ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Cloud Computing: A Study over Challenges, Threats and Security Models.

***Muhammed Sadique UK[1] and Divya James[2].**

1. Department of Information Technology,Rajagiri School of Engineering and Technology, Cochin, India
2. Department of Information Technology, Rajagiri School of Engineering and Technology, Cochin, India

Manuscript Info

Key words:
Cloud Computing, Data Security, Confidentiality, Classification, Security Models, Side channel Attack.

Abstract

Cloud computing is an internet-based computing technology, where shared resources such as platform, software, storage and information are provided to customers on demand. Cloud computing is widely used due to its readily available service at low cost. It is a computing platform for sharing resources that include infrastructures, applications, software, and business processes. When the number of cloud users increases this may subsequently lead to data security and privacy threats. Integrity, Availability, Authenticity and Privacy are essential concerns for both Cloud providers and consumers as well. Data confidentiality and efficient data retrieval are major issue which block users to adopt cloud computing. This paper provides relative analysis over the challenges, threats and different security enhancement models. The security enhancement models can enhance the security features of cloud computing. It also provides a scope for research on one of the big threat which can challenge the cloud computing features and ensures future work to overcome this threat to make the cloud computing platform safer.

Introduction:-

Cloud computing is a new paradigm shift with service models in distributed computing and has acquired greater attention in the research communities [13]. According to the National Institute of Science and Technology (NIST), cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications and other services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [14]. It has also been reported by the European Network and Information Security Agency (ENISA) that, cloud computing provides on-demand services to users based on the distributed and virtualization technologies [15]. The infrastructure, services and resource management of cloud computing aremore efficient and powerful than an organization's personal services. Cloud computing increases the income of an organization by reducing software and hardware purchasing, management, implementation and maintenance cost [15].

Current cloud computing systems pose serious limitation to protecting users data confidentiality. Since users sensitive data is presented in unencrypted forms to remote machines owned and operated by third party service providers, the risks of unauthorized disclosure of the user’s sensitive data by service providers may be quite high. There are many techniques for protecting users data from outside attackers. Many approach are presented to protecting the confidentiality of users data from service providers, and ensures service providers cannot collect users confidential data while the data is processed and stored in cloud computing systems. Cloud computing systems provide various Internets based data storage and services. Due to its many major benefits, including cost effectiveness and high scalability and flexibility, cloud computing is gaining significant momentum recently as a new paradigm of distributed computing for various applications, especially for business applications. Along with the rapid growth of the internet. With the rise of the era of cloud computing, concerns about Internet Security continue to increase. This paper provides relative analysis over the challenges, threats and different security enhancement models. The security enhancement models can enhance the security features of cloud computing. Also we discuss scope of side channel attack and the future work to overcome this threat to make the cloud computing platform safer.

A. Cloud computing architecture:-

The two most significant components of cloud computing architecture are known as the front end and the back end. The front end is the part seen by the client, i.e. the customer. This includes the clients network or computer, and the applications used to access the cloud via a user interface such as a web browser. The back end of the cloud computing architecture is the cloud itself, which comprises of various computers, servers and data storage devices. The three key cloud delivery models are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Infrastructure-as-a-Service (IaaS) is offered in the bottom layer, whereresources are aggregated and managed physically. The middle layer delivers Platform-as-a-Service (PaaS), in which services are provided as an environment for programming. Software-as-a Service (SaaS) locates in the top layer, in which a cloud provider further confines client flexibility by merely offering software applications as a service. Cloud deployment models include public, private, community, and hybrid clouds. Public clouds are external or publicly available cloud environments that are accessible to multiple tenants, whereas private clouds are typically tailored environments with dedicated virtualized resources for particular organizations. Similarly, community clouds are tailored for particular groups of customers.

B. Cloud computing Model:-

Cloud computing can be divided into four different models:public, hybrid, private and community. Public Cloud is ownedby cloud service provider and offers highest level ofefficiency. Private Cloud is only for one organization on aprivate network and is highly secured. Hybrid Cloud iscombination of public and private model. Community Cloudis for group of organization with agreement.

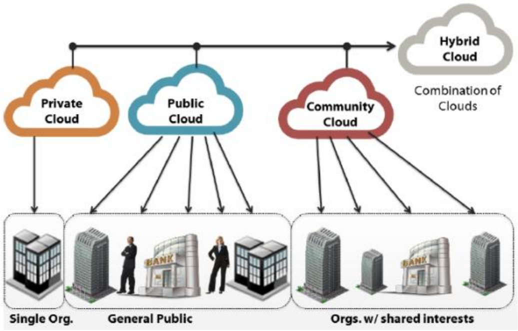

Figure 1: Cloud Computing Model

C. Cloud computing Services:-

Software-as-a-Service(SaaS): The cloud providers install and run a number of software’s on cloud servers and allow the users to access the software’s available in the cloud database through different web browsers. The software’s are virtualized on the cloud server and can be accessible from anywhere and at any time.

