A Comprehensive Research on Cloud Data Security

Dr. S.K.Jha, Dr.R.K.Singh, Prof. S.K.Ojha

[1] **Associate Professor, Dept Computer Science , Sityog institute of Technology , Aurangabad**
[2]. **Director , Sityog institute of Technology , Aurangabad**
[3]. **Assit. Professor , Dept Computer Science , Sityog institute of Technology , Aurangabad**

Abstract:

Today, cloud computing is an evolved technology in computing in computer science where a set of resources and services are offered by the network or internet allowing on-demand, scalable, autonomous and economical massive scale services shared among multiple users. Cloud facilitates its users by providing virtual resources via Internet. For IT professionals cloud computing is a new kind of business consists of new technology platform for developing and deploying applications and on the other hand end user finds it as a cheaper method to use applications. As the field of cloud computing is spreading the new techniques are developing. This increase in cloud computing environment also increases security challenges for cloud developers. Users of cloud save their data in the cloud hence the lack of security in cloud can lose the user's trust. Cloud security is one of the main concerns on interested parties' minds. While evaluating the security challenges in cloud computing, each concern has a variety of repercussions on specific assets. Despite numerous researches, we are still unable to specify the security requirements, Previous researches have formulated a lot of security solutions that service providers with various assessment methods can utilize. Consequently, there is a growing demand for a critical evaluation of earlier research on Cloud Security Ontology. This paper presents the latest noble approach for a secure cloud introducing IPSec Management providing data access security to thwart congestion attack and man-in-the-middle attack.

Keywords : Cloud Computing , Cloud Security, Security Threats, Security Techniques, Cloud Security Standards.

1. Introduction :

Cloud computing is another name for Internet computing. The definition of cloud computing provided by National Institute of Standards and Technology (NIST) says that: "Cloud computing is a model for enabling on-demand and convenient network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction[9]. Cloud Computing is the availability of any computer service on demand by paying for it such as online applications, remote computing resources, storage, databases etc. via Internet or network.

Cloud computing is a technology that increase or reduce the storage capacity as peruse without investment in new infrastructure. The process of cloud storage contains four layers newly storage layer that store data on cloud data centre, management layer which ensures privacy and security of cloud storage, application interface layer that provide cloud application service platform, and finally cloud access layer which provide accessibility to the cloud user.[2] In Cloud technology, application developers can get an interface or platform where they can get immediate and readymade infrastructure. As a term, cloud infrastructure can be used to describe a complete cloud computing system—once all the pieces are put together—as well as the individual technologies themselves. The cloud architecture typically includes multiple cloud components communicating each other over a loose coupling method such as a messaging queue. A cloud region is a geographic area or location where a cloud provider's infrastructure is clustered and it is an environment created by the cloud service provider through the world. The cloud regions are separated from one another because in case of failure of one region due to any natural reason or non natural reasons. Each Cloud Region can have multiple available zones which are typically distinct Data Centers with their own power, codling and networking resources. The isolation of zones improves the cloud's overall fault tolerance, decreases latency and avoids creating a single shared point of failure.[1]

The service delivery model of cloud are :

1.1 SaaS (Software as a Service) :

SaaS is known as **" On Demand Software "** . It is a software in which the applications are hosted by a cloud service provider. It offers complete applications to a cloud's end user. So,this is a typically end user applications which delivers on demand over a network on pay-as-per-use basis. The software requires no client installation , just a browser and network connectivity[10]. It is mostly accessed through a web portal and Service Oriented Architecture based on web technologies. SaaS platforms make it easier to construct applications by giving users access to development tools,abstraction layers, and software components that are ready to use.

1.2 PaaS (Platform as a Service) :

PaaS cloud computing platform is created for the programmer to develop, test, run, and manage the applications. PaaS is a cloud service where the customer gets asset of applications and product development tool hosted on the provider's infrastructure[11]. It is a platform that can be accessed through the internet provides developers with a framework and tools to build apps and software that are tailored to the organization's individual needs. Platform as a Service concentrates on giving developers access to Language Runtime and Services while leaving the provisioning and management of Infrastructure to the underlying Layer .

