ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 5, November 2019

Computing Service via the Internet on Demand in Cloud Computing

Rajiv Gupta, Vidhu Ghuse, Kiran Dukre, B. P. Borkar, Sanjogita Verma
Department of CSE, CIET, Ambikapur, Chhattisgarh, India

Abstract: ***Cloud computing is architecture for providing computing service via the internet on demand and pay per user access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. To overcome this disadvantage use Ripplet Transform (RT) has been implemented along with the neural network based mostly classifier referred to as multilayered perceptron (MLP) for locating a good retrieval of image. So it saves managing cost and time for organizations. For example, the same file may be saved in several different places by different users, or two or more files that aren't identical may still include much of the same data. De-duplication eliminates these extra copies by saving just one copy of the data and replacing the other copies with pointers that lead back to the original copy. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. The chemical composition analysis declared that the statues are made of leaded bronze alloy. The patina of the examined objects were consisted of two layers and composed of Cuprite, Atacamite, Quartez. Finally they obtained results helped us in treatment and conservation the selected objects.***

Keywords: **Security Issues, flow pattern, oscillatory flow reactor, Cloud Platform, Grid Computing.**

I. INTRODUCTION

Cloud computing in today's era is one of the most popular IT innovations. Several IT companies have decided or already acquired products which are as per the cloud computing paradigm. In future it can be expected to see lot new security exploitation events around cloud computing providers and users, which will give the cloud computing security research directions for the next decade. The most widely used method to produce biodiesel (monoalkyl esters) is transesterification method [3,4], where the raw materials are derived from a variety of bio-oils (triglycerides) is reacted with methanol (CH3OH) or ethanol (C2H5OH) by addition catalyst such as sodium hydroxide (NaOH) or potassium hydroxide (KOH) under conditions of temperature 65 ^{0}C approximately. In addition to biodiesel are formed, it is obtained glycerol by-product that can be used as raw material for organic cosmetics and soaps.

A. Cloud Computing

The National Institute of Standards and Technology (NIST) Information Technology Laboratory, cloud computing is defined as follows:

- Research on biodiesel production process is mostly done concerning some issues related; type of raw materials, catalysts, methods and production system.
- This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models [3,4,5].

B. Essential Characteristics

- So there exists a possibility of attackers which can easily compromise MANETs by inserting malicious or non-cooperative node into the network. So, security is the important aspect in deploying MANET[2].
- Many researchers are focusing in this specific area as there exists enormous number of security mechanisms. Due to MANET's distributed architecture and changing topology, a traditional monitoring technique or other security methods employed in strategic points like routers, switches are no longer feasible in MANETs. Intrusion detection system is to be designed specifically for MANETs which utilizes its properties and to reduce all its security challenges.
- Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- Educational institutions are regarded as service industry to have an important role in developing well educated, smart, talented human capital for the future. Hence, the primary players are teachers who are responsible to generate human capital for the future which is a requirement of the nation.

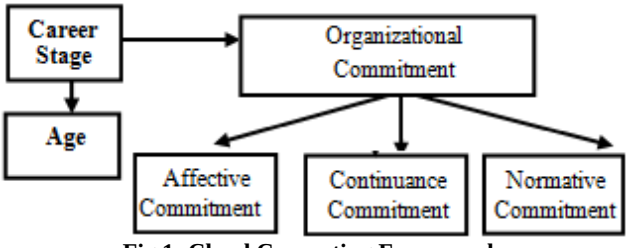

Fig 1: Cloud Computing Framework

C. Service Models

- Abaza, Bisset, and Sadler, 2004; and Krishnamoorthy, 2008; and Glasson, Therivea, and Chadwick, 2005 argued that, the following components including, self-directed assessment by development proponents and

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 5, November 2019

agencies; oversight of EIA implementation by a designated body; guidance on conducting EIA in accordance with legal and procedural requirements; and Public involvement including measures related to availability of information and opportunity to comment on the content of EIA reports and documentation. All of them comprise what may be termed the administrative machinery for delivering the principles of EIA process design and implementation that have gained a measure of international acceptance.

- Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.
- A comparative trend analysis of Non-Performing Assets of commercial banks in India is tabulated in the table. However, the asset quality has deteriorated during 2014 with sharp increase in gross NPA of commercial banks. There is sudden increase in NPA from 2.94% in 2013 to 3.42% in 2014. The sudden increase in NPA could be because of the slowdown in the domestic economy as well as inadequate appraisal and monitoring of credit proposals. (RBI, 2012).Growth rate of gross NPA has increased at higher rate and at the same time Growth rate of advances has also increased. This can be one of the causes for sudden increase of NPA in Commercial banks.

