ISSN: 0974-5823 Vol. 7 No. 7 July, 2022

International Journal of Mechanical Engineering

Comprehensive Study on Cloud Security

Kalyani, Shriya Singh*, Rehan Ahmad, Shivani Joshi, Shalu kumara

Dronacharya Group of Institution, Greater Noida, UP, India

Abstract - Nowadays, cloud computing provides services over the internet.It helps to preserve large amounts of data without storing them .By this, we can access our data anytime or anywhere we want . But it also has some issues like security issues.Security is the first priority to everyone. The cloud provider offers its services over the Internet and makes extensive use of web technology, which raises additional security concerns.In this paper, we are focusing on the topic cloud security. We talk about different types of security issues and their solutions.In this paper, we have also mentioned all the work has been done before in cloud security.

Keywords - Cloud security, requirements, threats, vulnerability, survey and conclusion.

1 Introduction

Cloud computing refers to the use of the internet to supply on-demand IT resources. Cloud Service Providers are the businesses that provide these computing solutions (CSPs). CSPs employ a number of billing methods to charge users and organisations for Cloud resources they utilise. A Hypervisor abstracts cloud resources from the underlying physical hardware. However, Cloud computing is fraught with ambiguity because it encompasses a wide range of services and deployment methodologies. This essay will explain the fundamentals of cloud computing to you.

Cloud deployment models can be divided into the following categories:

1) Private cloud
2) Public cloud
3) Hybrid cloud
4) Multi Cloud

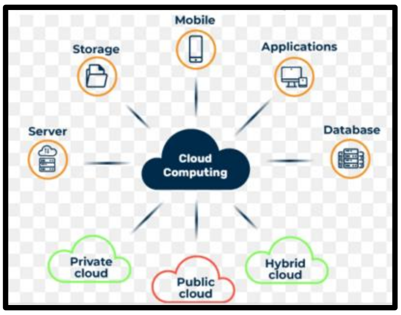

Fig 1 Types of cloud computing

The implementation kind, hosting type, and who has access to it all differ among these deployment models.

Private cloud

Private clouds are cloud environments dedicated entirely to a single end user or group, and run behind that user's or group's firewall.

Public cloud

Public clouds are cloud environments that are often built with IT infrastructure that does not belong to the end user. Alibaba Cloud, Amazon Web Services (AWS), Google Cloud, IBM Cloud, and Microsoft Azure are just a few of the most well-known public cloud providers.

Hybrid cloud

A hybrid cloud is a unified IT environment made up of different environments linked by LANs, WANs, VPNs, and/or APIs.

Multi cloud

Multi Clouds are a cloud strategy that combines many cloud services from multiple cloud vendors—public or private—into one solution. Multi clouds are hybrid clouds, however hybrid clouds are not always multi clouds. When different clouds are linked together through integration or orchestration, they become hybrid clouds.

2 Cloud services

Infrastructure, platforms, and software that are hosted by third-party providers and made available to consumers via the internet are known as cloud services. As indicated in fig.2, there are three basic types of as-a-Service solutions: IaaS, PaaS, and SaaS. Each allows the transfer of user data from front-end clients across the internet, to the cloud service provider's servers, and back—but they differ in the services they offer.