1.3 IaaS (Infrastructure as a Service) :

Infrastructure as as Service (IaaS) is a way of delivering cloud computing infrastructure-server, storage, network and operating system as an on-demand service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully out sourced service on demand. It is a computing infrastructure managed over the Internet in which a customer pay for the resources utilized such as storage, bandwidth, memory, load balancer etc. kept and managed by the provider. Eucalyptus [12], Nimbus/Cumulus [13], Open Nebula [14] and Open Stack [15] are the main rivals in the open source IaaS cloud branch. The user can deploy and run any computing resources where the consumer, including applications and operating systems,using these resources [16].

2. Cloud Storage :

Cloud storage is a data deposit model in which digital data information such as documents, Cloud storage includes at least one data server to which a user can connect via the internet. The user sends files to the data server, which forwards the message to multiple servers, manually or in an automated manner, over the internet. The stored data can then be accessed via a web-based interface. There are many cloud storage providers .Most of the providers provide free space up to certain gigabytes. For example DropBox provide free space up to 2GB, Google Drive, Box, Amazon, Apple Cloud provide free space up to 5GB, Microsoft SkyDrive provide free space up to 7GB . Customers have to pay amount according to their utility and if they cross the free space limit. It generally operates via a web-based API implemented remotely through its interaction with in-house cloud storage infrastructure. Storage virtualization is a grouping of multiple physical storage devices, which appear as a single storage device. This provides various benefits such as storage homogenization across multiple storage devices, reduced downtime, load balancing, and improved performance and speed optimization. Partitioning the hard drive into multiple sections is an example of this kind of virtualization. Cloud storage systems are expected to meet several rigorous requirements for maintaining users' data and information, including high availability, reliability, performance, replication and data consistency; but because of the conflicting nature of these requirements, no one system implements all of them together.

Typically, cloud storage can be sorted into three types: public cloud storage, internal cloud storage and hybrid cloud storage.

- Simple Storage Service from Amazon and storage provided by Nutanix provide a huge amount of file saving with low cost in the category of public cloud storage.
- Dropbox with excellent performance is capable of guaranteeing the independency and privacy for every client's storage.
- Internal cloud storage is similar to private cloud storage, however, the former is located inside the firewall of company.
- Eucalyptus, 3A Cloud, and Lenovo network drive are famous for provider private cloud storage.
- Hybrid cloud storage combines public and private cloud to configure the volume temporarily based on clients' requirements. Certain space acquired from public cloud storage to build private or internal cloud storage can help a company with rapidly increasing load fluctuation or peak time. Even so, hybrid cloud storage brings the complexity over public and private cloud distribution.

3. Security as a Service :

Right after the existing of cloud computing and cloud storage, security as a service arose that is a concept that contains all methods inorder to safeguard, fix, and ensure that data in computer systems is protected from a variety of dangers. Practically, security mechanisms implement security policies via security services provided. Features like non-repudiation, confidentiality, integrity, authentication, and availability are used by computer critical infrastructure to ensure security[35].

- **Confidentiality** is the most common aspect of information security. It signifies that only authorized access can be permitted to avail the sensitive and protected data. Invaders can try to capture the data. To avoid this information must be encrypted. To fight against confidentiality breaches, restricted data should be classified and labeled and implement access control policies, encrypt data, and use multi-factor authentication (MFA) systems. It is also advisable to ensure that all in the organization have the training and knowledge they need to recognize the dangers and avoid them.

- **Integrity** means data is protected from unauthorized changes to ensure that it is reliable and correct. It covers that data should be intact not divided, consistent, accurate and trusted over its entire lifecycle. Data must not be changed in transit and steps must be taken to ensure data cannot be altered by unauthorized people. To protect the integrity of your data, you can use hashing, encryption, digital certificates, or digital signatures. For websites, you can employ trustworthy certificate authorities (CAs) that verify the authenticity of your website so visitors know they are getting the site they intended to visit.

- **Availability** guarantees that systems, applications and data are available to authenticated users when they need. It means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information. In case of sudden technical faults and natural disturbances like power shut down ,data maintenance can be regained by backup. For instance, a source system will not be able to transfer the data successfully to the destination system if the Distributed Denial of Service (DDoS) attack takes place.

- **Authenticity** involves the process of verifying and authenticating the sources as well as destination ifthe identities of sender and receiver are confirmed.
- **Accountability** means that every individual who works with a system should have specific responsibility for information assurance. In this respect theft of user Id and password or to give others are not best practices in terms of accountability.
- **Non-repudiation** means sender and receiver cannot deny that either has not send or received the transmission. Repudiations come in two varieties: source repudiations and destination repudiations. Neither the sender nor the recipient may contest the message's transmission in the first case, and they also cannot contest its delivery in the second.

