American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-8, Issue-10, pp-165-175
www.ajer.org
Review Paper Open Access

Cloud Computing Security Challenges and its Potential Solution

Ahmad Waleed Salehi, Fakhruddin Noori, Raisa Saboori
Master in Computer Science, Shoolini University, Himachal Pradesh
Corresponding Author: Ahmad Waleed Salehi

ABSTRACT:*Cloud computing in present days is a developing and fast growing technology which is being used in many areas now a days around the world. It provides computing services based on demand and pay per use via the internet that access to a pool of shared resources, without physically acquiring them. The main feature of this technology is that the user does not need to worry of any setup of costly computing infrastructure and that saves cost and time for any organization. due to the scalability and availability of its services. Irrespective of its many advantages, the transformation of local computing system to a virtual computing environment also bring many security challenges and issues with it for both parties the consumer and service provider. The aim of this article is to provide a brief overview of cloud computing technology, the current and future trends of this technology, what services provided by the CC, security issues and challenges, Attacks on the Cloud Computing.*
KEYWORDS *Cloud Computing, Cloud Computing Architecture, Cloud Security, Challenges and Issues in Cloud Computing, Security Measure in Cloud.*

Date of Submission: 20-10-2019 Date of acceptance: 03-11-2019

I. INTRODUCTION

Cloud Computing(CC) in present days is a developing and fast growing technology which is being used around the world. In the past the data stored in hard drives on a computer when the cloud came this technology replaced that hard drive. It is a new and emerging idea that uses virtual computing service through the internet or network on demand to access various shared resources namely servers, storage, interfaces, networks, services, and application which can deploy, allocate or reallocate computing resources dynamically and manage, monitor the usage of resources all the time. CC is basically a distributed architecture which is the combination number of technologies, including multi-tenant application hosting, memory management, transaction management, resource scheduling, server virtualization, data access control etc. the three main concept of this technology are storage, processing and transferring of the information on the infrastructure (providers), which is not in the control policy (customer).

The most widely used definition of the cloud computing model is introduced by NIST as "a model for enabling convenient, on-demand 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"[1].

Cloud computing provides the facility to access the resources from anywhere, anytime online. It also provides flexibility in terms of usage in context to the price paid by the user. This allows it to be used by various industries, like health care [2], banking, companies, organizations, social network [3] and education [4]. An example of this technology like Some businesses may have very few customers to begin with, which may grow exponentially as the service offered become more interesting like in the case of Instagram [3], which is turned to Cloud Computing in order to deal with their growing data, handling of those data and to have better scalability. Just a few months later Instagram was handling millions of regular users. And like this many companies transformed their business to cloud computing.

There are many companies which are providing cloud computing services, for example, Google's Gmail which is a cloud computing provider. Other examples like Amazon, Microsoft which are vendors providing the facilities of cloud computing services and resources to the customers that they can use those services based on their needs or demands which are pay per use. With cloud technology companies are able to utilize the services which are managed and control by third-party companies. It increases the IT functionality and capacity of companies with the use of cloud computing companies need not worry about setting up new

infrastructure or investing in additional training and adding software, personnel.

So with all these features of Cloud Computing there are many security threats exist such as network illegal invasion or attack or denial of service attack and also some specific cloud computing threats like virtualization vulnerabilities, side channel attacks and so many other abuse of cloud by attackers can happen which is a very big concern in cloud it is actually a big issue to all users of cloud if there is no security then the sensitive user data will not be safe. In CC there are certain important services and models which are working behind the scene that makes the cloud computing feasible, controllable and accessible to its end users. Generally, there are three deployment models such as Public Cloud, Private Cloud and Hybrid Cloud the deployment model is actually describe the type right to use to the cloud, like how a cloud can be located. And also there are three service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), the service model it is actually being the reference models in which the Cloud Computing is based. Then discussed all these models and their security issues and go through some of the security threats which are associated with CC, other privacy issues, then identifying different attacks based on its service layer. And also see better strategies for data protection. Finally, we have proposed a mechanism from cryptographic algorithms for the purpose of data protection.

Cloud Computing or Cloud Apps are becoming an essential part of the businesses it has lots of advantages such as cost-effective, agility and speed, remote access, improved productivity, better collaboration. Some popular cloud service providers are discussed in the following.