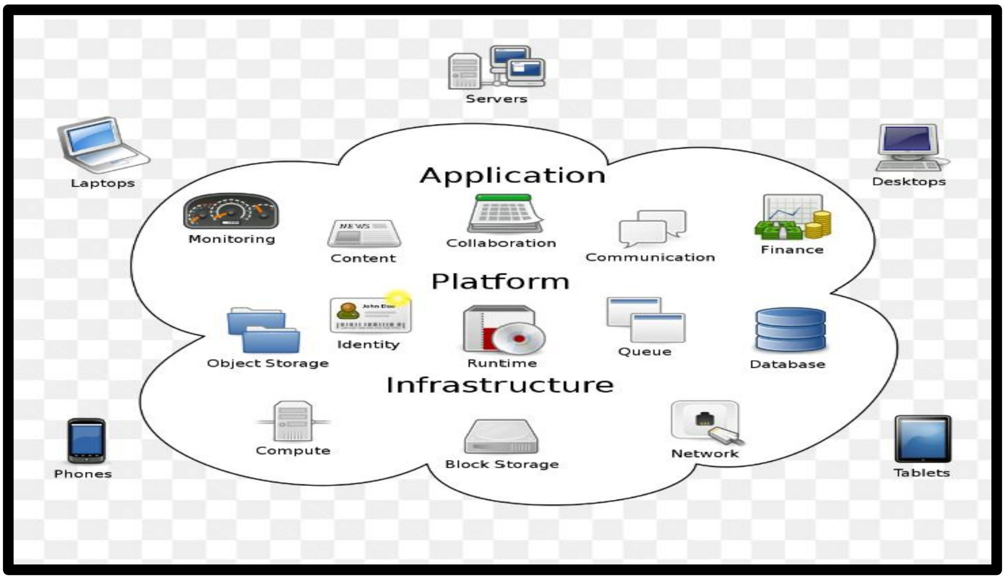

Fig.2 Types of as a service solution

2.1 IaaS

A cloud service provider manages your infrastructure, including physical servers, networking, virtualization, and data storage, via an internet connection. The infrastructure is rented and accessed through an API or dashboard by the user.

2.2 PaaS

PaaS is a cloud service model in which an external cloud service provider supplies and administers the hardware and software platform, but the user is responsible for the programmes that run on top of it as well as the data it utilises. PaaS is a shared cloud platform for application development and management (an important DevOps component) that eliminates the need to build and maintain the infrastructure traditionally associated with the process.

2.3 SaaS

SaaS is a service that provides users with access to a software application that is managed by the cloud service provider. SaaS apps are typically web applications or mobile apps that may be accessed through a web browser. The user is responsible for software updates, bug fixes, and other basic software maintenance, and they connect to cloud apps via a dashboard or API.

3 Characteristics and advantages of cloud computing

Some of the main characteristics of cloud computing are the following:

3.1 Provisioning via self-service

On-demand compute resources for nearly any form of workload are available to end customers. End users can provision computing resources such as server time and network storage, obviating the requirement for IT administrators to provision and manage compute resources in the past.

3.2 Elasticity

Companies have the freedom to scale up as computing demands rise and down as they fall. This reduces the need for large-scale expenditures in local infrastructure that may or may not be operational in the future.

3.3 Pay as you go

Users can pay only for the resources and workloads they utilise because compute resources are assessed at a granular level**.**

3.4 Resilience in the workplace

CSPs frequently deploy redundant resources to maintain reliable storage and to keep users' critical workloads running, which often span numerous global locations.

3.5 Flexibility in migration

Certain workloads can be moved to or from the cloud — or to multiple cloud platforms — as needed or automatically for cost savings or to take advantage of new services as they become available.

Access to a large network. A user can use any device with an internet connection to access cloud data or upload data to the cloud.

3.6 Resource pooling and multi-tenancy

Multi-tenancy allows several clients to share the same physical infrastructure or applications while maintaining privacy and security.

These features support a number of essential advantages for modern business, including:

Management of expenditures

Cloud infrastructure can lower capital expenses because companies don't have to spend as much money on purchasing and maintaining equipment. This lowers their capital expenditure expenses by eliminating the need to invest in hardware, buildings, utilities, or the construction of massive data centres to support their expanding operations. Furthermore, enterprises may rely on the experience of their cloud providers' teams to handle cloud data centre operations, so they don't need massive IT teams. Cloud computing also lowers the cost of downtime.

Mobility of data and workload

By storing data in the cloud, users can access it from any device with an internet connection from anywhere. This suggests that users aren't aware of it.

4 Business continuity and disaster recovery (BCDR)

Data loss is a concern for all businesses. Users may always access their data by storing it in the cloud, even if their devices, such as laptops or cellphones, are unusable. In the event of a calamity, such as a natural disaster or a power outage, cloud-based services allow businesses to quickly restore their data. This is advantageous to BCDR because it ensures that workloads and data remain accessible even if the business is damaged or disrupted.

5 Disadvantages of cloud computing

Despite the obvious benefits of using cloud services, cloud computing comes with its own set of problems for IT professionals:

5.1 Cloud safety

Cloud computing's main difficulty is frequently regarded as security. When businesses rely on the cloud, they risk data breaches, API and interface hacking, compromised credentials, and authentication concerns. Furthermore, there is a lack of transparency regarding the handling of sensitive data entrusted to the cloud provider. Cloud setups, as well as company policy and practise, must be carefully monitored for security.

