation is characterized as transfer of the essential quantity of resource concurrently to the user present in the cloud. The author in [15] presented with two types of resources namely, bandwidth and processing capability. The resource allocation of bandwidth and processing capability in [15] works on the principle that whenever the service request appears to the finest center that has been selected from frequent centers, both the dispensation capacity and bandwidth accessible in the chosen center are owed for a definite period of time. If no center has a satisfactory magnitude of secondary resources the request is discarded.

ORAT for Green Cloud Computing The green cloud computing distribution in[15] is designed in such a way that the both resource processing capability and bandwidth are maintained is assigned with the corresponding requests. The rate at which the amount of necessary resource processing is assigned is not only measured with that of necessary bandwidth but the resource allocation is said to be optimal if only a single resource category is calculated in the assortment of a center. The user which requires the balanced size of resources comprising of processing capability and bandwidth when compared to the resource as required by the user is selected as the recognized resource. The algorithmic representation of ORAT for green cloud environment is given below

```
Initialize available processing capability and bandwidth for
each type of processor from varied pools.
Repeat
User requests are received on hourly intervals.
For (each user request) do
    Identify resource and bandwidth utilization for
    respective user
    Identify jobs from job-resource appropriation file.
    For (each user request) do
    For (each job-resource appropriation) do
        Verify with varied processor pools.
        Perform allocation of resources to
        corresponding job
        Accomplished jobs for the users are
        recorded with its user consumption and bandwidth
        utilization.
        Measure actual utilized bandwidth and
        resource capability
        De-allocation of resources from
        corresponding user
    End for
    End for
End for
Until (job completion)
```

Performance Results

The section given below demonstrate the performance analysis of various scheme through experiments with trust based security cloud cluster storage processing scheme for virtualized green cloud computing applications. The performance metrics are measured in terms of

- Data Transfer Rate
- Energy Consumption
- Communication Overhead
- Resource Loss Probability

Data Traffic Rate

The table given below shows the data transfer rate on the basis of number of users present in cloud environment. Four methods CyberGuarder, GDH method, CIA method and ORAT are taken into consideration.

Table 1. No. of Users Vs Data Traffic Rate

No. of Users	Data Traffic Rate (%)			
	CyberGuarder	GDH Method	CIA Method	ORAT
2	15	30	43	50
4	34	43	56	65
6	39	49	62	68
8	52	57	70	75
10	63	70	75	80
12	67	75	80	82

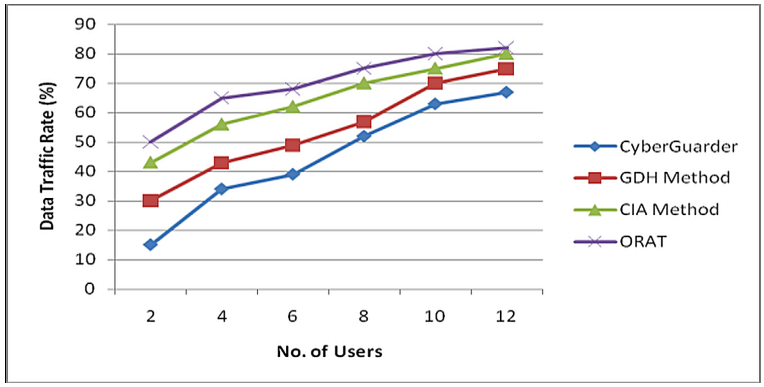

Figure 2. Measure of Data Traffic Rate

Fig 4.1 demonstrates the number of user with the data traffic rate using different methods. These results illustrates that when the number of user gets increased then the data traffic rate also gets increased. Data traffic rate gets higher in ORAT which is due to the fact that when compared to other three methods, ORAT followed resource utilization path by applying the optimal resource utilization technique. The ORAT when compared with the schemes of GDH method, CIA method and ORAT using cloud, Fig 4.1 shows that these experimental results prove to be better in terms of performance in ORAT when compared with other methods.

Energy Consumption

The table given below shows the energy consumption level on the basis of the mobility rate of the user present in cloud environment. Four methods CyberGuarder, GDH method, CIA method and ORAT are taken into consideration.