There are some common cloud service providers:

Amazon Web Service (AWS) it is from Amazon that provides on-demand cloud computing service platform to the users. It provides wide set of infrastructure services like computing, database storage, networking, power, bandwidth and etc. by using these services, users can build their own applications that scalable and flexible. Today AWS provides a secure, scalable, low-cost infrastructure platform and reliable to the business in different countries around the world.

Google Cloud Platform this platform provides cloud services for the users where they can host their programs, google cloud platform makes it possible for startups, individual developers, businesses to run their software on Google's cloud infrastructure. It has many online cloud applications such as Google Docs, Google Slides, Google Sheets, Gmail and so on.

Microsoft Azure it is a cloud computing service which is created by Microsoft, it also provides a wide range of cloud services to the consumers including that computing, storage, analytics and networking. Users can choose and pick from these cloud services in order to run their existing applications in the public cloud or to develop new applications.

The contrast among these providers in the context of Public Cloud where Amazon Web Service has a significant head start on the others [5], where the two other providers Google Cloud Platform and Microsoft Azure are far from out of the competition. The core computes service of Amazon is EC2 (Elastic Compute Cloud) which allow the individuals to configure virtual machines using custom or pre-configured. Where Google Cloud Platform is having GCE (Google Compute Engine) for its computing cloud services. It allows users to configure virtual machines like AWS. And Microsoft Azure enables users to create a virtual machine using VHD (Virtual Hard Disk). And these cloud service providers offer many services different from one another including Database and Storage, Networking, Compute that is mentioned briefly in the above. The following figure shows a general view cloud computing services with three common providers.

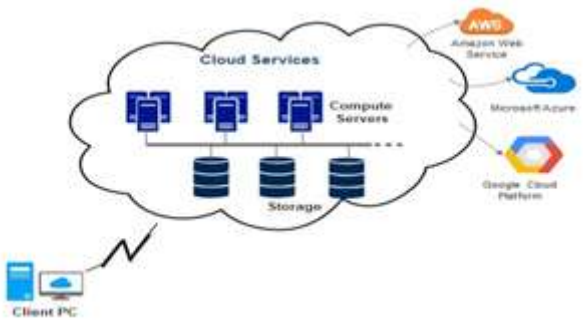

Fig.1. Cloud computing building blocks

II. CLOUD COMPUTING BUILDING BLOCKS

Cloud Service Models:

Cloud Computing is on-demand service delivery model which provide us computing capabilities as much as we want per requirement automatically and this service delivery system is utilized through different devices, machines such as laptop, desktop, PDA, mobiles, tablets etc. Cloud Computing is based on service models; the basic cloud service models includes the following:

Infrastructure as a Services (IaaS) This model provides access to important resources such as virtual machines, physical machines, virtual storage. Infrastructure as a Service provides virtual machines and other basic storage and computing capabilities as a standardized service over the internet or network. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). In this model the subscriber or the user completely outsource the resources and storage, such as hardware and software which they need. They are all controlled through API service. Like it includes Terre mark Enterprise Cloud, Amazon EC2, Windows Live SkyDrive and etc.

Advantage of IaaS Solutions

- The services are pay per use; users can pay what service they want.
- Cost saving while IaaS model has lower infrastructure costs.
- Scalable and flexible the resources can be scale up and scale down quickly based on user's requirements at any time.
- Access to a pool of resources or infrastructure and high availability.
- Better on business growth.

Platform as a Services (PaaS) it allows customers to develop new applications using APIs deployed and configurable remotely, it includes the development, design and hosting of new applications. Users can purchase the platform to access, enabling users to deploy their own application and software in the cloud. The platforms offered include development tools, configuration management, and deployment platforms. Examples are Microsoft Azure, Force and Google App engine [6]. In this model, the Platform as a Service provider gives authority to the user or subscriber ate the component level access so that they can develop and operate cloud applications as per requirement over the internet or network. The security problems caused by data sharing and multi-tenancy has to be taken care by both the cloud user and the cloud provider.

Advantage of PaaS Solutions

- Organizations need not to care about the underlying infrastructure they can easily focus on their development.
- Update or upgrade are not required for the infrastructure software. Where the provider of PaaS handles all updates or upgrades and routine maintenance.
- Lower cost, PaaS reduces organizational costs where companies do not have to make an investment in hardware and software. PaaS platform provides tools to develop, test and host applications.

