ISSN:0975-9646

Cloud Computing Security, Defense In Depth Detailed Survey

Ajitabh Mahalkari[1] Avni Tailor[2] Aniket Shukla[3]
Department of Computer Science & Engineering and Information Technology
SD Bansal College of Technology, Indore (M.P) -452001 India

Abstract--Cloud computing is an entirely new approach of computing that offers a non-traditional, but, shared computing paradigm for organizations and individuals. It provides a way to adopt information Technology and its features without huge expenditure on infrastructure and applications. Cloud computing provides multiple on-demand services accessible from a broad network with the ease of scalability even in shared environment so to achieve cost effectiveness.

However, despite the potential gains of cloud computing, security of an open access and shared environment is still a question mark, which directly impact cloud adoptions. Deploying data and business applications to a third party, security and privacy becomes critical concerns. Cloud computing is going to serve enterprise needs for confidentiality of the customer data and compliance, service providers have to provide intense security to ensure sensitive enterprise applications.

In this paper, we surveyed a detailed analysis of the security problems and remedial solutions preferred by cloud service providers. We investigated the layered approach to security, which says that a different security, defense mechanism should be used in different vulnerable areas of the system. As a result, if some part of defense gets compromised, it reduces the risk of security breach on other parts of the system.

Because there are multiple measures of security at different levels, the system will also get extra time to detect and respond to the attack will be an added advantage. It is a security solution to the complete system so it may also be called as defense in depth.

Keywords—Cloud Secuirty, defense in depth (DID), Services, cloud architecture, deployment models, virtualization, vulnerability,Cloud service provider(CSP).

I. INTRODUCTION

Cloud computing is a model for provide more flexibility, shared pool of resources to get on demand network access to configurable computing resources (e.g., networks, servers, storage, applications, and services) which can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud in a service which perform on real time network and give a computation, unite more than two computing resource in type of bunch in another word cloud additionally called Distributed Computing [7].

Most cloud three sort service gives us, Paas and Saas Together with virtualization, clouds could be characterized as computers that are networked anywhere on the planet with the availability of paying the used clouds in a pay-per-use way, implying that simply the resources that are, used will be paid.
In the accompanying, the types of clouds will be presented[7].

- Public Cloud: The Public Cloud alludes to the hosting of a customer's computing infrastructure at a Cloud vendor's premises. That implies the services and infrastructure are provisioned and accommodated geographic removed location over the general population world wide web. The consumer has no visibility and control over where the Cloud service has been hosted. The core-computing infrastructure is shared between numerous organizations and people; on the other hand, every consumer data, platforms, applications, and infrastructure resources were consistently isolated so only authorized clients are permitted access.

- Private Cloud: The Private Cloud service implies that the computing infrastructure has hosted on a "Private Cloud" private and restrictive allocated platforms to a specific organization or individual, and not imparted to different consumers. There are two variations of Private Clouds: on-premise Private Clouds and externally-hosted Private Clouds (externally-hosted Private Clouds likewise only utilized by one body, yet are hosted and kept up by a third-party that practices and convey Cloud infrastructure).

- Hybrid Cloud: At a middle to the Public and Private Cloud, the Hybrid Cloud has turned out to be more popular for businesses needing to receive Cloud Computing for efficiency and cost efficiency, yet seeking to oblige privacy and control for core business data, applications and systems. The qualities of both Private and Public Clouds together has called a Hybrid This often motivates the customer company's use of its own personal (in-house) computing infrastructure for regularly used operations, together with the hosting of some specific applications or systems on the Cloud[8].

- *Software as a Service (SaaS):* The ability gave to the consumer is to utilize the supplier's applications running on a cloud infrastructure. The product and applications are accessible from different client gadgets through either a thin client interface, for example, a web browser (e.g., Internet-based email service), or a project interface or an environment. The consumer does not have control or deal with the basic cloud infrastructure, operating systems, networks, compute and storage servers, or even individual application list, with the limitation user-specified application configuration settings[8].