4. Literature Survey :

Subashini and Kavitha described different security threats on survey that the cloud encounters [19]. It focussed on the security issues concerned with cloud service delivery paradigms. A risk model for the cloud has also been created by Kamongi et al. [22], however it is not connected to any current compliance standards. Popovi et al.[23] noticed the cloud security pitfalls in the standards on the cloud engineering and provider end.

The cloud provider is the administrator / controller of security and privacy regulations according to NIST's cloud technology reference architecture [24 - 26]. But on the other hand, its reference architecture's security compliance model is relevant to all of the roles. For any and all cloud delivery types, the same security policies are utilised to safeguard cloud environments. The application of compliance standards to these security controls. The network, IT infrastructure, and electronic data processing are the main topics of the information technology compliance model [27]. To ensure that all of the IT components function together smoothly, compliance models apply rules and regulations to each one. On the basis of these compliance models, organisations frequently establish security controls

Gordin et al. [28] discussed the possibilities of an open cloud in 2018. In contrast to open clouds, where vendors have maintained security, experts have suggested that private clouds are more concerned with security. This Openstack Pike version's security was examined and explained by the author. Both externally and internally, security is examined. The researcher also examines and discusses containment of hypervisor-based virtual servers in the study. Therefore, a conclusion is deduced from the multi-tenant setting. Lattice computation and distributed computing were the perspectives Jujare [29] used to explore computer technology.

According to the client's fundamentals as well as the pay for use front, this provides enormous IT organisations to the end user here on system. The researcher Kumar focussed on the security of cloud computing in hid research work on security threats utilizing transmission of data from one place to another. Encryption and decryption techniques are the basis of security implementation in cloud computing [30].

Bashir with Haider [31] carried out the detailed literature survey to expose the cloud computing vulnerabilities that are areas of high risk. This literature survey has also taken into account the main security risks posed by suppliers and consumers in relation to cloud hosting by analysing various security mechanisms and solutions. The Cloud Security Alliance developed a Trusted Cloud Initiative Reference Architecture [32]. The design suggested in the literature aims to give a straightforward yet precise cloud infrastructure by outlining the potential roles of the entities inside this cloud computing system as well as their system accessories and operations.

5. Threats For Clod Security Providers :

i). Responsibility Ambiguity : Different user roles, such as cloud service provider, cloud service user, client IT admin, data owner, may be defined and used in a cloud system . Ambiguity of such user roles and responsibilities definition related to data ownership, access control, infrastructure maintenance, etc, may induce business or legal dissention

ii). Protection Inconsistency : Due to the decentralized architecture o a cloud infrastructure, its protection mechanisms are likely to be inconsistency among distributed security modules. For example, an access denied by one IAM module may be granted by another. This threat may be profited by a potential attacker which compromises both the confidentiality and integrity.

iii). Evolutional Risks : One conceptual improvement of cloud computing is to postpone some choices from the design phase to the execution phase. This means, some dependent software components of a system may be selected and implemented when the system executes. However, conventional risk assessment methodology can no longer match such an evolution. A system which is assessed as secure during the design phase may exploit vulnerabilities during its execution due to the newly implemented software components.

iv). Business Discontinuity : The as a service feature of cloud computing allocates resources and delivers them as a service. The whole cloud infrastructure together with its business workflows thus relies on a large set of services, ranging from hardware to application. However, the discontinuity of service delivery, such as black out or delay, may bring out a sev ere impact related to the availability.

v). Supplier Lock-in : The platform of a service provider is built by some software and hardware components by suppliers. Some supplier- dependent modules or workflows are implemented for integration or functionality extension. However, due to the lack of standard APIs, the portability to migrate to another supplier is not obvious. The consequence of provider locked- in could be a lack of freedom regarding how to replace a supplier.

vi). License Risks : Software licenses are usually based on the number of installations, or the numbers of users. Since created virtual machines will be used only a few times, the provider may have to acquire from more licenses than really needed at a given time. The lack of a clouded license management scheme which allows to pay only for used licenses may cause software use conflicts.

vii) Data Breach : A "data breach" or data stealing is when someone gains unauthorized access to sensitive credentials they are not supposed to have. When there has been a data breach, regardless of whether it was accidental, the most often targeted kinds of data are Personal Health Information (PHI), Individually Identifiable Data (IID), Trade Secrets, and Copyright Law. It has an impact on data confidentiality and, eventually, the organisation. Encrypted data makes it impossible for an attacker to use it even if it is stolen.