Software as a Service (SaaS) SaaS is software which is provided by the provider available on demand pay per use through the internet or computer network and it is configurable remotely. It allows us to use software applications as a service to end users. Example, Google apps (Email, Games, Google Docs) which are accessible via different devices such as computers, laptops, smart phones etc. another example of SaaS is Office 365 which is provided by Microsoft and this application offer an online platform including Word, PowerPoint, Excel and these are available through internet web and mobile applications. In this model, the provider gives the authority to the user or subscriber for accessing both resources and applications. it provides the facility to the user to install all the necessary software on cloud so they can access the software by all types of their personal devices through the internet connection or network. The SaaS provides a standard Integrated Development Environment (IDE) to its client to access the applications and transfer the data and applications to a remote storage server through on-line software services [7]. It helps in reducing the effort of installation and maintenance of complex software, as one can essentially get it from the Internet. Furthermore, it liberates the user from intricate programming and equipment management [8].

Advantage of SaaS Solutions

- Accessibility of applications is from anywhere via different devices connected to the internet.
- Rapid scalability of resources depending on service requests.
- Remove infrastructure concerns the users do not have to worry about the infrastructure of SaaS that is handled by the provider.
- Data is secure and it provides a package of support and maintenance

NO	Layers	Examples of each Architecture
1	Client	Users: Computers, Mobile, Operating system, browsers and other electronic devices.
2	SaaS	Software as a Service: Salesforce, Facebook, Google apps.
3	PaaS	Platform as a Service: Force.com, Google app engine, Microsoft Azure.
4	IaaS	Infrastructure as a Service: Amazon EC2, Windows Live SkyDrive

Table 1. Basic layers of cloud computing

Cloud Deployment Models:

There are four different cloud deployment model that is Public cloud, Private cloud, Hybrid cloud and Community cloud. the deployment model is actually describing the type right to use the cloud.

Public Cloud: public cloud allows system and services to be easily accessible to the general public and the services on the public cloud are made available to the general public or a large number of group. Although the data is owned by an organization selling the cloud services, it may be controlled and managed by a third party beyond the vendor firewall. This type of cloud is completely managed and hosted with all responsibilities of management, installation, maintenance, and provisioning. Consumers are only paying for the resources they want and the use. Its benefits are cost-effective, reliability, flexibility and so on. Examples of this type of cloud include Google App Engine and Microsoft Azure.

Private Cloud: private cloud also identified as an internal cloud. It allows system and services to be accessible within an organization only consumers who belong to the same organization which is the owner of that cloud can access to its resources and can access services, it is only operated only within a single organization. However, it may be controlled and managed internally by the organization itself or by the third party. Its benefits are high security and privacy, more control, cost and energy efficiency.

Hybrid Cloud: the hybrid cloud is a mixture of public cloud and private cloud. Non-critical activities are done or performed using public cloud while the critical activities are perform suing private cloud. It benefits are scalability, cost efficiency, flexibility, and security.

Community Cloud: it is one of rarely offered cloud deployment model, where many several organizations shared the infrastructure for the shared purpose and which is managed by them or the services provider. it is based on some agreement among related organizations such as educational organization or banking. Facebook is an example of a community cloud.

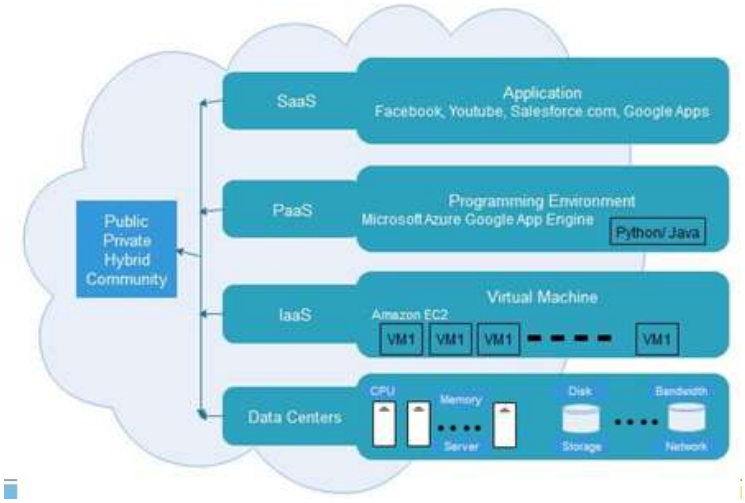

Fig. 2. Cloud computing architecture

III. TRENDS AND ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING

Based on cloud computing definition there are ten essential characteristics of cloud computing. So it is understandable that are the main characteristics that are highly considered in cloud computing.