Infrastructure-as-a-Service(IaaS): the IaaS provides hardware services to users for virtualization, file systems, network resources and data storage for rent. Users do not need to purchase the infrastructure, i.e., servers, hardware, software and other supporting tools to fulfil their organizational requirements. By this means, the purchasing cost of the infrastructure can be saved by the organization. The IaaS model assists in providing three main services such as Hardware as a Service, Storage as a Service and Database as a Service.

Platform-as-a-Service (PaaS): The PaaS is also a service model that provides a software development environment, in which the users are able to develop and deploy their own applications on the cloud servers using Application Programming Interface (API) frameworks. Using these facilities, users have full control of their deployed applications in the cloud. The best example of PaaS providers is the Google App Engine which is used to develop software and provides different APIs for software development.

D. Need for Security in Cloud:-

Data security: It focuses on protecting the software and hardware associated with the cloud. It deals with choosing an apt location for data centres so as to protect it from internal threats, different types of weather conditions, fire and even physical attacks that might destroy the centre physically and external threats avoiding unauthorized access and break ins.

Network security: Protecting the network over which cloud is running from various attacks DOS, DDOS, IP Spoofing, ARP Spoofing and any novel attacks that intruders may device. Attack on data affects a single user whereas a successful attack on Network has the potential to affect multiple users. Therefore network security is of foremost importance.

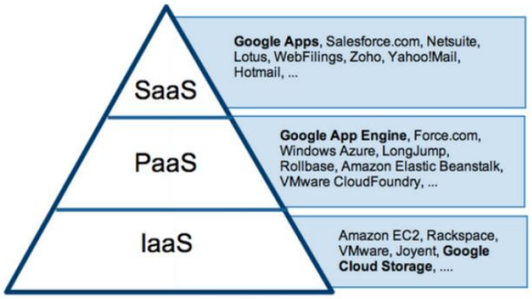
SaaS
Google Apps, Salesforce.com, Netsuite, Lotus, WebFilings, Zoho, Yahoo!Mail, Hotmail, ...
PaaS
Google App Engine, Force.com, Windows Azure, LongJump, Rollbase, Amazon Elastic Beanstalk, VMware CloudFoundry, ...
IaaS
Amazon EC2, Rackspace, VMware, Joyent, Google Cloud Storage, ...

Figure 2: Cloud Computing Service

Cloud Confidentiality: Confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorized persons, processes, or Devices. ie, customers data and computation tasks are to be kept confidential from both the cloud provider and other customers.

Cloud Integrity: the notion of integrity in cloud computing concerns both data integrity and computation integrity. Data integrity implies that data should be honestly stored on cloud servers, and any violations are to be detected. Computation integrity implies the notion that programs are executed without being distorted by malware, cloud providers, or other malicious users, and that any incorrect computing will be detected.

Cloud Availability: Availability is crucial since the core function of cloud computing is to provide on- demand service of different levels.

Cloud Accountability: Accountability implies that the capability of identifying a party, with undeniable evidence, is responsible for specific events.

Related Works:-

Different techniques and models are developed for data security and privacy in cloud. A lot of research has been conducted in different areas of this field but the most focused area in research is data security.

B.Hayes [7] proposed a new idea of using a third party for security, to keep an eye on the agreement signed between a cloud vendor and a user. If it finds something against the agreement it would inform the cloud vendor and the user. In the next study [3], conducted by Yildiz; he proposed a layered security approach for cloud computing. The different layers of the network focused in this model for data security. In the same year [8], the concepts of implicit and shared key techniques were proposed. In the implicit technique, the data is partitioned into different chunks and stored in different cloud servers. The shared data can only be reconstructed when all partitions are combined together. Where as in the shared key technique, data is encrypted by using an encryption technique and the encrypted data is stored in a single cloud server. However, it is difficult to remember the key. So, the key must be secured and divided into different parts and stored in different servers.

The benefits of cloud services for end users were discussed and it also pointed out eight cloud risks, which are very necessary to be fixed [9]. Another solution given for security issues is the crypto co-processor [6]. Crypto co-processor provides security-as-a-service on demand and is controlled by a third party. The crypto co-processor allows the users to select the encryption technique to encrypt the data and divide data into different fixed chunks. In such a way a hacker does not know the start and end of data. In the same year, a new concept of inner-cloud was published by IBM to solve the security issues of a single cloud. This study also proposed an inner-cloud model known as the Inner-cloud Storage [10]. In this model, Hash function and digital signature are hybridized to provide data authentication and integrity in a cloud. Where the security key is divided and shared in multiple clouds.