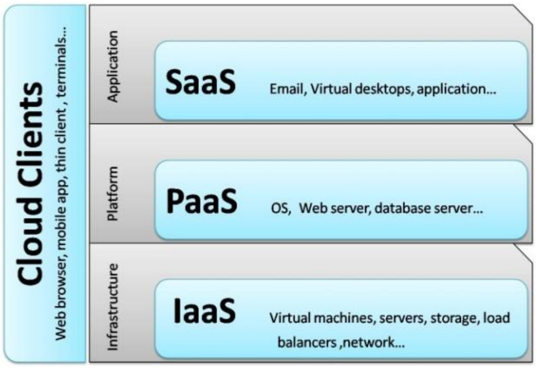
Cloud Clients
Web browser, mobile app, thin client , terminals...
Application
SaaS
Email, Virtual desktops, application...
Platform
PaaS
OS, Web server, database server...
Infrastructure
IaaS
Virtual machines, servers, storage, load balancers ,network...

FIG 1. CLOUD SERVICES WITH EXAMPLES.

- *Platform as a Service (PaaS)*: The capability provided to the consumer is to deploy onto the cloud infrastructure, acquired and developed applications, using programming languages, frameworks, services, and tools supported by the provider[8].
- *Infrastructure as a Service (IaaS):* The service provided to the consumer is to provide compute processors, storage and network access, and other required computing resources from the pool where the consumer is able to deploy and run software and applications, which can include different operating systems. The consumer cannot manage or control the underlying cloud infrastructure but has possibly limited control of select networking components (e.g., host firewalls**)** [8].

II. CLOUD ARCHITECTURE

The Cloud infrastructure framework consists of the following components[4]:

- Physical infrastructure
- Virtual infrastructure
- Applications and platform software
- Cloud infrastructure management tools

The resources of the above components are aggregated to provide Cloud services.

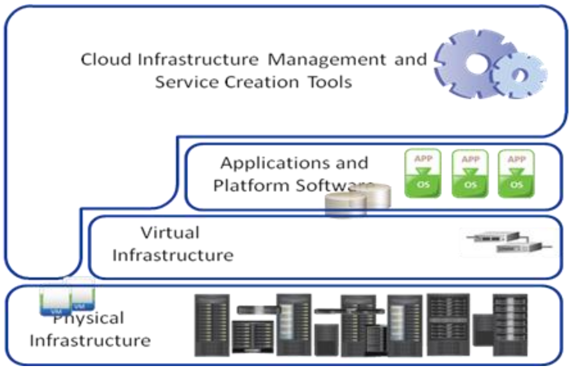
Cloud Infrastructure Management and Service Creation Tools
Applications and Platform Software
APP
OS
Virtual Infrastructure
Physical Infrastructure

FIG 2. CLOUD ARCHITECTURE.

- ***Physical Infrastructure***

The physical infrastructure consists of physical IT resources that include physical servers, storage systems, and physical network components, such as physical adapters, switches, and routers. Physical servers are connected to each other, to the storage systems, and to the clients via physical networks such as IP network, FC SAN, IP SAN, or FCoE network.

- ***Virtual Infrastructure***

Virtual IT resources consist of:

- VMs, virtual volumes, and virtual networks
- VM network components such as virtual switches and virtual NICs

- ***Applications and Platform Software***

Applications and platform software layers include a suite of software's such as:

- Business applications
- Operating systems and database.
- Migration tools

Applications and platform software are hosted on VMs to create software-as-a-service (SaaS) and platform-as-a-service (PaaS).

- ***Cloud Infrastructure Management and Service Creation Tools***

Cloud infrastructure management and service creation tools are responsible for managing physical and virtual infrastructures. They enable consumers to request for Cloud services; they provide Cloud services based on consumer requests and allow consumers to use the services.

III. CLOUD SECURITY

Cloud computing shares similar concerns about security and privacy with traditional computing models that means non-cloud services also suffer from security breaches, but privacy and security vulnerabilities became the major aspects in shared environment of cloud computing. Security concerns are amplified by third party control over organization's data and applications. The potential leakage and mismanagement of those organizational assets became a problem[1] [3].

Components that were under the organization’s direct control before, but after deploying on the third party cloud decisions made about the computing environment by the provider or consumer may have dependency[6].

The consumer need to achieve the believe that data and applications hosted on a cloud provider's infrastructure is in a safe hands, by guaranteeing that the contract agreement with the provider and its related service level agreement (SLA) has fitting provisions and policies for security and privacy. The SLA must keep up legal protections for privacy identifying with data and applications put away on the provider's infrastructure[1][3].

➢ ***Challenges of the Cloud Security***

Cloud computing benefits involve major changes for organizations. Majorly to gain the trust to deploy crucial data and complex business applications to a third party's infrastructure. Certainly it makes security a major issue as organizations need to look at cloud services and providers.