D. Deployment Models

- It has been observed that the percentage of net NPAs to total advances declined from 2.98 per cent in March 2008 to 1.10 per cent in March 2014 and further 0.431 per cent in March 2015. This significant reduction of net NPAs may be due to the definitional changes of NPAs with the introduction of 'net NPA' concept by RBI.
- Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).
- The underlying technology also provides comparatively reduced sample size, reagent volume and power consumption by micromanipulation of discrete fluid particles (droplets).

II. SECURITY ISSUES

Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form. T In a study, meditation and relaxation were compared with the control group to see the effects on psychological distress, positive states of mind, distractive-ruminative thoughts, behaviors, and spiritual experience. Though, both the groups improved significantly with the control group but the meditation group was found to be relatively more efficacious as compared to the other groups [4].

The given below are the various security concerns in a cloud computing environment:

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

Access to Servers & Applications: In traditional datacenters, administrative access to servers is controlled and restricted to direct or on-premise a connection which is not the case of cloud data centers. In cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. As we could see that, the case has improved much on the symptoms of psychological distress, upset mood and negative thoughts and ruminations by her involvement in the process of self realization process, bringing a significant change in her attitude [3,4]. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users.

Data Transmission: Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here. In Cloud environment most of the data is not encrypted in the processing time. Hence, she realized that these voices cannot harm her and the only thing that could harm her is her own thoughts and ruminations of the mind. But to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 5, November 2019

Virtual Machine Security: Virtualization is one of the main components of a cloud. Virtual machines are dynamic i.e. it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. Watkins and Teasdale [9] elaborated similar effects due to adaptive analytical and experiential self focused treatment on ruminations and depressive symptoms. They can also be readily cloned and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. Vulnerabilities or configuration errors may be unknowingly propagated. Also, it is difficult to maintain an auditable record of the security state of a virtual machine at any given point in time. Full Virtualization and Para Virtualization are two kinds of virtualization in a cloud computing paradigm. In full virtualization, entire hardware architecture is replicated virtually. However, in para-virtualization, an operating system is modified so that it can be run concurrently with other operating systems. VMM (Virtual Machine Monitor), is a software layer that abstracts the physical resources used by the multiple virtual machines. The VMM provides a virtual processor and other virtualized versions of system devices such as I/O devices, storage, memory, etc. 10 gm powder of each plants parts (stem and leaves) were extracted successfully with methanol, ethanol, chloroform and petroleum ether and water. The extract obtained from successive solvent. Extract were filtered and stored in air tight bottle at 4 c and further used for investigation. Vulnerability in Xen can be exploited by “root” users of a guest domain to execute arbitrary commands.

Network Security: Networks are classified into many types like shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of DNS attacks, Sniffer attacks, issue of reused IP address, etc which are explained in details as follows.

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems.

Sniffer attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. The paper disc(6 mm diameter) were separately impregnated with 15 µl of extract or main components of essential oils and placed on the agar which had previously been inoculated with the selected test microorganism.

Reused IP address issues have been a big network security concern. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches. And hence, we can say that sometimes though the old IP address is being assigned to a new user still the chances of accessing the data by some other user is not negligible as the address still exists in the DNS cache and the data belonging to a particular user may become accessible to some other user violating the privacy of the original user [12].

Data Security: For general user, it is quite easy to find the possible storage on the side that offers the service of cloud computing. To achieve the service of cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). Plant derived antimicrobial agents has great perspectives in medicine and pharmaceutical industries. In the present investigation, methanolic and other extracts of *Tamarix ericoides* were tested for its antibacterial activity against few pathogenic bacterial strains like Bacillus subtilis, E. coli, S. typhi and fungal strain *C. albicans* The results are presented in Table-1. All such accesses are logged and routinely audited. While the data at rest in Simple Storage Service (S3) is not encrypted by default, users can encrypt their data before it is uploaded to Amazon S3, so that it is not accessed or tampered with by any unauthorized party [13].

Data Privacy: The data privacy is also one of the key concerns for Cloud computing. A privacy steering committee should also be created to help make decisions related to data privacy. Requirement: This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks [13].