The single cloud does not provide as much security as the customer may need. Some issues in a single cloud are also traced out by AlyssonBessani and M. Correia [5]. Authentication, data security and availability are main concerns in single cloud computing. The DepSky model divides a cloud into multi-clouds to overcome the single cloud issues and implements Byzantine and Secret Sharing Cryptography in model by using Depsky-A and Depsky-CA algorithms. The key is divided and shared with the distributed data in multi-clouds [5]. Although this approach is more secure as compared to others but it does not provide the IaaS model, only a storage service model [2]. In the same year, M.A. Alzain and Ben Soh considered the IaaS model issue of the DepSky study and suggested a Multi-cloud Database Model (MCDB) developed [2].

The model divides the data into a number of chunks and stores them in different clouds. DBMS is able to manage data and all the information about the shares. Shamir's secret sharing is used for the data distribution. However, it is not without drawbacks; the most common limitation of Shamir's Secret Sharing Scheme is that at the time of recovery of a few chunks of data, all the secret shares are combined including those which are not needed [11]. Hu and Qui conducted a review study on design challenges in cloud architectures and security threats.Security can also be enhanced by adding false data into original data and then dividing the data into different chunks and sending the chunks of data in different clouds [12]. In the same year, a survey was conducted on security issues in cloud computing delivery models. Although there are many advantages in cloud computing, but there are also many security threats in cloud computing such as data security, services availability, integrity, authentication, privacy and service level agreements. To overcome these threats, an integrated security framework is required for data security in cloud computing [9]. The contracted trust agreement binds the cloud vendors and customers on the basis of trust. Therefore, they trust each other. The agreement fixes the critical data handling, multiple stakeholders issue and open space security issue [4]. However, a few studies have suggested that only agreement trust is not enough for a cloud environment which contains a huge amount of data from different organizations. In the same year, another study was conducted on the same topic. This study provided a proactive model for security, based on the policy. The policy is signed by a cloud and a customer and the policy is managed by a private cloud, which continuously gives feedback about the policy [7]. HMCDS Model, Hybrid Multi-Cloud Data Security Model, the HMCDS model improves efficiency of data retrieval, data confidentiality and availability. It provides two levels of data confidentiality,ie, high level and low level. HMCDS model is divided into 3 layers: Layer 1- Cloud user, Layer 2- Data management, Layer 3- Database layer [1].

Data Confidentiality in HMCDS Model - User data classified in to different classes and each class is stored in different clouds of different clusters. Data Retrieval Efficiency in HMCDS Model- In this approach the user is able to access complete data as well as the required part of data. Most Sensitive Data- Here data is encrypted using any encryption algorithm and encrypted data is further divided in different chunk and each is stored in to different clusters. Sensitive Data- Here encrypted data is divided into different number of chunks and is stored in a single cloud clusters. Non Sensitive Data- Here data is stored directly in a cloud without encryption. The data of the user can be divided on the basis ofthe following equation:

$$\mathrm{P} = \sum_{i=1}^{n} \mathrm{Pi}$$

Where P is a complete data set and Pi represents the parts of the data set where i = 1, 2, 3. Where P Complete data set.n Total number of encrypted data parts. i Summation variable.

Proposed System:-

In cloud computing resources are shared between different clients. If an attacking program can carefully monitor those resources behaviour, it can theoretically determine what another program is doing with them, this can be termed as Side Channel attack. Side-channel attacks have played a major role in the history of cryptography. Usually, these attacks occur when a machine leaks details of its internal operation through some unexpected vector for example, computation time or electromagnetic emissions. The cloud environment offers a bonanza of potential side channels because different VMs share physical resources for example, processor, instruction cache, or disk on a single computer. If an attacking program can carefully monitor those resources behaviour, it can theoretically determine what another program is doing with them. This threat has long been discussed by cloud security experts but has largely been dismissed by providers. This is because in this area, turning theory into practice turns out to be surprisingly difficult. There are many reasons for this. For one thing, cloud providers often run many different VMs on the same server, which tends to add noise and foil an attacker’s careful measurements.