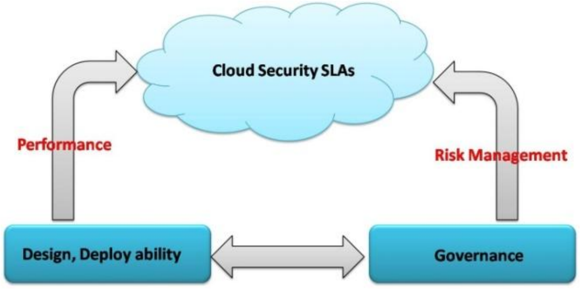

FIG 3. SECURITY CHALLENGES OF CLOUD.

Main principles for Securing the Cloud computing are Secure Identity, Information, Infrastructure.

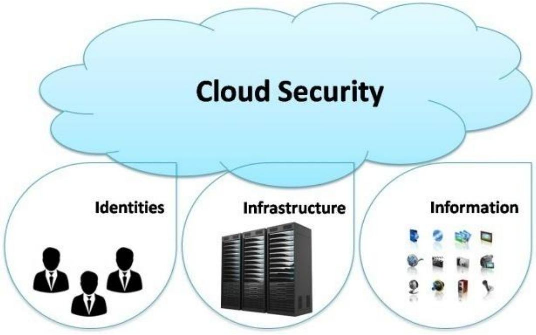

FIG 4. CONCERNED AREA OF CLOUD SECURITY ATTENTION.

Public cloud computing needs to adopt a strong security model that maintains scalable and multi-tenant supports with the need for trust and assurance. As enterprise organizations deploy their computing systems with their identities, business information and infrastructure to the cloud, some level of controls, they must be willing to give up to the providers.

For the same, they must be able to develop a trust cloud system and service providers, and verify CSP and their processes, events and provisioning schemes. Major factors in the building blocks of trust and verification relationships include access control management, security of data and information management, compliance and event management – all security challenges are well understood by IT departments today, concerns with the existing products and technologies, and extendable into the cloud systems.

➢ ***Identity security management***- End-to-end identity management, outsider authentication services, and federated identity will turn into a key component of cloud security. Identity security safeguards the integrity and confidentiality of data and applications while making access promptly accessible to the proper users. Help for these identity management abilities for both users and infrastructure parts will be a real prerequisite for cloud computing, and identity will must be overseen in ways that assemble trust. It will require:

- *Strong authentication*: Cloud computing must move past powerless username-and-password authentication in the event that it is going to be backing the enterprise. This will mean receiving techniques and technologies that are starting now standard in enterprise IT, for instance, solid authentication (multi-factor authentication with one-time passwords) [2] [5].
- *More granular authorization*: Authorization can be coarse-grained within an enterprise or even a private cloud, however, with a specific end goal to handle sensitive data and compliance requirements, public clouds will require granular authorization capabilities, (for example, role-based controls and IRM) that can all be persistent through the cloud infrastructure and the data and information lifecycle[2] [5].

➢ ***Information Security***- In the traditional data center, controls on physical access, authorized access to hardware and software and identity controls all combine to ensure the data. In the cloud, that protective barrier that secures infrastructure is spread. The data needs its security that goes with it and ensures it[9] [13] [18]. It will require:

- *Data isolation*: In the multi - tenancy model, data and application must be kept securely in order to protect it when multiple consumers are using shared resources and infrastructure. In the future time, data isolation will be more important and executable for IAAS services, then perhaps for PAAS and SAAS services.
- *More granular data security:* As the affectability of information builds, the granularity of data classification implementation must increment. For information in the cloud, sensitive data will demand secured access at the file, fields of data, or even block -levels to meet the demands of affirmation and compliance.
- *Consistent data security*: There will be a major requirement for a policy-based content protection scheme to meet the organization's own needs as well as regulatory policy adoptions.
- *Effective data classification*: Cloud computing always faces a resource tradeoff between high performance and the changing requirements of increasingly robust security needs. Data classification would an essential and recommended tool for balancing that equation.
- *Information rights management*: IRM is often treated as a part of identity management, a policy of setting broad-brush controls on which users have access to specific data and applications.
- *Governance and compliance*: A key need of corporate information governance and compliance is the creation of management and validation information – managing, monitoring and auditing the security status of the information and applications with identical capabilities.