viii) Traffic Hijacking : One of the major risks that end users encounter while using cloud computing is traffic hijacking. It was identified as the third-most serious threat to cloud security in 2013 by Cloud Security Alliance. Hackers typically steal a user's security credentials in this form of assault and claim illegal access to the user's data. An attacker is then able to view all of a user's activities, along with any private cloud transactions they may have.

ix) Insider Attack : When a corporation hires someone, they will thoroughly investigate that person, especially if that person is an IT professional because the most successful attack that anyone can predict will originate within the business. An Ex- employee or not fully protected employee who seeks to exploit data or services for money or evil intentions is often the insider. It is quite challenging to distinguish between different assaults or privileged insider operations because of the Multitenancy of the cloud computing domain

6. Cloud Security Threats

Following are the most significant cyber security threats for cloud networks that businesses face when migrating data or applications to the cloud.

a). Abuse And Nefarious Use of Cloud Computing:

The hackers gain advantage of shortcomings in the process of authentic registrations of cloud. Further, they are provided with services of SaaS, PaaS, IaaS. It is possible for hackers to make their move with suspectible activities like Phishing and/or spamming. These threats are available in allthe 3 layers.

b). Traffic Eavesdropping :

Traffic listening happens when information being moved to or inside a cloud is inactively captured by a vindictive assistance specialist for ill-conceived data gathering purposes . The point of this assault is to straight forwardly bargain the secrecy of the information and conceivably the classification of the connection between the cloud buyer and cloud supplier. Due to the uninvolved idea of the assault, it can all the more effectively go undetected for broadened timeframes.

c). Net Sniffers :

It is also threat associated with SaaS. Through this type of threat, the hacker gains the access via applications. This enables them in capturing packets which flows within a network and also the data if they are transited through the captured packets unencrypted. If this happens, the data become available to everyone.

d). Session Hijacking :

Over a protected network, it is an attack on the security of a user session. When a website is logged in by a user, a new session starts in that server. The new session comprises of all the data and the information of the user which the server uses so that password won’t be needed every time the user enters a new page. With all the needed knowledge, the hackers can enter a running session and succeeds in gaining access of that session identifier via HTTP. Session identifier is used by the server in order to identify the user for that particular session. This session hijacking is used by the hacker for gaining the control over the session identifier which further enables them in gaining unauthorized control over the user’s information. Cross site scripting, session fixation, session side-jacking and session prediction are the most commonly known session hijacking attacks.

e). Data Breaches : Data breaches occur when unauthorized individuals access cloud systems and interfere with the data stored in them. Whether attackers view, copy or transmit data, an organization’s safety is not guaranteed once such individuals gain access. The primary cause of data breaches is human error. Lack of knowledge or not educating your staff on how to keep data safe and secure can easily expose your business to a hacker. This is why providing sufficient cybersecurity education on data protection to your employees is crucial, as nearly 90% of professionals agree that improved data protection skills can significantly reduce risks and data breaches happening within their respective organizations.

f). Man In The Middle Attack :

MITM attack is another kind of session hijacking in which a sniffer is used by the hackers to hack the communication among the devices through which data collection is done and hacker further transmits the data. An independent connection is established by the hackers with the user’s device and the user is convinced that the connection is direct and private. But in reality, the hackers control the session completely. It is a big threat to the SaaS model.

g). Insider Threats :

Sometimes, the biggest threats to an organization's cybersecurity are internal. Insider threats are usually seen as more hazardous than outsider threats as they can take several months or years to identify. The masterminds are usually individuals with legitimate access to an organization's cloud systems. Whether they happen intentionally or maliciously, insider threats will cause a lot of harm to the cloud system. Therefore, it is essential to detect, investigate and respond to them as fast as possible. The reason why these attacks can go undetected for long periods is that businesses lack the proper systems to identify these attacks and are unprepared to identify and resolve them. In addition, companies have little to no control over underlying cloud infrastructure. Traditional security solutions may not be effective as long as significant power remains with the vendors.

h). **Denial-of-Service Attacks :**

In a denial-of-service attack, a hacker floods a system with more web traffic than it can handle at its peak. This results in operations stalling entirely, with internal users and customers unable to access the system, making resources unavailable for the user virtually..

i) Insecure Interfaces and APIs :

Software user interfaces and APIs are usually responsible for the provision, monitoring and management of cloud services. Cloud service providers are working tirelessly to advance APIs and interfaces, but this growth has also increased security risks associated with them.