5.2 Unpredictability of costs

Pay-as-you-go cloud subscription options, along with resource scalability to accommodate changing workload demands, can make it difficult to define and anticipate final prices. Cloud prices are frequently intertwined, with one cloud service relying on one or more other cloud services.

5.3 Inadequate capability and knowledge

Organizations are trying to keep up with the growing demand for tools and workers with the right skill sets and expertise needed to plan, deploy, and manage workloads and data in the cloud as cloud-supporting technologies advance.

5.4 IT management

Because there is no control over provisioning, deprovisioning, or management of infrastructure operations, cloud computing's emphasis on do-it-yourself capabilities can make IT governance challenging. This can make adequately managing risks and security, IT compliance, and data quality difficult.

5.5 Observance of industrial regulations

It might be challenging to monitor compliance with industry requirements through a third party when transferring data from on-premises local storage to cloud storage. It's critical to understand where data and workloads are located.

5.6 Multiple cloud management

Because each cloud is unique, multi-cloud deployments might cause efforts to address more general cloud computing concerns to become disjointed.

5.7 Performance of the cloud

The organisation contracting cloud services with a provider has little control over performance metrics like latency. If companies do not have contingency plans in place, network and provider failures can interrupt productivity and business processes.

5.8 Creating your own private cloud

Architecting, creating, and administering private clouds, whether for their own use or as part of a hybrid cloud strategy, may be a difficult process for IT departments and personnel.

5.9 Migration to the cloud

Moving applications and other data to a cloud infrastructure is a time-consuming operation. Migration projects are notorious for taking longer than expected and going over budget. The problem of workload

5.10 Lock-in of vendors

Switching cloud providers can frequently result in serious problems. This involves technical incompatibilities, legal and regulatory constraints, and significant expenses associated with large data moves.

6 Cloud computing security

Security remains a primary concern for businesses contemplating cloud adoption -- especially public cloud adoption. Public CSPs share their underlying hardware infrastructure between numerous customers, as the public cloud is a multi-tenant environment. This environment demands significant isolation between logical compute resources. At the same time, access to public cloud storage and compute resources is guarded by account login credentials.

Many organisations bound by complex regulatory obligations and governance standards are still hesitant to place data or workloads in the public cloud for fear of outages, loss or theft. However, this resistance is fading, as logical isolation has proven reliable and the addition of data encryption and various identity and access management tools have improved security within the public cloud.

This boost in processing power and infrastructure nodes can come from a huge distributed system that combines a large number of resources into a single unit that can handle extremely taxing computations like scientific simulations.Clusters and grids are two often used components in distributed systems[1] .Clusters and grids are two separate methods. The cluster paradigm allows homogeneous networks to be coupled, whereas grids are used to create large distributed and heterogeneous networks.Due to the high cost of central processing units like parallel supercomputers, the cluster approach is more expensive. The grid is the most widely utilised architecture for creating servant computational nodes by desktop and home users, and it is created over the Internet.

The utility of computers,term was coined by Corbato and Vyssotsky in 1965 to describe a business model for on-demand transmission of computing resources based on a pay-as-you-go paradigm, which allows consumers to choose which resources (platforms,) security policies they want.Cloud computing is becoming more popular as more businesses use the technology, however there are significant security concerns. When moving data to faraway locations, each company selects a secure infrastructure.The primary barriers to cloud computing adoption, according to the NIST security, are portability and interoperability. Many businesses expressed their concerns and thoughts on cloud security vulnerabilities in 2009.IDC is a market research and analysis business that advises enterprise Chief Information Officers (CIOs) on the most vulnerable security vulnerabilities.According to the study results, 87.5 percent of respondents ranked security as a top priority. Many hazards are associated with storing sensitive data in the cloud, hence many organisations are hesitant to transfer their sensitive data to distant storage clouds[2] .To achieve multi-tenancy, the cloud uses a virtual environment. Virtual machines have flaws that pose a direct danger to the security and privacy of cloud services. Cloud services also include online and data movement through the Internet.The browser Application Program Interface (API) and the network channel both have numerous security flaws. Multi-tenancy principles are used to distribute and share cloud resources across numerous users. This idea is a roadblock to establishing a security architecture that protects data and services completely.Due to concerns about transparency, the cloud service provider will not allow its customers to integrate security monitors or intrusion detection systems into the management service layer at the back of the virtualized cloud environment. An attacker could, for example, use a back channel attack with a kernel level rootkit to gain access to cloud data. Physical level attacks, such as reading cloud-stored data, are also known to the community. Cloud service providers and cloud consumers agree on a Service Level Agreement (SLA) to ensure the security and privacy of associated data and services.The survey paper offers a thorough examination of many security challenges and their remedies, which are summarised in each subsection's summary table. In addition, the article discusses cloud security issues, the assault, and possible solutions