➢ ***Infrastructure Security***- The base infrastructure for a cloud must be certain secure whether it is a private or public cloud model or whether the services may be SAAS, PAAS or IAAS[6][9]. It will be required:

- *Inherent component-level security*: The cloud needs to be build and organized to be secure, incorporated with inherently secure components and parts, deployed and provisioned securely with interfaces to other components strongly and, finally, support securely.
- *More granular interface security*: The particular areas in the system where hand-offs occur – user-to-network drivers, server-to application – need granular security policy schemes and controls that ensure consistency and validate accountability.
- *Resource lifecycle management:* The Financials of cloud computing are based on multi-tenancy and the sharing of resources and applications. As a customer's needs and requirements change or increases, a cloud service provider must provision and decommission those resources – like bandwidth, servers, storage, and security – accordingly changes. This lifecycle process must be managed for accountability in order to build trust and performance assurance.

Cloud computing speaks to an exceptionally rapid territory at the present time, with new suppliers and new offerings arriving constantly. There are various security risks connected with cloud computing, for example, Loss of governance. Obligation ambiguity. Detachment disappointment. Merchant lock-in. Compliance and legal risks. Handling of security episodes. Management interface vulnerability. Data protection. Vindictive conduct of insiders. Business disappointment of the provider. Service unavailability. Unreliable or incomplete data deletion, that must be adequately addressed.

IV. DEFENSE STRATEGIES

In cloud computing there are different levels on which a security policy or method must be applied to as to cover all security challenges[2]. All these security methods are explained below:

➢ ***Security at Compute Level***

Securing a compute infrastructure includes ensuring security at compute infrastructure includes enforcing security of the physical server, hypervisor, VM, and guest OS. Virtualization is created and managed by hypervisor, security at the hypervisor level, mainly aims at securing the hypervisor from the rootkits and malware based attacks and protection of the hypervisor management system because if hypervisor compromises it may be a single point failure. VM isolation and hardening are two main popular techniques for securing VMs. Guest OS needs should also be taken into account, security at the guest OS level uses sandboxing and hardening as two key methods. Application level hardening is used to reduce vulnerability of the applications from getting exploited by malicious attackers[6].

a) *Physical Server Security*

Server security considerations include identifying server application details such as:

- Make a deciding factor if the server will be used for specific applications (for example backup applications) or for general purpose.
- Identifying the network services to be provided on specific server; for example, LAN connections, wireless connections, etc.
- Identifying users and/or user groups who will be given access rights on the server site. Determining their specific access privileges under this process.

Based upon the details of server, suitable protection measures need to be decided including the following:

- Choosing best suited authentication and authorization mechanisms of users.
- If the server has unused hardware components such as NICs, USB ports, or drives, they should be removed or disabled. This should also be done in the VM (template).
- Adequate physical security protection, including safety of the premises where the server will be housed.

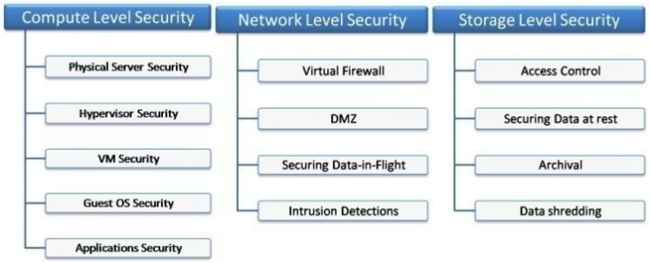

FIG 5. COMPUTE, NETWORK AND STORAGE LEVEL SECURITY STRATEGIES.

b) *Hypervisor Security*

Hypervisor in a virtualized environment presents a single point of security failure for all the VMs running on it currently. Only a single point breach of the hypervisor may cause all the guest OSs on these VMs at high risk of vulnerability. Protection against attacks, security-critical hypervisor security updates should always be installed on a regular basis, and the VMs hosted and running on it should be hardened properly (VM hardening measures are discussed next).

The management system of hypervisor must be protected at a peak. Serious malicious attacks and infiltration of the management system can impact all the existing and running VMs and allow attackers to create new VMs as well and even infect VMs templates too. Malicious or unauthorized access to the management system should be restricted only to authorized administrators and reliable identities.

c) *VM Security*

VM isolation is one of the measures that helps in preventing a VM and compromised guest OS from impacting other OSs on the same hypervisor. VM isolation is applied at the hypervisor level so that VMs running on the hypervisor kept secured.