- **Agility:** agility cloud works in the distributed fashion and It shares the resources among the users and its performance is very fast.
- **On-demand self-service:** the services which are provided by the cloud computing providers enables the consumers on demand the provision of cloud resources. Users can access cloud services through the internet.
- **Rapid Elasticity:** the cloud computing provides the scalability and flexibility or the services of cloud computing is elastically provisioned so that the customer can extend by adding new services as per they need or they can remove also.
- **Reliability:** in the cloud area the availability of servers is very high and more reliable because chances of failure of infrastructure are minimal. In case any of any failure in one of the servers there will always a backup of that data in another server. Cloud environment ensure the high reliability of the service. A reliable system always tries to do not deliver results that include uncorrected or corrupted data.
- **Multi-sharing:** with the use of cloud computing multiple users can work very efficiently. the cloud provides the feature of multi-tenant which enables the users to share computing resources in a private or a public cloud. In which each tenant's will be invisible to other tenants.
- **Maintenance:** it is stress-free to maintain the cloud computing applications, since they do not need to be installed on each user's machine. The service providers are responsible to do the maintenance activity whenever its required so the client does not worry about anything they can just using the platform.
- **Low cost:** by using cloud computing the cost will be reduced because to take the services of cloud computing, IT companies do not to set its own infrastructure. Perhaps, it is one of the most significant advantages of cloud computing while savings in IT Costs of companies. Many businesses nowadays moving towards cloud computing they can save large capital costs over reduction in spending on infrastructure, physical components, equipment. This is the benefit of cloud computing which allows renting more processing power through the internet without investing lots of money on machines or systems as servers.
- **Virtualization:** Cloud computing makes the facility to user to get service from anywhere, through any kind of device. Users can attain or share it safely through an easy way, anytime, anywhere1. Virtualization allows the physical resources by multiple users or consumers it creates virtual version of resources or devices such as servers, network resources, and storage devices. So it plays an essential part in the cloud deployment.
- **Measured service:** Cloud computing technology is affordable in which the consumer can access the cloud services and for whatever the services consumer used they need to pay for it. And it can be checked from both party including consumer's sides and provider's side, therefore, it improves transparency.
- **Broad Network Access:** the resources which are hosted in the cloud can be accessible or available to access from different types of devices, such as mobiles, laptops, tablet, etc. all these kind of devices from wherever they get connected to the internet or a simple network access point they can access broad networks. So it is very useful in businesses, employees can stay active and connected with projects, contracts and customers during their work time and even in off-times.

Current and Future Trends:

This technological trend is generally known as cloud computing it provides a better solution to the current and future information and communication technology desires. Also, we can address the most Internet Future trend is a combination of CloudIoT the integration of these two represents the next rise into the future [9]. With the systematic growth and the future CC Trends, the new opportunities are rising for the professionals of the cloud.

Distinction among IaaS, PaaS and SaaS:

IaaS offers to user's access to computing resources and scalable environment with high flexibility and control over it. While PaaS provides a platform for fast developing, designing and deploying applications by automated infrastructure and management. No need to install and run any program on different devices, SaaS makes it possible and provide applications which are accessible to users online via the internet. The bellow figure identifies all accessibility to the services for the user.

IV. SECURITY CONCERNS IN CLOUD COMPUTING

Security is measured as one of the most critical parts in everyday computing and it is not different for cloud computing because of the sensitivity and importance of information or data that stored on the cloud. In cloud computing, the consumers are unaware of the exact place of their sensitive data, because the Cloud Service Providers maintain data centers in geographically distributed locations causing number of security threats and challenges as compare to the traditional security methods or techniques like firewalls, host-based software (antivirus) and intrusion detection systems (IDS) do not offer suitable security in virtualized systems because of the rapid spread of the threats via virtualized environments [10]. however, cloud computing significantly benefits an organization, but cloud computing carries along itself concerns over the security which is a big issue for the organization. As we know cloud computing has three models by which these three models are SaaS, PaaS and IaaS which provide different types of services to the end users. IaaS is the foundation of all cloud services, with PaaS built upon it and SaaS in turn built upon it, in which these service models also place a different level of security requirement in the cloud computing environment [11]. Various security concerns in cloud computing have given in the following table.