Table 2. Mobility Rate Vs. Energy Consumption

Mobility Rate	Energy Consumption (Joules)			
	CyberGuarder	GDH Method	CIA Method	ORAT
20	200	300	410	500
40	218	320	425	520
60	220	342	431	534
80	246	354	439	548
100	251	363	446	562
120	259	376	453	569

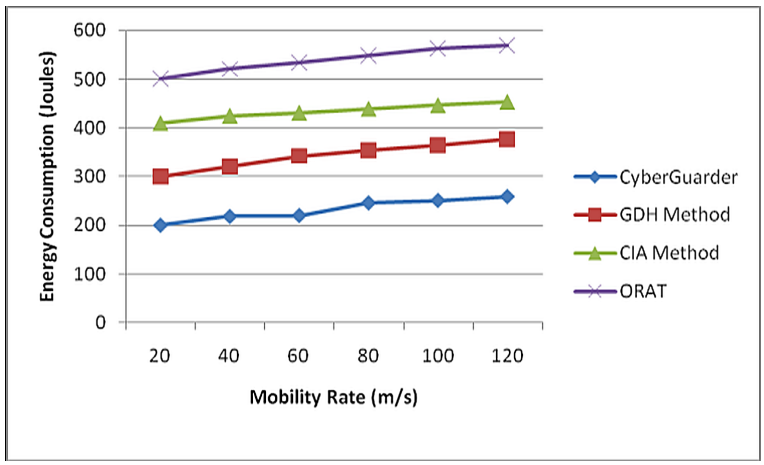

Figure 3. Measure of Energy Consumption

Fig 4.2 demonstrates energy consumption with respect to mobility rate. This analysis relies greatly on CyberGuard. When the mobility rate increases the energy consumption also gets increased. This experimental result shows the better performance of energy consumption. CyberGuarder present the minimum energy consumption due to the VMM-based integrity measurement approach when compared with the existing methods.

Communication Overhead

The table given below shows the communication overhead generated for the different number of users present in cloud environment. Four methods CyberGuarder, GDH method, CIA method and ORAT are taken into consideration.

Figure 4.3 illustrates the communication overhead generated for different number of users present in the cloud computing environment. The communication overhead increases with the number of available users. From the figure it is evident that communication overhead is less in CIA when compared to three other methods, CyberGuarder, GDH method and ORAT method. This is due to the fact that CIA

Table 3. No. of Users Vs Communicational Overhead

No. of Users	Communication Overhead (secs)			
	CIA Method	CyberGuarder	GDH Method	ORAT
2	4	7	8	12
4	7	10	14	18
6	8	15	20	22
8	12	15	19	25
10	15	20	25	28
12	20	22	25	30

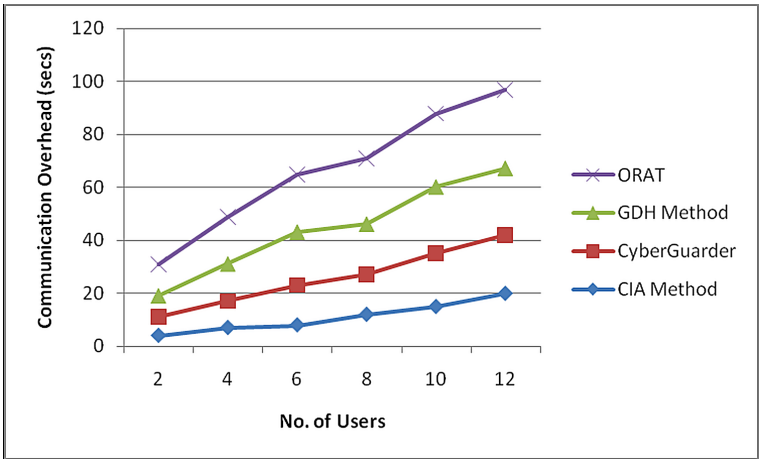

Figure 4. Measure of Communicational Overhead

is a framework based on information accountability that provides end-to-end accountability in highly distributed fashion.

Resource Loss Probability

Table 4. No. of Users Vs Resource Loss Probability

No. of Users	Resource Loss Probability (%)			
	CIA Method	CyberGuarder	GDH Method	ORAT
2	0.25	0.15	0.12	0.5
4	0.30	0.22	0.15	0.9
6	0.35	0.35	0.22	1.2
8	0.45	0.45	0.28	1.4
10	0.50	0.50	0.35	1.5
12	0.55	0.55	0.40	1.8

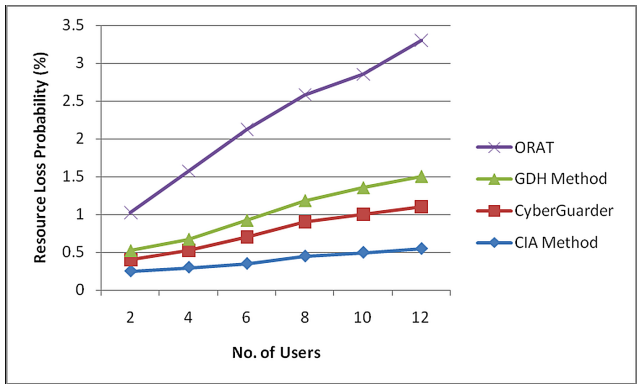

Figure 5. Measure of Resource Loss Probability

Fig describes the users' task resource loss probability based on number of user present in the cloud computing environment. It compares the resource loss prospect in the situation where the sizes of processing capability and bandwidth are high. From the figure it is evident that ORAT reduces the resource loss possibility and as a result, minimizes the total amount of resource when compared with the three other methods, CyberGuarder, CIA and GDH.