TABLE 1

Cloud overview, cloud automation, security requirements, cloud trust, Cloud security (abstraction, threats & attacks), Cloud security challenges, Security solutions, and Open issues are compared with the survey.

S.No	Survey	Year	Topic discussed	Cloud overview	Cloud automation	Security requirements	Cloud trust	Cloud security (threats & attacks)	Cloud security issues	Security solutions	Open issues
1	Takabi et al. [5]	2010	Security and privacy, virtualization, trust management ,secure service management	-	X	X	✓	-	-	X	X
2	Grobauer et al.	2011	Vulnerablelity in the cloud,	-	-	-	X	X	-	X	X

	[6]		risk in the cloud, authentic ation, Authorization and access control								
3	Zissis et al.[7]	2012	Cloud trust, cryptographic security methods, security standards, trusted third-party	-		✓	✓	-	X	X	X
4	Modi et al.[8]	2013	Threats and attacks in the cloud, security challenges at various layers, authentication and virtualization security concerns	X	X	✓	✓	✓	-	-	✓
5	Fernandes et al.[9]	2014	Cloud computing concepts and technologies, as well as cloud security Concerns	✓	✓	✓	✓	X	✓	X	✓
6	Ali et al. [10]	2015	Security difficulty s in mobile cloud computing g, cloud computing g overview, cloud security issues, cloud	✓	X	X	-	-	-	-	✓

			security solutions								
7	Ashish et al.[11]	2016	Cloud overview, cloud technologies, cloud security requirements, cloud trust, Cloud security (abstraction, threats & attacks), cloud security issues and their solutions, future research directions	✓	✓	✓	✓	✓	✓	✓	✓

The “-” symbol denotes less discussion on each aspect. The “ ” and “X” symbols denote that the specific domain is covered and the domain is not covered with respect to the given aspect respectively.

7 Cloud security concepts

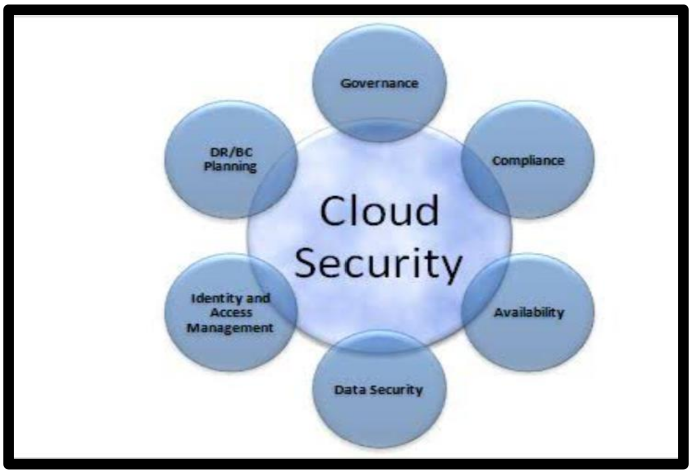

Fig. 3 Cloud security

To comprehend the security challenges in the cloud, this part goes through various cloud-specific concepts such virtualization, multi-tenancy, cloud platforms, data outsourcing, data storage standardisation, and trust management as shown in fig.3

7.1 Virtualization aspect

Virtualization is a concept that separates services, applications, computing resources, and operating systems from the hardware they run on. A component of virtualization is the virtual machine (VM) and the virtual machine manager (VMM). A virtual machine (VM) is a per-image of a large-size operating system (OS) called guest OS content memory and storage. The guest OS is in charge of executing various programmes. It's similar to a host operating system, but it doesn't provide you direct access to the hardware.VMMs, which are in charge of allocating virtual hardware resources such as CPUs, RAM, network, and hard drive to each VM, can access this resource. When a new VM requests hardware resources from VMMs, a new image of that resource is produced rapidly and assigned to the requested VM. VMMs is also in charge of connecting many virtual machines. Finally, virtual machines are linked to virtual switches and comprise external and internal networks

7.2 Multi-tenancy

Multi-tenancy is a characteristic of the cloud computing environment that introduces the sharing notion, allowing one or more tenants to share each running instance. It allows several users to share a single cloud platform. VMMs is a multi-tenancy sharing platform that is designed to secure IT assets, and it is considered an IaaS provider.