Various Security Concerns in Cloud	Descriptions
Virtual Machine Security	As far as IaaS is using the concept of virtualization so it is a big issue in case of security[12].
Data Security and Data Integrity	It refers to the security of data and the data integrity is the foundation to offer cloud services such as IaaS, PaaS and SaaS. So the data must not be modified or lost by an unauthorized person.
Data Location	Servers stores the data in the cloud
Data Availability	It is the term in which the service provider of the cloud must ensure the availability of the data to be available at any time.
Data Transmission	Transferring the data in the cloud, and the cloud providers should maintain the security of data while transmission.
Access to Servers	Accessibility of the servers remotely through the internet.
Access to Applications	Accessibility of the customers to applications.
Security Policy	Cloud provides a broad range of security policies in order to protect the virtualized environment.

Table 2. Security concerns in cloud environment

And we have considered some of the most common distinct security considerations for cloud-based services and service compositions include the following [13].

- Shared and virtualized resources the services physical infrastructure, can be shared among several tenants.
- Data privacy where the data is being lay on in the vendor's data Centre.
- Multi-tenancy the service hosting processes and the exchanged data are managed and executed in shared environments.

It is also possible that the data of organizations may be stored with the data which is in a shared environment with their competitor's and if there is any bug in the execution environment of vendor's, isolation of processes can be breached which may result in stealing of data. Basically in cloud storage environment, the users store their data in the cloud storage and there is no longer possess the data locally. Therefore, the accuracy and availability of the data files being stored on the distributed environment (cloud servers) must be guaranteed.

Although virtualization and cloud computing can help companies accomplish more by breaking the physical bonds between its users and the IT infrastructure, heightened security threats need be overcome so that benefit fully from this new computing model or paradigm [14]. With the cloud computing environment, you will lose control over physical security. In a public cloud deployment, you are actually sharing computing resources with other organizations. In a shared pool of resources outside the enterprise you even don't have the knowledge of where the resources run. In simple word since you share the environment in the cloud space, you may place your data at risk and it will be very risky to your sensitive data. To ensure data availability, confidentiality, and integrity(CIA), the service or storage provider must provide capabilities that, at a minimum, include a tested encryption schema to ensure that the shared storage environment protects or safeguards all data; stringent access controls to prevent unauthorized access to the data; and arranged data backup and safe storage of the backup media [14]. Therefore, security and privacy issues related to these systems so the network that interconnects these systems in a cloud environment has to be ensured about its security. In figure 5 we have shown 4 layer of cloud with its security level.

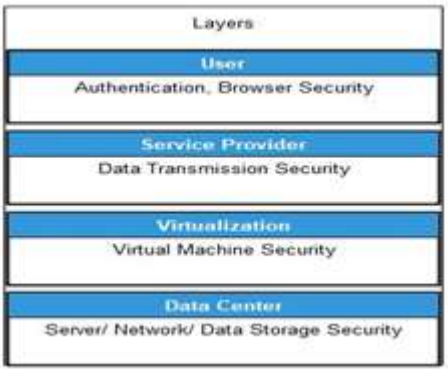

Fig. 3. Security architecture of cloud layers

In cloud computing the security issues can be categorized into the following three broad classes:

1- Common Attack Vectors to Cloud

These security issues are Virtual Machine(VM) level attacks, vulnerabilities associated with CSPs, or phishers and vulnerabilities in the hypervisor or VM technology used by CSPs are a possible threat to cloud security [15]. Basically providers of cloud use virtual machines and a hypervisor to separate customers and cloud providers use sophisticated monitoring tools like firewalls to alleviate the virtual machine level attacks.

2- Cloud Data availability to User

Here, concerns Centre on critical cloud applications and data being available to users. Here, keeping the cloud system uptime, 'Distributed denial of service (DoS)' attacks avoidance and robustness of computational integrity are major issues [15].

3- Legal Issues Related to Data Control

In cloud computing the data of the user is stored on the cloud which means the storage of data may be held by many parties. Here, a potential lack of control and transparency exists as the legal implications of data and applications being held by a third party are very difficult and it varies according to country rules and regulations [15]. According to the SPI service delivery models, deployment models and essential characteristics of cloud, there are security issues in all aspects of the infrastructure including network level, host level and application level. The cloud security architecture as shown in Fig. 2.