The Virtual Machine Manager (VMM) software itself adds more noise, and places a barrier between the attacking user and the bare metal of the server. Moreover, individual VMs are routinely swapped between different cores of a multicore server, which makes it difficult to know what you are actually measuring. The Attacker arranges to place their malicious VM on the same physical machine. After successful placement of the malicious VM to the targeted VM extract the confidential information, file and documents on the targeted VM.VMs running in same server, they share processor, instruction cache and disk on a single computer. Also there is no lot of Virtual Firewall, and which are exist that support today are very limited too.

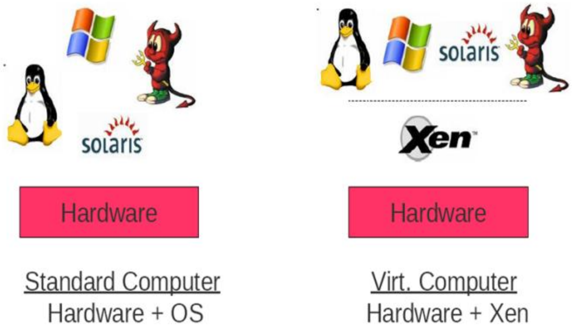

Figure 3: Layers of Standard and Virtual Computer

Conclusion and Future Work:-

Cloud computing is one of the most exciting paradigm shifts in distributed computing. Cloud computing is being widely used due to its readily available service at low cost. In this paper, conducted a specific literature review on cloud models and also security techniques used in cloud computing. The HMCDS Model, Hybrid Multi-Cloud Data Security Model, provides a high level of confidentiality, availability and efficiency of data retrieval in terms of hybrid multi-cloud and clusters. This security enhancement model can enhance the security features of cloud computing.The future plan is to identify Side channel attack between VMs. As side-channel is a mode of bypassing virtual machine for gaining information from the physical implementation rather than brute force or theoretical weaknesses in the algorithm, it can be implemented practically through installing Xen Hypervisor. Later analyse whether this attack happens. If it is happening, suggest best methods to eliminate it.

References:-

1. **Zardari, M.A.; Low Tang Jung; Zakaria, M.N.B. (2013).** Hybrid Multi-cloud Data Security (HMCDS) Modeland Data Classification, Advanced Computer Science Applications and Technologies (ACSAT), International Conference on , vol., no., pp.166,171.
2. **M. A. Alzain. B. Soh and E. Pardede. (2011)** MCDB: Using Multi-cloud to Ensure Security in Cloud Computing. IEEE Ninth International Conference on Dependable. Autonomic and Secure Computing. pp. 784-791.
3. **G. Wang. Q. Liu. J. Wu. and M. Guo. (2011)** "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers" Computers Security. vol. 30.no. 5. pp. 320-331.
4. **H. Sato. A. Kanai. and S. Tanimoto. (2010)**A Cloud Trust Model in a Security Aware Cloud. 10th IEEE/IPSJ International Symposium on Applications and the Internet.pp.121-124.
5. **M. Correia and F. Andr. (2010)**DEPSKY : Dependable and Secure Storage in a Cloud-of-Clouds. 6th ACM SIGOPS/EuroSys European Systems Conference.
6. **C. P. Ram and G. Sreenivaasan. (2010)** Security as a Service (SasS): Securing user data by coprocessor and distributing the data. Trendz in Information Sciences and Computing(TISC2010). pp. 152155.
7. **P. Srivastava et al. (2011)** "An architecture based on proactive model for security in cloud computing. IEEE International Conference on Recent Trends in Information Technology. pp. 661-666.
8. **Parakh and S. Kak. (2009)**Online data storage using implicit security. Information Sciences.Vol. 179.no. 19. pp. 3323-3331.
9. **Catteddu and G. Hogben. (2012)** Cloud Computing: Benefits. risks and recommendations for information Security. ENISA report.
10. **Cachin and R. Haas.(2010)** Dependable Storage in the Intercloud. IBM Research Report RZ 3783.

11. **S.-sharing Schemes. R. Steinfeld. J. Pieprzyk. and H. Wang.(2004)** Lattice-Based Threshold-Changeability for Standard Shamir, Springer Verlag Berlin Heidelberg. pp. 1-28.
12. **D. Wang. (2011)**An Efficient Cloud Storage Model for Heterogeneous Cloud Infrastructures. Procedia Engineering. vol. 23. pp. 510-515.
13. **P. Jain. D. Rane and S. Patidar. (2011)**A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment, pp. 456-461.
14. **M. A. AlZain. E. Pardede. B. Soh and J. a. Thom. (2012)** Cloud Computing Security: From Single to Multi-Cloud, 45th Hawaii International Conference on System Sciences. pp. 5490-5499.
15. **D. Catteddu and G. Hogben. (2012)** Cloud Computing: Benefits. risks and recommendations for information Security. ENISA report.