Cloud service providers use a specific framework to provide APIs to programmers, which leaves their systems more vulnerable to attackers. As such, organizations risk improper authorizations, previously used passwords and anonymous access.

The best way to solve this is knowing how to properly design the cloud security with a multi-layer approach, which is required to help curb unauthorized access and ensure that the software you create is secure.

j). SQL Ijnjection Attack :

This is a virtual attack made to a computer and it mostly damages the SaaS. This attack damages SaaS the most because of the poor design of application. It also completes the execution of the commands of SQL (unauthorized) through taking benefits of insecure interface. These types are attacks are programmed for accessing unauthorized data which is under protection and not allowed to access publically.

k). Misconfiguration :

Misconfiguration is one of the leading threats businesses face in their cloud-based systems. Most business owners are inexperienced in matters surrounding cloud-based infrastructure, which exposes them to various data breaches that can impact their operations.

7. Threats with Cloud Service Models

1. Software-as-a-service (SaaS) :

The prime security issues of applications of cloud which are faced with SaaS are mentioned below:

i. The applications of cloud do not provide a clear visible picture about what data is within it.

ii. Data theft from a cloud application through malicious actor

iii. The control in respect the accessibility of the sensitive data is incomplete

iv. Inability in reference of monitoring the data in transferring from/to cloud applications.

v. Cloud applications being provisioned outside of IT visibility (e.g., shadow IT)

vi. For managing the issues and development of security of the applications of cloud, the available staffs are not sufficient or skilled.

vii. Inability in reference of preventing

malicious inside misuse of data or data theft.
viii. High tech fire attacks and threats against providers.

2. Infrastructure-as-a-service(IaaS) :
Some of the major threats on IaaS are as follows :

i. Cloud workloads and accounts being created outside of IT visibility (e.g., shadow IT) .
ii. Incomplete control over who can access sensitive data .
iii .Data theft hosted in cloud infrastructure by malicious actor
iv. Lack of staff with the skills to secure cloud infrastructure
v. Lack of visibility into what data is in the cloud
vi. Inability to prevent malicious insider theft or misuse of information
vii Lack of consistent security controls over multicloud and on-premises environments
vii Advanced threats and attacks against cloud infrastructure
ix. Inability to monitor cloud workload systems and applications for vulnerabilities
x. Lateral spread of an attack from one cloud workload to another"

3. Platform-as-a-service (PaaS) :
Some of threats posed on PaaS are as follows :

i. Consistent spanning of control in relation to the security is lacking in the virtualized and traditional server private cloud infrastructure.
ii.Hike in the infrastructure's complexity results in more effort/time of maintenance and implementation.
iii.Skilled staff is available as per the requirement for managing the software defined data centre's security.
iv. Visibility is not complete over the software defined data centre's security.
v. Newly developed advance level attacks and threats.

8. Proposed Cloud Security Model :

Network layer security is a key aspect of the Internet based security mechanism. Originally concentration for security is given on application layer security. However ,new security requirements demand that even the lower level data units should be protected. Security at network layer encompasses the technologies related with IP Packets and Encapsulating Security Payload (ESP) protocol. This proposed security measures that organizations deploy to defend public or private cloud networks from breaches and cyber attacks .

Encapsulating Security Payload (ESP)
Encapsulating Security Payload (ESP) protocol provides confidentiality and integrity of message . ESP is based on symmetric key cryptographic technique used in the IPsec (Internet Protocol Security) suite to provide confidentiality, integrity, and authenticity for data packets in an IP network. ESP can operate in two modes:

Transport Mode: Only the payload (data) is encrypted and authenticated, while the original IP header remains intact. This is typically used for end-to-end communication.

Tunnel Mode: Both the original IP packet and the IP header are encapsulated and encrypted, allowing the creation of a secure tunnel between networks. This is commonly used in VPNs.

Mechanism of operation :
With ESP, both communicating systems use a shared key for encrypting and decrypting the data they exchange. Operation of the ESP to provide authentication can be applied as follows :

1. At the sender's end, the block of data containing the ESP trailer and the entire transport layer segment is encrypted and the plain text of this block is replaced with its corresponding cipher text to form the IP packet. Authentication is appended, if selected. This packet is now ready for transmission.

2.The packet is routed to the destination. The intermediate routers need to a look at the IP header as well as any IP extension header, but not at the cipher text.