7.3 Cloud platforms

Cloud customers need to install their utility and offerings to the cloud, it requires some doable frames to be useful to install their utility.The platform offers APIs, and IDE for improvement of the cloud applications. All the gear depends on the underlying infrastructure of the platform and the programming language.

7.4 Security identification of the threats

The maximum difficulty at the time of implementation of appropriate countermeasure in an IS, is figuring out the unique protection threats. In the usual protection gadget designing technique, the primary purpose is to pick out protection threats related to them, then discover the safety requirements then practice decided on protection controls to reap the excessive reliability, maintainability and supportability.The confidentiality, integrity, availability is the constructing block of designing any protection gadget.These vital protection components are essential to make a stable cloud. The cloud architectural layout affords some protection advantages, which protects the excessive availability, centralization of protection, redundancy, and records and technique segmentation.

7.5 Data outsourcing

For their business purposes, companies nowadays employ outsource data models. It's a technique in which people delegate data collecting and extraction to a third-party supplier. This third party usually works on a contract basis with another corporation. This function allows for both capital and operational investment. Data outsourcing has certain disadvantages, such as creating a physical barrier between data owners and their data. When a consumer transfers her data to a third party first, he assures that the data computing and storage takes place in a secure manner.

8 Threats to security are identified

The most difficult part of implementing appropriate countermeasures in an IS is identifying the particular security threats. The goal of the standard security system design process is to identify security threats, then determine security needs, and then apply selected security controls to achieve high dependability, maintainability, and supportability. The building blocks of any security system are confidentiality, integrity, and availability. These crucial security features are required to provide a secure cloud. The cloud architectural design offers several security benefits, including high availability, security centralization, redundancy, and data and process segregation.

9 Requirements of cloud security

Authentication or identification, authorisation, secrecy, integrity, non-repudiation, and availability are the six security requirements. To prevent unauthorised access to the public cloud, each service model (IaaS, PaaS, and SaaS) requires authorisation. The hybrid cloud is more secure than public and private clouds because the hybrid cloud concept necessitates higher security standards than public and private clouds. In addition, the integration possibilities in the hybrid cloud give an extra degree of protection.

10 Threats to cloud computing

Threat is defined in computer security as anything that has the potential to do substantial harm to a computer system fig.4 shows different threats to cloud computing. Threats can lead to potential computer system or network infrastructure attacks. The biggest [3] threats to the security architecture of cloud services were presented in the paper. The following are some potential threats to the cloud:

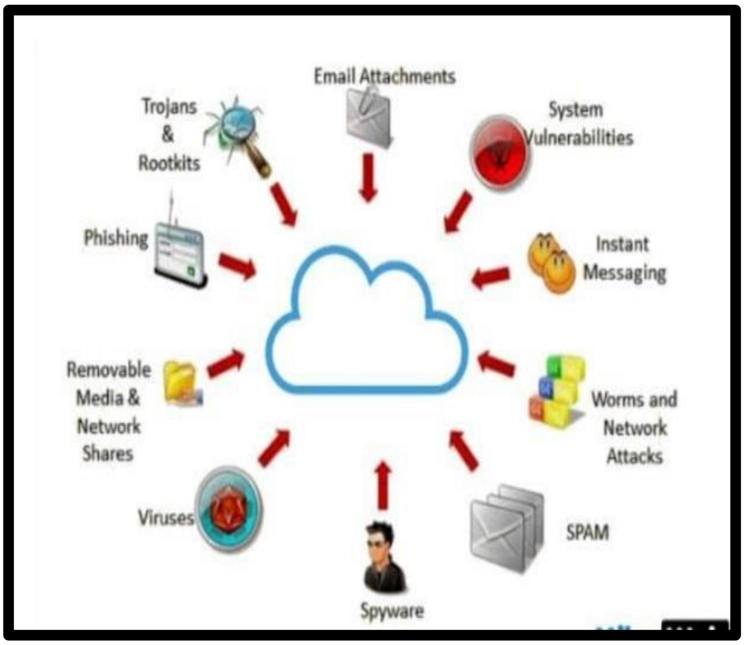

Fig. 4 Threats to cloud computing

10.1 Receiving model

Both the cloud computing and business models use distinct delivery/receiving services. As a result, cloud computing has the ability to change the way it delivers services. The cloud service provider assigns all services and applications to remote locations. Companies must consider all of the dangers connected with losing control of their cloud.

