Journal of Advances in Science and Technology
Vol. 14, Issue No. 2, September-2017, ISSN 2230-9659

An Efficient Security Model in Cloud Computing Based on Soft Computing Techniques

A. V. Ramana[1]* Dr. Ashish Chaturvedi[2]

[1] Research Scholar, Kalinga University, Chhattisgarh

[2] Associate Professor, Kalinga University, Chhattisgarh

Abstract – In recent years, Cloud computing is one of the most appealing technological studies region due to its flexibility as well as cost performance. Generally in a cloud the information are transferred some of the purchaser and the server.

Records takes place, protection will become the major problem. Efficient protection device have to be hired in a cloud in order to make the computing environment relaxed from unauthenticated customers. Due to this cause, cloud securities have emerged as the recent dialogue inside the IT sector. Various strategies have been formulated in order to make the cloud computing environment secure. In this paper, we provided an green safety model in cloud computing surroundings with the assist of Soft Computing Techniques. Here, a robust safety in cloud computing is managed with the assist of recognition management system to ensure the information safety. Also maintaining the transaction desk that carries the statistics associated with the preceding transactions just like the previous transaction identification of the cloud node concerned, timestamp, public keys of the cloud involved, agree with evaluation and so on, can be very useful to perceive the relevant cloud nodes suitable of records transmission.

Soft Computing Techniques utilizes fuzzy good judgment, neural network or genetic algorithm for processing. In the proposed technique, we applied genetic algorithm as the computing technique to perceive the appropriate nodes for transmission.

----------♦----------

INTRODUCTION

The vendors have to ensure that they get the safety factors proper, for they are the ones who will shoulder the obligation if matters move incorrect. The cloud gives numerous advantages like speedy deployment, pay-for-use, decrease expenses, scalability, speedy provisioning, speedy elasticity, ubiquitous community get right of entry to, greater resiliency, hypervisor safety against community Regulatory requirements, and provides extra enterprise manage over deployment and use.

Hybrid Cloud: A hybrid cloud is a personal cloud linked to 1 or greater external cloud services, centrally managed, provisioned as a single unit, and circumscribed through a comfy network . It provides virtual IT answers via a mixture of each public and personal clouds. Hybrid Clouds provide greater at ease control of the statistics and packages and allows numerous events to access facts over the Internet

Also, there are five most important technical traits of cloud computing: (i) huge scale computing sources (ii) excessive scalability & elastic (iii)shared resource pool (virtualized and bodily useful resource) (iv) dynamic aid scheduling and (v) well known reason. Specifically, cloud computing affords computing assets as on call for offerings which are hosted remotely, accessed over the Internet, and generally billed on a in keeping with-use foundation.

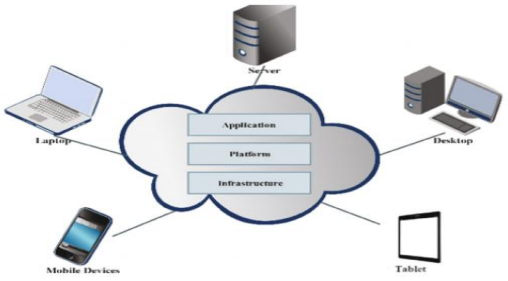
For cloud computing, the facts are stored in "facts center", the safety and confidentiality of person statistics is even more crucial. The so-called integrity of statistics in any country isn't always challenge to the need to assure unauthorized deletion, change or harm. The availability of data way that customers may have the expectancies of the use of data via using capability. To make sure statistics confidentiality, integrity, and availability (CIA), the storage company should offer talents.

i. Tested encryption schema to make sure that the shared storage environment safeguards all records.

ii. Stringent get entry to controls to save you unauthorized get entry to to the data.

iii. Scheduled statistics backup and secure garage of the backup media. Data protection

includes encrypting the facts in addition to making sure that suitable rules are enforced for records sharing. In cloud computing, security applies to two layers inside the software stack. First, customers' workloads should be run isolated from each other, so that one (malicious) consumer can not affect or secret agent on any other user's workload. Second, every person is also involved with the safety of their very own workload, in particular if it is exposed to the Internet (as in the case of an internet carrier or Internet application.



Cloud Basic Articheture

CHARACTERISTICS:

National Institute of Standards and Technology (NIST) put the following set of characteristics which should hold by any cloud definition. These characteristics help in shifting the business to the cloud .