3.At the receiver's end the IP header plus any plain text IP extension headers are examined. The remaining portion of the packet is then decrypted to retrieve the original plain text transport layer segment.

Result :

If you decide to use both encryption and authentication, then the responding system first authenticates the packet and then, if the first step succeeds, the system proceeds with decryption. This type of configuration reduces processing overhead, as well as reduces your vulnerability to denial-of-service attacks.

9. Future Scope :

As the massive number of data is generated by the user especially by IoT, data security in cloud is exigent and there is scope for the improvement in cloud computing and its security:

- With the increasing implementation / use of cloud services in the different fields, extended range of security concerns and vulnerabilities have been exposed by the heterogeneity of enterprise environment.
- Non-transparency about the real–time location of data and work load storage makes it difficult
  for the reorganization and reduction in the escalation of security concerns.
- Non-transparency in cloud architecture leads to duplication, inability to recognize different types of attacks on time, lack of control over the data access and also the security necessary for meeting regulatory requirements.
- To achieve cloud security effectively both the data and infrastructure must be safeguarded against all types of attacks like: data breaches, hacking of interfaces, use of insecure APIs etc.

10. Conclusion :

Cloud computing model can scale up services and virtual assets /resources on request. To process clients traditional cluster system, cloud service gives a considerable measure of points of interests. Issue of security benchmarks and similarity must be tended to including strict verification, secure authentication, assigned authorization, key management for encoded information data misfortune assurances and regulatory reporting. There are several ways to stop each type of attack, but none of them are effective enough to stop them in all circumstances. It is quite difficult to create a system that is completely impervious to any of these serious threats. Discussed were a few potential methods that were put up to address issues with communication security, data anonymization, and data kept in cloud storage. As a result, it was identified that different kinds of algorithms can defend the cloud on various levels and for diverse purposes With all of this degree of technological shortcomings, the only factor that may be used to determine whether to employ cloud technology is the advantages to risk ratio. Both the client as well as cloud host ends must have a thorough knowledge of one another therefore for the cloud to be protected from across

11. References :

[1] S. Vaishali and Pandey S. K., "A Comparative Study of Cloud Security Ontologies", Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization, India, 2014.

[2] H. Amit and J Karuna Pande, "A Semantic Approach to Cloud Security and Compliance", IEEE 8th International Conference on Cloud Computing, pp. 1081, 2015

[3] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. Foster, "Virtual Infrastructure Management in Private and Hybrid Clouds", IEEE Internet Computing, vol. 13, no. 5, pp. 14-22, Sep. 2009.

[4] L. Hsin Tse, K. Chia Hung, W. Po Hsuan and L. Yi Hsuan, "Towards a hosted private cloud storage solution for application service provider", Proceedings of 2014 International Conference on Cloud Computing and Internet of Things, 2014.

[5] M Armbrust , A Fox , R Griffith , AD Joseph, RH Katz , A Konwinski, G Lee, DA Patterson, A Rabkin, I Stoica and M Zaharia, "Above the Clouds - A Berkeley View of Cloud.". Technical report UCB/EECS-2009-28, EECS Department, University of Berkeley, California, 2009.

[6] Ling Zheng; Yanxiang Hu; Chaoran Yang, "Design and Research on Private Cloud Computing Architecture

to Support Smart Grid", Third International Conference on Intelligent Human-Machine Systems and Cybernetics, pp. 1, 2011

[7] G.Adam,"The Hybrid Cloud Security Professional", IEEE Cloud Computing, Volume: 3, Issue: 1 pp. 2, 2016

[8] P. Mell and T. Grance, The NIST Definition of Cloud Computing, Nat'l Inst. of Standards and Technology, pp. 3, 2011.

[9] J. Sathyan and K. Shenoy, "Realizing unified service experience with SaaS on SOA", 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE '08), 2008.

[10] L. Gouling "Research on Independent SaaS Platform", 2nd IEEE International Conference on Info rmation Management and Engineering, 2010.

[11] D. Rajdeep, R. A. Reddy and K. Dharmesh, "Virtualization vs Containerization to support PaaS" pp-2, 2014.

[12] http://www.eucalyptus.com, February, 2013.