Data Integrity: Data corruption can happen at any level of storage and with any type of media, So Integrity monitoring is essential in cloud storage which is critical

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 5, November 2019

for any data center. Data integrity is easily achieved in a standalone system with a single database. Data integrity in such a system is maintained via database constraints and transactions. The adsorption capacity q (mg/g) and removal efficiency were calculated according to the equations (1) and (2) respectively: Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control.

Data Location: In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. In many a cases, this can be an issue. Due to compliance and data privacy laws in various countries, locality of data is of utmost importance in many enterprise architecture. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In addition to the issue of local laws, there's also the question of whose jurisdiction the data falls under, when an investigation occurs. Next in the complexity chain are distributed systems. In a distributed system, there are multiple databases and multiple applications [15].

Data Availability: Data Availability is one of the prime concerns of mission and safety critical organizations. When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider. If the Cloud goes out of operation, data will become unavailable as the data depends on a single service provider. The questionnaire includes construction parameters like labors, measures, materials, methods, equipment unassignable events, scheduling, contract procedures and site management safety measures adopted at the construction site such that from the questionnaire survey the factors affecting quality in the construction sites is determined. The Cloud application needs to ensure that enterprises are provided with service around the clock. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. A multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers. Resiliency to hardware/software failures, as well as to denial of service attacks, needs to be built from the ground up within the application. At the same time, an appropriate action plan for business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies.

Data Segregation: Data in the cloud is typically in a shared environment together with data from other customers. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data. Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals [16].

Security Policy and Compliance: Traditional service providers are subjected to external audits and security certifications. There are several MGA tools were proposed like Ridgelet, Curvelet and Contourlet etc. These MGA tools do not suffer from the problems of wavelet. for improve the fusion result used MGA tools [3], [4]. For proposed technique used RT in the proposed method, because RT is capable of resolving two dimensional (2*D*) singularities and representing picture edges more efficiently. If a cloud service provider does not adhere to these security audits, then it leads to a obvious decrease in customer trust. Enterprises are experiencing significant pressure to comply with a wide range of regulations and standards such as PCI, HIPAA, and GLBA in addition to auditing practices such as SAS70 and ISO. Enterprises need to prove compliance with security standards, regardless of the location of the systems required to be in scope of regulation, be that on-premise physical servers, on-premise virtual machines or off-premise virtual machines running on cloud computing resources. An organization implements the Audit and compliance to the internal and external processes that may fallow the requirements classification with which it must stand and the requirements are customer contracts, laws and regulations, driven by business objectives, internal corporate policies and check or monitor all such policies, procedures, and processes are without fail.

Securing Data-Storage: Data protection is the most important security issue in Cloud computing. In the service provider's data center, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. Encryption keys share securely between Consumer and the cloud service provider and encryption of mobile media is an important and often overlooked need. PaaS based applications, Data-at-rest is the economics of cloud computing and a multitenancy architecture used in SaaS. In other words, data, when stored for use by a cloud-based application or, processed by a cloud-based application, is commingled with other users' data. In cloud computing, data co-location has some significant restrictions. In public and financial services areas involving users and data with different risks. The cloud-wide data classification will govern how that data is encrypted, who has access and archived, and how technologies are used to prevent data loss. At the cloud provider, the best practice for securing data at rest is cryptographic encryption and shipping self encrypting is used by hard drive manufacturers. Self-encrypting provides automated encryption with performance or minimal cost impact [17].

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 5, November 2019

Cloud Management: The self-service nature of cloud computing may create confusion for patch management efforts. Once an enterprises subscribes to a cloud computing resource—for example by creating a Web server from templates offered by the cloud computing service provider—the patch management for that server is no longer in the hands of the cloud computing vendor, but is now the responsibility of the subscriber. Keeping in mind that according to the previously mentioned Verizon 2008 Data Breach Investigations Report, 90% of known vulnerabilities that were exploited had patches available for at least six months prior to the breach, organizations leveraging cloud computing need to keep vigilant to maintain cloud resources with the most recent vendor supplied patches. Transform used to create a new tight frame with sparse representation for picture with discontinuities along *Cd* curves [12]. If patching is impossible or unmanageable, compensating controls such as "virtual patching" need to be considered.