A. **On-demand self-service:** client can calculate the computation efforts needed from the cloud.

B. **Broad network access:** services should be available over the internet to access by the client by using smart phones, laptops etc.

C. **Resource pooling:** All the required computing resources should be pooled or managed in such a way that at a time multiple clients can access them.

D. **Rapid elasticity:** Computation resources can be increased or decreased by the client on the basis of demand.

E. **Measured services:** The computational services going to be used by the client should be measurable to make them charge pay-per-use basis.

Public cloud infrastructure is a top mission for cyber security leaders and a chief supply of Cyber Exposure. Just gaining visibility into cloud property is tough enough, not to mention constantly scanning them for vulnerabilities and misconfigurations as they spin up and down. You want a complete picture of your cyber hazard, not siloed visibility due to using separate tools for one of a kind property.

Cloud is one of the maximum technological research region because of its flexibility and cost efficiency and transformation of statistics among patron and server. this paper elaborates to make certain the sturdy facts protection is controlled with the assist of popularity control gadget additionally preserve the transaction table that contains the records. In cloud, virtualization is critical for cloud computing however the protection for virtualization isn't always effectively studied.

CLOUD COMPUTING ISSUES AND CHALLENGES:

Researchers identify many issues and challenges which are required to be address properly as follows:

A. **Security:** According to the International Data Corporation (IDC) survey, Security, Availability and Performance are three major issues in adoption of cloud technology. System is more prone to security threats like data loss, phishing etc. because of movement of data, data storage and processing of data outside the control of organization. Security threats can be categorized into two categories – internal and external. Cloud computing also poses privacy concern due to deliberate or accidental access of data which may lead to breach of trust. So novel techniques must be used to reduce the impact of such threats.

B. **Performance:** According to IDC's Survey, Performance is the second major issue in adoption of Cloud Computing Technology. Performance is generally measured in terms of capabilities of application running on the cloud. Poor performance may be caused due to lack of resources like limited bandwidth, less disk space, lower CPU speed and network connections etc. . Low performance may result in low revenue, termination of deal or end of service etc. .

C. **Reliability and Availability:** Reliability and Availability are two major factors for the success of any technology. Reliability gave us idea of availability of the required resources without any failure. Availability can be defined as the time needed by the system to provide the required resources on their demands.

D. **Energy Consumption:** As per Amazon survey, 53% of total cost is consumed by servers for a 3 years of amortization period while 42% of total budget spent on energy and cooling requirement.

ENHANCE HYBRID CLOUD SECURITY USING VULNERABILITY MANAGEMENT:

Cloud computing is one of the emerging technologies in last decade; this technology provides a service model to organizations and public users. Organization users and developers, they start and maintain their organization without any hardware and software infrastructure they can develop their company with the help of cloud technology. Cloud deployment is categorized into three types, private, public and hybrid cloud environment and here public and private cloud more secure comparatively hybrid cloud because when data is moving from private to public cloud security problem is occur. Data communication is most important task in a network environment so the proposed model is focus on data security in hybrid cloud environment. In a hybrid cloud the participation of private cloud and its nodes very important after that the data transmission is depends on active node, In this node selection is based on genetic algorithm. The result of proposed model is going to compare with private and public cloud security parameters.

RELATED WORK

The proposed model is focus on hybrid cloud security so the literature survey is done on private and public cloud security.

PUBLIC CLOUD SECURITY:

Public cloud model offer a provider thru an internet to customers, as it's miles the standard cloud techniques. Any type of customers within the international can use public cloud based on their call for and they need to maintain their in widespread cloud services like Amazon Web Service, Google Cloud. In public cloud protection and useful resource allocation are taken into consideration to be the main problems. In public cloud they use the encryption thru secure sockets layer (SSL) for safety purpose and the encryptions executed best whilst information is transmitting from one to other. It doesn't work while the facts is in relaxation (stored) . To guard the records in rest we use some encryption tolls inclusive of True crypt and Bit Locker for home windows after that for Linux and Unix they may be equipped with encryption functionality for storage also.