Apart from isolation, VMs should also be hardened against security loopholes. It is a process of altering the default configuration in order to achieve greater security at the VM level. Also perform vulnerability scanning of the guest OS regularly to identify existing vulnerabilities. Regularly perform a penetration testing to determine the feasibility of an attack and the extent of business impact of the attack.

d) Guest OS and Application Security

Along with the measures to secure a hypervisor and VMs, Data Centers and Cloud environment also require further measures on the guest OS and application levels. As hardening is one such important measure which can effectively safeguard guest OS and the applications running on it.

OS hardening, involves actions such as configuring system and network nodes, flushing unused files, and latest updates must be applied. Application hardening helps to prevent exploitation of vulnerabilities in software applications that have not been patched so far. The key steps for hardening a vulnerable application may include disallowing the application from spawning executable files, disallowing the application for creating or modifying executable files with the applications, do not allow the application from modifying sensitive areas.

➢ ***Security at Network Level***

a) Virtual Firewall

A firewall is a security technology designed to permit or deny network transmits data based upon a set of rules defined by the providers. A firewall is implemented on a compute level and limits access between networks and/or systems in accordance with a specific security policy inside it. A firewall is a popular tool, used to protect networks from unauthorized access while permitting only legitimate communications[11].

Securing the VM-to-VM traffic running on a server is a key security problem in a data center environment. Securing this virtual network is a considerable challenge because virtual switches could be invisible to network and/or system administrators, who usually enforce security at the network level. Because the virtual network traffic may never leave the server, security administrators cannot observe traffic between VM to another VM, cannot intercept and read it, and so, cannot know what that traffic is for.

b) Demilitarized Zone

In a network, the nodes (compute systems) that are most vulnerable to an attack are those that provide services to users outside of the network; for example, e-mail and Web servers. Therefore, these nodes are placed into their own sub-network in order to protect the rest of the network from intruders.

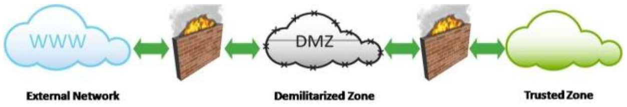

FIG 5. DEMILITARIZED ZONE IN CLOUD COMPUTING

Such a sub-network is known as a Demilitarized Zone (DMZ), which is isolated from the rest of the network.

c) Securing Data-in-Flight

Data-in-flight refers to the data transferred over a network, and means that the data is “moving” state. The encryption process of data-in-flight is the main method for providing confidentiality and integrity services.

➢ ***Storage Security in Cloud***

Major threats to storage system in a VDC and Cloud environment arise due to vulnerability at compute, network, and/or physical security levels. This is because an access to storage systems needs to be made by using compute and network infrastructure. Therefore, adequate security measures need to be in place at compute and network levels to ensure storage security. Storage Area Networks (SAN) have their own unique vulnerabilities, which can be used to compromise their integrity. These include unauthorized device gaining fabric connection, DOS attack, WWN spoofing, which would enable a device to masquerade as a different entity, zoning bypass, etc. Security mechanisms that might help to protect storage includes[13]:

a) Securing Data-at-Rest

Data-at-rest refers to the data which is not being transferred over a network, i.e., is “not moving”. It includes data that resides in every form of databases, file systems, flash drives, memory of all types, networked storage like SAN, etc.

Encryption of Data-at-rest is the key method for providing confidentiality and integrity. Encryption makes the data indecipherable to unauthorized users. Full disk encryption is the key method used for encrypting data-at-rest residing on a disk. Full disk encryption employs software application or built-in hardware capability to encrypt every bit of data that goes on a disk or disk volume. Disk encryption thus prevents unauthorized access to data storage.

b) Data Shredding

Unlike data stored in a privately controlled storage or in a CDC, data and information in a Cloud remain vulnerable even if deleted by the client or a process. This is because this data and information may still have recoverable traces about it on the system, and therefore, can be a potential source of attack on the data center. Data shredding scheme is therefore an important and critical factor for data security to be considered in a Cloud infrastructure, deleted data includes:

- Logs of deleted VMs including its configuration files and application executions
- Logs of old files, folders, and other resources
- Logs of data communication involving deleted VMs

➢ ***Physical Security in Cloud and Data Centers***

Cloud customers essentially lose control over physical security when they move to the Cloud, because the actual servers can be anywhere the provider decides to put them. Typical security measures that must be in place for securing physical Cloud infrastructure include:

- Leaving a port in unconfigured or disabled state so that unknown devices or components cannot connect to the infrastructure. Additionally, bind specific devices to designated ports. Apply MAC/WWPN binding and VLAN restrictions to physical Ethernet switches.
- 24/7/365 on-site security for the premise where the Cloud physical infrastructure is hosted.
- Biometric authentication based access to the premises
- CCTV camera surveillance to monitor activity throughout the facility

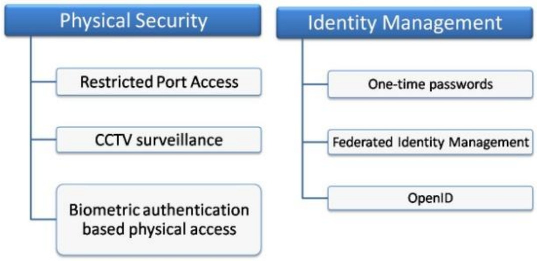

FIG 6. PHYSICAL LEVEL SECURITY AND IDENTITY MANAGEMENT STRATEGIES IN CLOUD.

➢ *Role Based Access Control*

In a Role Based Access Control (RBAC) model, resource access rights (permissions) are given to subjects (users and processes) based upon their roles. A role may represent a job function, for example, an administrator. Permissions are associated with the roles and subjects are not given any direct permissions. Subjects acquire permissions to perform operations on resources based upon the roles assigned to them[12].

➢ *Identity Management (IM) in Cloud*

Identity management is an administrative process that deals with identifying users of an information system. Additionally, identity management also controls access to system resources by placing restrictions using user identities. The key identity management-related aspects in Cloud are, One-time password, Federated Identity Management process, OpenID[15].

V. DEFENSE IN DEPTH

Defense-in-depth represents the use of multiple security defenses to help mitigate the risk of security threats, if one component of the defense is being compromised. An example, could be an antivirus software installed on individual VM when there is already a virus protection on the firewalls within the same environment. Different security products from multiple vendors may be deployed to defend different potential vulnerable resources within the network.

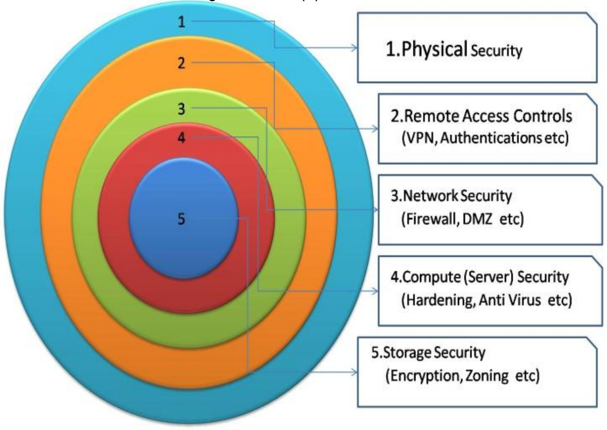
1
2
3
4
5
1.Physical Security
2.Remote Access Controls (VPN, Authentications etc)
3.Network Security (Firewall, DMZ etc)
4.Compute (Server) Security (Hardening, Anti Virus etc)
5.Storage Security (Encryption, Zoning etc)

FIG 7. DEFENSE IN DEPTH SECURITY POLICY IN CLOUD.

Defense-in-depth is an information assurance strategy in which multiple layers of defense are placed throughout the system. For this reason, it is also known as a “layered approach to security”. Because there are multiple measures of security at different levels, defense-in-depth gives additional time to detect and respond to an attack. This reduces the scope of a security breach. However, the overall cost of deploying defense-in-depth is often higher, compared to single-layered security mechanisms[1] [15].

VI. ADVANTAGES OF APPROACH

- Multilayered cloud security approach.
- Minimizes the risk of security breach even other components of the system get compromised.
- Compete CIA triad assurance for critical enterprise business information and applications.
- Provides additional time to detect and respond to the attacks.
- Can handle higher velocity and different varieties of attacks.
- Crucial data storage is at the deepest layer to provide stronger protection.
- Includes all the areas of possible security vulnerabilities even with the virtualized components.
- Complete security solution for cloud computing, well suited for all types of deployment models of cloud.
- Use of best practice security mechanisms in the different areas of concerns.
- Meets all the requirements of the SLAs and other legal issues.
- Performance management and focus on the availability of the cloud resources and services.
- Less overheads on the client sites so to avoid throughput issues.
- The overall cost of the approach is higher, but can be optimized.