[13] J. Bresnahan, D. LaBissoniere, T. Freeman and K. Keahey,"Cumulus: An Open Source Storage Cloud for nternational Journal of Intelligent Systems and Applications in Engineering IJISAE, 2023, 11(2), 956–966 | 964 Science", Science Cloud 2011, San Jose, CA. June 2011

[1 4] B. Sotomayor, R. S. Montero, I. M. Llorente, and I. Foster, "Virtual Infrastructure Management in Private and hybrid Clouds', IEEE Internet Computing, vol. 13, no. 5, pp. 14-22, Sep. 2009.

[15] http://www.openstack.org, February, 2013.

[16] P. Chandan and D. Surajit, "Cloud Computing Security Analysis: Challenges and Possible Solutions",

International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016

[17] L. Han, X. Wenjuan and D. Yi, "Research on Building of Electronic Community Based on Cloud Computing".,2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce

[18] L. Han, X. Wenjuan and D. Yi, "Research on Building of Electronic Community Based on Cloud Computing"., 2nd International Conference on Artificial Intelligence, Management Science and ElectronicCommerce

[19] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, Volume 34, Issue 1, pp, 1-11, Jan 2011.

[20] Ramgovind, S.; Eloff, M.M.; Smith, E., "The management of security in Cloud computing," Information Security for South Africa (ISSA), 2010, vol., no., pp.1,7, 2-4 Aug. 2010.

[21] T. Mather, S.Kumarswamy, S. Latif, "'Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Media, 2009.

[22] P Kamongi, "Nemesis: Automated Architecture for Threat Modeling and Risk Assessment for Cloud Computing", ASE 2014

[23] Popović, K. and Hocenski, Z., "Cloud computing security issues and challenges," MIPRO, 2010 Proceedings of the 33rd International Convention, vol., no., pp.344,349, 24-28 May 2010

[24] NIST, NIST Cloud Computing Reference Architecture, 2011.

[25] Cloud Security Alliance, "The Notorious Nine: Cloud Computing Top Threats in 2013"', p8-p21, 2013.

[26] Mell, P. and Grance, T., "'The NIST Definition of Cloud Computing", (Special Publication 800-145), W3C recommendation, World Wide Web Consortium, 2004.

[27] Jörg Hladjk, "Privacy and Data Protection", Vol 7 Issue 4, IT compliance and IT Security-Part 1, p 987-997 2017.

[28] Gordin, A. Graur, A. Potorac and D. Balan, "Security Assessment of OpenStack cloud using outside and inside software tools", International Conference on Development and Application Systems, pp. 170-174, 2018.

[29] V.A. Jujare, "Cloud computing: Approach, Structure and Security" In Second International Conference on Computing Methodologies & Communications, 2021.

[30] K. Raj, "Research on Cloud Computing Security Threats using Data Transmission" International Journal of Advanced Research in Computer Science and Software Engineering, India Volume 5, Issue 1, pp. 399-402, Jan 2

[31] Bashir SF and, Haider S., "Security threats in cloud computing", Proceedings of the International Conference for Internet Technology and Secured Transactions, pp 214–219, 2011

[32] J. Orea, "Quick guide to the reference architecture: Trusted Cloud Initiative", Cloud Security Alliance, 2011.

[33] T. Hamed and R. Marjan Kuchaki, "A survey on security challenges in cloud computing: issues, threats, and

[34] F. Liu, "NIST Cloud Computing Reference Architecture", National Institute of Standards and Technology, U.S Department of Commerce, Special Publication 500-292, Sep. 2011.

[35] R. Roman, J. Lopez and M. Mambo, "Mobile Edge Computing: a survey and analysis of security threats and challenges", Future Generation Comput Syst 78:680–698, 2018.

[36] GICTF, "Use cases and functional requirements for inter-Cloud computing", GICTF White Paper, Global Inter- Cloud Technology Forum, 2010.

[37] Celesti, F. Tusa, M. Villari and A. Puliafito, "How to Enhance Cloud architectures to enable cross-federation", Cloud Computing (Cloud), IEEE 3rd International Conference on, Seiten 337 – 345, 2010.

[38] H. Takabi and J. Joshi, "Security and Privacy Challenges in Cloud Computing Environments", IEEE, 2011.

[39] Salasiah and A. B. Khairul Azmir, "Toward Cloud Computing Reference Architecture", Cyber Resilience Conference (CRC), 2018

[40] Yanuarizki, L. Charles, I. Heru Purnomo and J. Arkav "Toward Cloud Computing Reference Architecture: Cloud Service Management Perspective", International Conference on ICT for Smart Society, 2013.