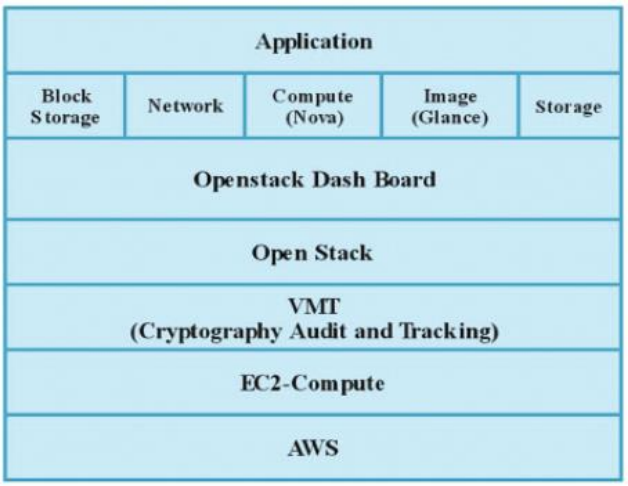
PRIVATE CLOUD SECURITY:

Private cloud affords a manner of storing and retaining big facts, compute and networks in separate clouds for small company and it providing privacy. Private clouds are specially preferred for privateer's motive and it have better control over the facts, consumer assets and the information assets.

Related paintings attention at the heritage of the public and private clouds. In private and public cloud coping with the safety and privateers of the touchy details difficult because if the organization forgets the code space then the entire information can be hacked. Every data inside the cloud is inclined because the hackers or attackers need no longer have any talent to take others data .The proposed version suggests how to manipulate the susceptible facts and its security and privacy features.

PROPOSED HYBRID CLOUD SECURE ARCHITECTURE:

The proposed architecture shown to define sequence of steps to be performed. The first step is to login to the AWS public cloud and release a new instance inside the EC-2 issue. Once the instance is launched, join the configured security issue (VMT) on the top the EC-2 aspect. Then install the Open-stack on the AWS cloud and after set up, open the dashboard to access the Open stack components like Block garage, Neutron, Nova, Glance and Swift components. Use those components for the applications.



Hybrid cloud security architecture

AMAZON WEB SERVICES (AWS):

AWS is one of the public cloud programs that can be accessed by any user who are having account and AWS offers security not most effective in all its layers but also on each services it renders to the developers. It works efficiently and provides safety to all its users. It offers a big quantity of offerings, providing the developers to use it to scale up and down in step with their use. AmazonEC2 is an important key element in dealing with Amazons IAAS services. It helps in coping with security and enhancing scalability. The EC2 components pro-vides more than one layer safety on the host working gadget, digital or the guest operating gadget, firewalls in the device and the APIs. AWS uses a highly customized xen hypervisor to carry out para virtualization because the paravir-tualized software depends upon the xen hypervisor to control operations based on the get entry to privileged modes

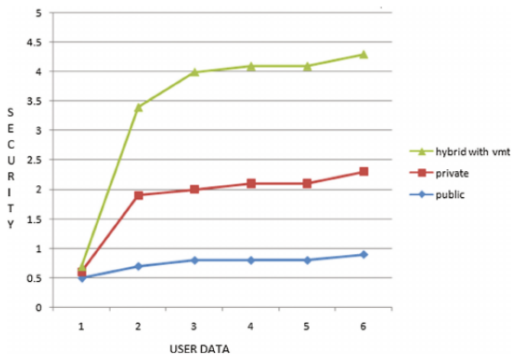
The AWS is configure with VMT and it can manage and manipulate the facts protection.

NETWORK:

Open Stack Neutron is a Software-Defined Networking and a networking con-troller within the cloud which affords Networking-as-a-Service. A neutron, also called as quantum, is a hard and fast of APIs and software program modules that offers inter-operability within IAAS carrier. In open stack, the API set of neutron has been changed. A neutron is used to expose the shortage of tenant manage over the topologies in a multi tenant environment. A neutron is a person service with Nova,Glance, Keystone, Horizon. The assigning of a neutron includes the following processes The authorization and authentication of a neutron depends at the keystone. The neutron and the Nova combines together with the API calls The Horizon allows its tenants to create subnets and networks. It permits the instances to connect with tenants internet-paintings.

IMPLEMENTATION AND RESULT:

The proposed paintings Hybrid Cloud security is applied in windows 7 environment, sixteen GB Ram, 1 TB difficult disk. AWS account become created and configured the account with AWS. Then launch the EC2 instance for ubuntu 14.04. After launch the ubuntu pinnacle on the ubuntu constructed the open stack and configures the opens tack component like Horizon, Neutron, Cinder, Nova, Glance, Swift and cello motor. After configure the open stack surroundings hook up with VMT and then join the open-stack to AWS through VMT. Result for this proposed version in comparison with existing private and public cloud.