10.2 Insecure interface and API

Users can communicate with cloud services using a set of software interfaces and APIs provided by the cloud provider. These interfaces are built on top of the cloud foundation in the form of a layer, adding to the cloud's complexity. Customers can use such interfaces for all provisioning, management, and monitoring services. As a result, the cloud's security and availability are heavily dependent on the security of these APIs.However, both inadvertent and deliberate attempts can compromise the APIs' security. API threats may have an impact on PaaS, IaaS, and SaaS service models.

10.3 Data loss and leakage

Due to the productive and sharing nature of cloud computing, data loss can occur when data is deleted, altered, or stolen without a backup of the original content. Data loss can also occur when an encoding key is lost. Lack of authentication, authorisation, and access control, as well as weak encryption techniques, weak keys, danger of association, unstable data centres, and catastrophe recovery, are the main causes of data loss and leakage.

10.4 Account hijacking

The service hijacking process involves redirecting the client to a malicious website.

This can be accomplished by deception, phishing, and the use of software flaws. Such assaults are frequently caused by the reuse of credentials and passwords.

10.5 Risk profiling

Because of the high workload, clouds are less concerned with hardware and software ownership and maintenance. The cloud offers organisations contracts to maintain software and hardware. This concept is sound, but the cloud is unaware of the company's internal security procedures, such as patching [4], audits, security policies, hardening, and logging