VII. FUTURE WORK

Above review focuses on the security challenges of the cloud computing paradigm. We investigate all the available security mechanisms for the cloud, we found there is a need of complete stack of the methods that can handle all the types of attacks on the cloud. The strategy must keep the performance and overhead issues in mind. We could find such a mechanism as the complete security solution for the CSPs. We can title it as "Defense in depth", but the over cost of the mechanism is higher because it includes a security mechanism from different vendors, as mentioned in the advantages of the approach. The future of this work would be at the cost of the method. Researchers may work on the cost optimization of the approach so that CSPs can adopt it as the best cloud security mechanism.

VIII. CONCLUSION

Throughout this paper, the author has systematically studied the security and privacy issues in cloud computing based on cloud architecture components. We have identified the most representative, security/privacy attributes (e.g., confidentiality, integrity, availability, accountability, and privacy-preservability), as well as discussing the vulnerabilities, which may be exploited by adversaries in order to perform various attacks. Defense in depth strategy and suggestions were discussed as well. We believe this review will help shape the future research directions in the areas of cloud security and privacy.

REFERENCES

[1] Zhifeng Xiao And Yang Xiao, Senior Member, IEEE "Security And Privacy In Cloud Computing" published in IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013.

[2] Ryan Ko, Stephen S G Lee "Cloud Security Alliance Cloud Computing Vulnerability Incidents" Published In IEEE Spectrum Volume 49 Issue 12

[3] Keiko Hashizume, David G Rosado2, Eduardo Fernández-Medina and Eduardo B Fernandez " An analysis of security issues for cloud computing " Springer Hashizume et al.: An analysis of security issues for cloud computing. Journal of Internet Services and Applications 2013 4:5.

[4] Peter Mell, US National Institute of Standards and Technology " What’s Special About Cloud Security ? " Published by the IEEE ComputerSociety IT Pro July/August 2012.

[5] Stephen Coty, Patrick Snyder, Kevin Stevens" Research on the Evolving State of Cloud Security " Alert Logic Cloud Security Report Spring 2014.

[6] RSA White paper "The Role of Security in Trustworthy Cloud Computing ".

[7] J.Srinivas, K.Venkata Subba Reddy, Dr.A.Moiz Qyser "Cloud Computing Basics " Published In International Journal Of Advanced Research In Computer And Communication Engineering Vol. 1, Issue 5, July 2012.

[8] Rahul Bhoyar, Prof. Nitin Chopde "Cloud Computing: Service models, Types, Database and Issues" published in International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 3, March 2013

[9] Dr Nashaat el-Khameesy, Hossam Abdel Rahman "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems " Journal of Emerging Trends in Computing and Information Sciences VOL. 3, NO. 6, June 2012.

[10] Pardeep Kumar, Vivek Kumar Sehgal , Durg Singh Chauhan, P. K. Gupta and Manoj Diwakar "Effective Ways of Secure, Private and Trusted Cloud Computing " published in IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, May 2011.

[11] Fang Hao, T.V. Lakshman, Sarit Mukherjee, Haoyu Song " Secure Cloud Computing with a Virtualized Network Infrastructure " white paper Bell Labs.

[12] M V Rajesh, Soma Sekhar T And Siva Rama Krishna T "Enhanced Secure Data Access Model For Public Clouds " International Journal For Research In Science & Advanced Technologies Issue-1, Volume-1, 039-045

[13] Lei Xu, Chunxiao Jiang,Jian Yuan "Information Security In Big Data: Privacy And Data Mining" Ieee Access Received September 21, 2014, Accepted October 4, 2014, Date Of Publication October 9, 2014, Date Of Current Version October 20, 2014.

[14] Cloud Standard Customer Council White Paper "Security For Cloud Computing 10 Steps To Ensure Success".

[15] Jianhua Che, Yamin Duan, Tao Zhang, Jie Fan" Study on the security models and strategies of cloud computing" 2011 International Conference on Power Electronics and Engineering Application

[16] Farhan Bashir Shaikh , Sajjad Haider "Security Threats in Cloud Computing" International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates

[17] Wentao Liu "Research on Cloud Computing Security Problem and Strategy" IEEE 2012

[18] Cloud Security Alliance "The Notorious Nine: Cloud Computing Top Threats In 2013" Csa White Paper.