Hybrid cloud security performance evaluation with private and public cloud

REVIEW OF LITERATURE:

The comprehensive look at and analysis after the literature evaluation shows various strategies, frameworks and algorithms which can be proposed by way of various researchers over a period of time. The graphs and the table in the paper suggest exceptional methods and their sub-methods proposed with the aid of researchers and on which QoS parameters. Different paintings proposed inside the area of cloud is mentioned in info and the position of QoS parameters enables in finding out the applicable offerings. The have a look at of current literature executed in research in shape of proposed paintings of numerous authors is accomplished and mentioned on various parameters. The boundaries within the present literature lay a basis for ability studies instructions. Authors can also explore multi- goal optimization trouble and techniques for choosing services while considering a couple of criteria at time of service selection wherein traditional processes are not taken into consideration as gifted approach for service choice

Background of the cloud service provides.

- Trust management in cloud.
- Each and every action and notification monitoring.
- User and admin log monitors.

Background of the cloud service provides.

- Trust management in cloud.
- Each and every action and notification monitoring.
- User and admin log monitors.
- Background of the cloud service provides.
- Trust management in cloud.
- Each and every action and notification monitoring.
- User and admin log monitors
- Background of the cloud service provides.
- Trust management in cloud.
- Each and every action and notification monitoring.
- User and admin log monitors.
- Background of the cloud service provides.
- Trust management in cloud.
- Each and every action and notification monitoring.

- User and admin log monitors.

CONCLUSION:

The proposed at ease hybrid cloud environment became built the usage of VMT tech-nique and the hybrid cloud is evolved in Amazon public cloud, within AWSEC2 the personal cloud setup Open Stack applied. Compute, storage and infrastructure are actively operating inside the invented model. The version is com-pared with private and public cloud security parameter and finally the proposed work is extra efficient then the present version. Here the safety parameter like data classification, authentication code and cryptographic method are evaluated with different paintings-masses in a proposed hybrid cloud model. The developed hybrid cloud version satisfies all of the parameter in actual time method and it works efficiently

REFERENCES:

1. Cho S.B. (2017). Incorporating soft computing techniques into a probabilistic intrusion detection system. IEEE Trans Syst Man Cybern C Appl Rev .

2. Gupta B.B., Agrawal D.P., Yamaguchi S. (2016). Handbook of research on modern cryptographic solutions for computer and cyber security. IGI Global Publisher, Hershey.

3. Gupta S. et. al. (2017a). Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges. Int J Cloud Appl Comput (IJCAC).

4. Gupta B.B., Gupta S., Chaudhary P. (2017b). Enhancing the browser-side context-aware sanitization of suspicious HTML5 code for halting the DOM-based XSS vulnerabilities in cloud. Int J Cloud Appl Compute (IJCAC)

5. Gupta B.B., Yamaguchi S., Agrawal D.P. (2016). Advances in security and privacy of multimedia big data in mobile and cloud computing. Multimed Tools Appl.

6. Hossain MS et. al. (2016). Cloud-assisted secure video transmission and sharing framework for smart cities. Future Gener Comput Syst .

7. Jain A.K. & Gupta B.B. (2016). A novel approach to protect against phishing attacks at client side using auto-updated white-list. EURASIP J Inf Secur 2016.

8. Lee K. et. al. (2017). A comparative evaluation of atrial fibrillation detection methods in Koreans based on optical recordings using a smartphone. IEEE Access.

9. Negi P., Mishra A. et. al. (2017). Enhanced CBF packet filtering method to detect DDoS attack in cloud computing environment. Int J Comput Sci Issues (IJCSI) .

10. Plageras A.P., Psannis K.E. et. al. (2016). Efficient IoT-based sensor BIG Data collection-processing and analysis in smart buildings. Future Gener Comput Syst .

11. Psannis K., Stergiou C., Gupta B.B. (2016). Advanced media-based smart big data on intelligent cloud systems. IEEE Trans Sustain Comput.

12. Stergiou C. et. al. (2016) Secure integration of IoT and cloud computing. Future Gener Comput Syst.

13. Wang Y., Liu Q., Hou H.D. et. al. (2016). Big data driven outlier detection for soybean straw near infrared spectroscopy. J. Comput Sci.

14. Zhang Z et. al. (2016). Social media security and trustworthiness: Overview and new direction. Future Generation Computer Systems. Elsevier, Amsterdam.

Corresponding Author

A. V. Ramana*

Research Scholar, Kalinga University, Chhattisgarh