III. SOLUTION FOR SECURITY ISSUES

Following approaches can be helpful for secure cloud computing:

- Investigation Support: Audit tools provided to the users to determine how their data is stored, protected, used, and verify policy enforcement. But investigation of illegal activity is quite difficult because data for multiple customers may be collocated and may also be geographically spread across set of hosts and datacenters. To solve this audit tools must be contractually committed along with the evidence.
- Geopolymerization is the chemical reaction between alumino silicate oxides with silicates under highly alkaline condition to form polymers called geopolymers. Geopolymer is an alternate to the Ordinary Portland Cement.
- Network Security: A user can deny the access of any Internet based service by using IP Spoofing which can be a cause of security harm [6]. To solve this we can use Digital Signature technique. SSL (Secure Socket Layer) Protocol is used for managing security of message transmission on The Internet. Which also avoid resource hacking.
- Encryption Algorithm: Obviously cloud service providers encrypt the user's information using strong encryption algorithm. But problem is that encryption accident can make data totally unusable and encryption also complicates the availability [6]. The term six sigma (6σ) originated as a performance measure or a measure of quality. Six sigma, process goals are set in parts per million (PPM) in all areas of the building production process. To solve this problem the cloud provider must provide evidence that encryption scheme were designed and tested by experienced specialists.
- Backup: Natural disaster may damage the physical devices that may cause of data loss. To avoid this problem backup of information is the key of assurance of service provided by vendor.
- Customer satisfaction: Very hard for the customer to actually verify the currently implemented security practices and initiatives of a cloud computing provided by the service provider because the customer generally has no access to the provider's facility which can be comprised of multiple facilities spread around the globe [8]. Then the sigma level for buildings is calculated using the DPMO computation methodology after identifying the defects and the root causes for the defects are analyzed and suggests the improvisation method or eliminates the root causes for defects. Solution for this Provider should get some standard certificate from some governing or standardized institution that ensures users that provider has established adequate internal control and these control are operating efficiently.
- Although it is discussed on how to go about this analysis, the steps are not clearly stated and the work is too much detailed implying that incase one is interested in the procedure only, he has then to go through all the writing to really identify and extract the steps.

IV. CONCLUSION & FUTURE SCOPE

Cloud Computing can be considered as the future of IT industries, it will help the industries in getting efficient use of their hardware and Software at very cheaper cost. If the fluctuations for your time series data are roughly constant over time you may need to use an additive model. An additive model is not appropriate for describing a time series, if the size of the seasonal fluctuations and random fluctuations seem to increase with the level of the time series. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security issues and research challenges in cloud computing.

This made the scientists to think about a substitute to the Portland cement. The future of cloud computing is really appealing, giving the vision of cheap communications. Here we investigate the lag after which the autocorrelogram or the partial correlogram becomes zero or tends to zero (this gives us the values of q and p respectively). Large scale cloud computing is another challenging issue in the near future which can be already foreseen.

REFERENCES

[1] A. Kundu, C. D. Banerjee, P. Saha, "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 9, Issue 5, November 2019

[2] Lizhe Wang, Jie Tao, Kunze M., Castellanos A.C., Kramer D., Karl W., "Scientific Cloud Computing: Early Definition and Experience," 10th IEEE Int. Conference on High Performance Computing and Communications, pp. 825-830, Dalian, China, Sep. 2008, ISBN: 978-0-7695-3352-0

[3] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202

[4] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009

[5] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing," Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009

[6] G. Mckay, H.S. Blair, J.R. Gardener, Adsorption of dyes on chitin I. Equilibrium studies, J. Appl. Polym. Sci. 27 (1982) 3043–3057.

[7] T.W. Weber, R.K. Chakraborty, Pore and solid diffusion models for fixed bed adsorbents, J. Am. Inst. Chem. Eng. 20 (1974) 228–238.

[8] A. EL-Kamash, A. A. Kaki and M. EL-Geleel, Modeling batch kinetics and thermodynamics of zinc and cadmium ions removal from waste solutions using synthetic zeolite A, J. Hazard. Mater. B127 (2005) 211-220.

[9] Y.S. Ho, Citation review of Lagergren kinetic rate equation on adsorption reaction, Scientometrics 59 (2004) 171–177.

[10] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing"; Journal of Network and Computer Applications, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, 2011, ISSN: 1084-8045

[11] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran "Research Issues in Cloud Computing " Global Journal of Computer Science

[12] Robert H. Shumway, David S. Stoffer, "Time Series Analysis and Its Applications", EZ-Third edition, version: 20140526170200, 2003.

[13] Akaike,H."Fitting autoregressive models for prediction", Ann. Inst. Stat.Math., 21, 243-247, 1969.