Research Directions

Cloud computing is one of the natural extension of virtualization technologies that enable scalability in the management of virtual machines. The virtualization-based cloud computing paradigm offers a practical approach to green IT/cloud, scalability and energy-efficient network software applications. Recent works on virtualization security assurance strategies include data dynamism for storage security, virtual machine security service, analysis of energy consumption, inclusion of third party auditor, RSA encryption algorithm and so on.

The virtual machine security service incorporates VMM-based integrity measurement approach, Multi-granularity mechanism to enable OS user isolation and Dynamic approach to virtual machine and network isolation for multiple NetApp based on energy-efficiency and security requirements. At the other end, analysis of energy consumption in cloud computing includes both public and private clouds which evolves the inclusion of energy consumption in switching and transmission. Subsequently, the deployment of Third party auditor (TPA) verifies the integrity of the dynamic data stored and also eliminates the involvement of the client through the auditing. The introduction of RSA encryption algorithm results in the enhancement of data Security in cloud computing environment whilst demonstrating the authenticity of a digital message.

In all the recent works presented, data confidentiality is assumed learning high level intuitions are set of classification and automatic partitioning of the applications. From the above listed research gap, a refined approach to verify the security of different users using trust as a model can be proceeded in the cloud computing environment to achieve higher data processing rate as a key factor.

Conclusion

This paper discussed about the CyberGurder, an approach to demonstrate its important security assurance aspect to solve the security related issues. The Cloud Service Provider (SCP) acts as one of the important storage space and computation resource that in turn maintains the client data that uses Hardware as a service (vHaaS) and software as a service (vSaaS) to maintain the application scenario. At the same time, CIA presented with the novel methods for the sake of automatically logging of access to the data in the cloud environment in addition to the auditing mechanism. The advantage of CIA was the acceptance of the owner of data to provide with back-end protection. The optimal resource allocation technique in the green cloud computing assume the utilization of two types of resource of processing capability and bandwidth that are distributed to the users requested of timely manner.

References

[1] Yanping Xiao, Chuang Lin, Yixin Jiang, Xiaowen Chu, and Fangqin Liu, "An Efficient Privacy-Preserving Publish-Subscribe Service Scheme for Cloud Computing", IEEE Communication Society, 2010.

[2] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of network and computer applications, Vol. 32, pp. 1–11, 2011.

[3] Jinzhu Kong, "A practical approach to improve the data privacy of virtual machines", IEEE International Conference on Computer and Information Technology, 2010.

[4] Uma Somani, Kanika Lakhani, and Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", International Conference on Parallel, Distributed and Grid Computing, 2010.

[5] Mahbub Ahmed, Yang Xiang, and Shawkat Ali, "Above the Trust and Security in Cloud Computing: A Notion towards Innovation", IEEE International Conference on Embedded and Ubiquitous Computing, 2010.

[6] Zhidong Shen and Qiang Tong, "The Security of Cloud Computing System enabled by Trusted Computing Technology", International Conference on Signal Processing Systems, 2010.

[7] Sun Lei, Dai Zishan, and Guo Jindi, "Research on Key Management Infrastructure in Cloud Computing Environment", International Conference on Grid and Cloud Computing, 2010.

[8] Jinzhu Kong, "Protecting the confidentiality of virtual machines against untrusted host", International Symposium on Intelligence Processing and Trusted Computing, 2010.

[9] Krishna P. N. Puttaswamy, Christopher Kruegel, and Ben Y. Zhao, "Silverline: Toward Data Confidentiality in Storage-Intensive Cloud Applications", Journal of Computer Applications, 2011.

[10] Sherif Sakr, Anna Liu, Daniel M. Batista, and Mohammed Alomari, "A Survey of Large Scale Data Management Approaches in Cloud Environments", IEEE Communications Surveys and Tutorials, Vol. 13, No. 3, 2011.

[11] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 5, May 2011.

[12] Jayant Baliga, Robert W.A. Ayre, Kerry Hinton, and Rodney S. Tucker, "Green Cloud Computing: Balancing Energy in Processing, Storage, and Transport", IEEE Transactions, Vol. 99, No. 1, Jan 2011.

[13] Jianxin Li, Bo Li, Tianyu Wo, Chunming Ju, Jinpeng Hu, Lu Liu, and K.P. Lam, "CyberGurder: A virtualization security assurance architecture for green cloud computing", Journal of Future Generation Computer Systems, Vol. 28, pp. 379–390, 2012.

[14] Smitha Sundareswaran, Anna C, Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud", IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 4, July/August 2012.

[15] K. L. Giridas, "Optimal Resource Allocation Technique (ORAT) for Green Cloud Computing", International Journal of Computer Applications (0975–8887) Volume 55– No.5, October 2012.