11 Attacks on cloud security

•Denial of service attack

•Service injection attack

•Port scanning

•User to root attacks

•Phishing attack

•Backdoor channel attack

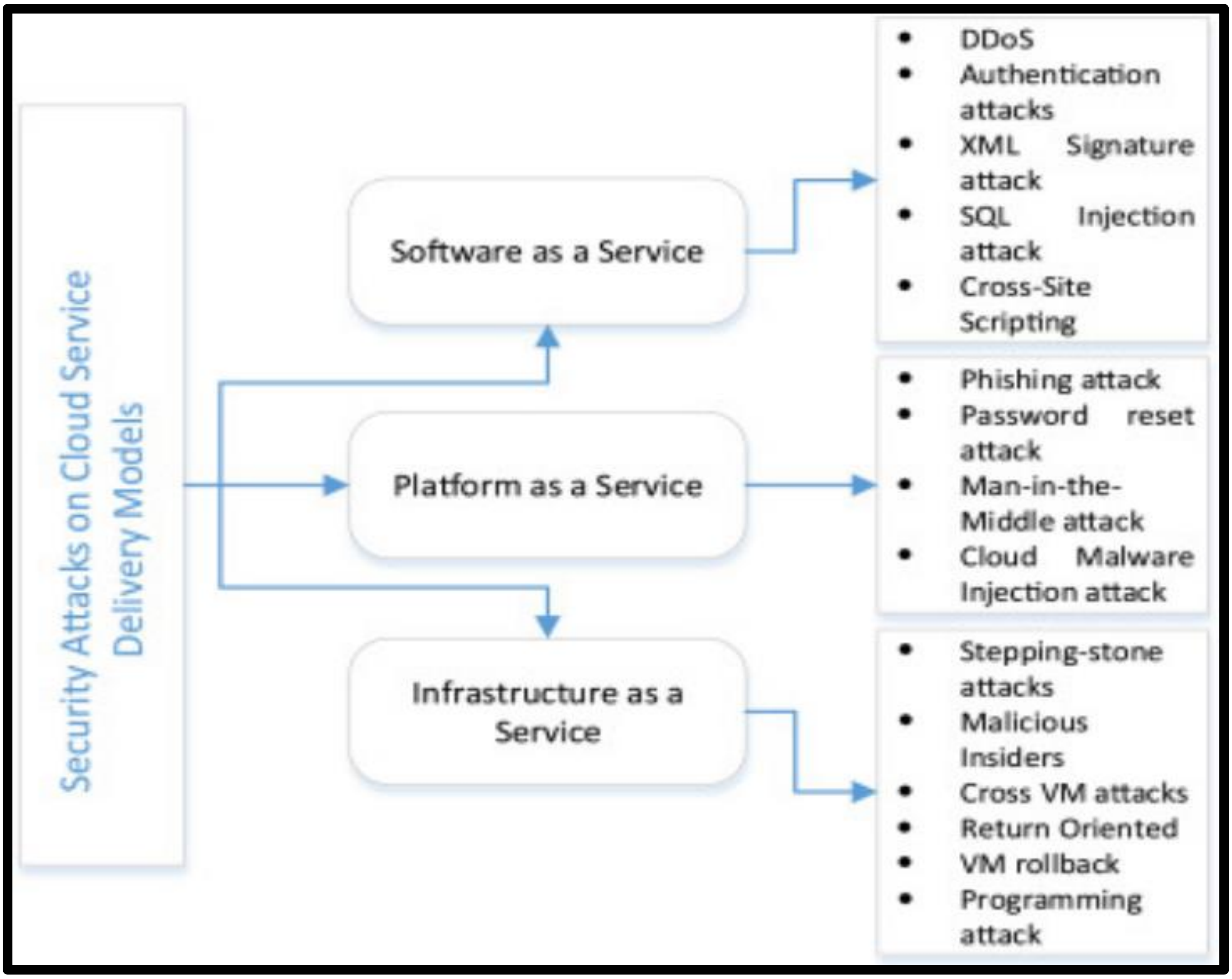

Fig. 5 Security attacks on cloud service delivery models

Security is the very concerning part in the current situation. Fig.5 shows several security attacks on cloud service delivery modes.

Conclusion

Cloud computing marks the commencement of a new stage in the arena of data and communication technology as it carries with it a development pattern which has the possibility to change the way in which computing was done. Owing to this technology, developers with ideas about internet service will no longer need to spend large amounts of currency to structure their program and tools infrastructure capabilities.

References

[1] . Stanoevska-Slabeva K, Wozniak T, Ristol S, editors. Grid and cloud computing: a business perspective on technology and applications.Springer Science & Business Media; 2009 Nov 4.

[2]. Armbrust, M., Fox, O., Griffith, R., Joseph, A.D., Katz, Y., Konwinski, A., Lee, G., Patterson, D., Rabkin, AStoica, I. and Zaharia, M.Above the clouds: a Berkeley view of cloud computing. Technical Report UCB/EECS-2009-28. Electrical Engineering and Computer Sciences University of California 2009.

[3]. Hubbard D, Sutton M. Top threats to cloud computing v1. 0. Cloud Security Alliance. 2010 Mar.

[4].Fan K, Mao D, Lu Z, Wu J. OPS: Offline Patching Scheme for the Images Management in a Secure Cloud Environment. InServices Computing (SCC), 2013 IEEE International Conference on 2013 Jun 28 (pp. 587-594). IEEE.

[5].Takabi H., Joshi J. B., and Ahn G.-J. Security and privacy challenges in cloud computing environments. IEEE Security & Privacy, 2010; no. 6, pp. 24-31.

[6]. Grobauer B, Walloschek T, Stcker E. Understanding cloud computing vulnerabilities. Security & privacy, IEEE. 2011 Mar;9(2): pp. 50-57.

[7].Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generation computer systems. 2012 Mar 31;28(3): pp. 583-592.

[8].Modi C, Patel D, Borisaniya B, Patel A, Rajarajan M. A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing. 2013 Feb 1;63(2): pp. 561-592.

[9].Fernandes DA, Soares LF, Gomes JV, Freire MM, Incio PR. Security issues in cloud environments: a survey. International Journal of Information Security. 2014 Apr 1;13(2): pp. 113-170.

[10]. Ali M, Khan SU, Vasilakos AV. Security in cloud computing: Opportunities and challenges. Information Sciences. 2015 Jun 1;305: pp.357-383.

[11].Ashish Singh and Kakali Chatterjee, Cloud security issues and challenges: a survey, Journal of Network and Computer Applications,http://dx.doi.org/10.1016/j.jnca.2016.11.027