4- Denial of Service (DoS) attacks

In DoS attack the hackers or attackers attempt to overload a cloud system with sending excessive messages or requests so that prevent the other users to request hence made inaccessible or unavailable the resource to its intended users. Some Cloud Security Alliance has said that vulnerability of cloud for DoS is more while it used by many users or consumers which cause it much more damaging. And it has many types.

1) An attacker can overload a system with so much amount of junk data that waste and consume the resources and bandwidth. For example, ICPM flood which also known as a ping flood, SYN flood and etc.
2) An attacker can perform DoS attack by making an HTTP request with the large amount so that cannot control by the server, for example, XML DDOS attack, HTTP DDOS attack.

Solution for DoS attacks:

On the basis of authorization, we can classify the traffic for preventing DoS attack. So we can allow those traffic that is authorized and block those traffic which are not authorized. A firewall is used very well in case of that is on the basis of access protocols, IP Address which allow or deny the traffics. We have listed practical solution and techniques of preventing these attacks, decreasing their impacts.

- Firewalls implementation
- Network monitoring
- Traffic encryption

5- Cloud Malware Injection Attack

Malware injection attack is an attack where an attacker attempt to inject a malicious service or virtual machine in to the cloud system. An attacker creates its own malicious service module (SaaS or PaaS) or instance of a virtual machine (IaaS), and attempt to add or inject it to the cloud system. So that appears a valid service among the other valid service implementation instances. If this type of attack happens or attacker succeeds the cloud system automatically redirects those request which is coming from a valid user to a malicious service

implementation, and then the attacker service implementation starts and execute. And the purpose of this attack is depends on the attacker interests it can be a modification of data, full functionality changes, or blockings.

Solution for cloud malware injection attack:

We can maintain some kind of information of platform type version so that a customer uses to access the cloud system in the first stage when a customer opens an account so they can use that information which we maintain in order to check the validity of the customer of the new instance.

6- Authentication Attack

One of the weak point in cloud computing which is often targeted by the attacker is authentication attack. As we can see today every service still using the simple username and password type for authentication but some of the organization, financial institutions in which they have potential information they are using some different sort of authentication like site keys, shared secret questions and etc. which makes it very difficult for different kinds of attack. The following are the authentication attacks:

1) Dictionary attacks: it is a type of attack which is used to break password-based security systems, in this type of attack it will go for checking likely probabilities and tries to match and test all possible matches with most occurring words or the higher possibility of matching.
2) Brute Force Attack: in this type of attack, it tries all various combinations of password or and username to break the password. Generally, the passwords are stored in the form of encrypted cypher text so this type of attack is generally going to crack those encrypted cypher text which is actual password.
3) Replay Attacks: it is also known as playback attack, in this type of attack when the attacker eavesdrops on a secure network, intercept it and resends the whole thing or fraudulently delays it.
4) Shoulder surfing: it's a kind of spying in which the attacker covers the person's movements to get her/his password. The attacker detects the user how he/she enters the password. Like looking to his/her finger what keys of keyboard he/she pressed.
5) Key loggers: key loggers are the programs that are monitor and capturing each key that a user pressed.

Solutions for Authentication attacks:

Locking accounts, it means accounts become locked after a few unsuccessful login tries which can prevent attackers from checking many passwords in a sensible time.

7- Man-In-The-Middle Attack (MITM)

In cryptography a man-in-the-middle attack is one where the attacker relays on communication between two parties and it appears for both parties and thinks that we are communicating directly and normally. So that the sender can't recognize that on the receiver side is an unknown person trying to access or modify the data and that modified message or data will retransmit to the receiver. Therefore, the entire communication is under the control of the attacker. Some type of this attack are as follow:

1) ARP (Address Resolution Protocol) Communication
2) DNS Spoofing
3) Session Hijacking

8- Malicious Insider

According to survey in 2016 a malicious insider is one of those high threats, which can threat an organization and the threat can be former employee, current employee, contractor, or any other business partner who had or has authorized access to an organization system. a determined insider can find more ways to attack and cover the track in a cloud scenario [16].

According to the SPI service delivery models, deployment models and essential characteristics of cloud, there are security issues in all aspects of the infrastructure including network level, host level and application level, as shown in figure 4 [17] in Fig. 2.

The third topology that can be used for PV monitoring system is the web based server with a SCADA (Supervisory control and data acquisition) system implemented to monitor the parameters of the system and giving alarms in case of errors occurred. Fig. 4 shows an example of such network. Fig. 5 shows sample of the results of the system for real time data, historical data and alarms.

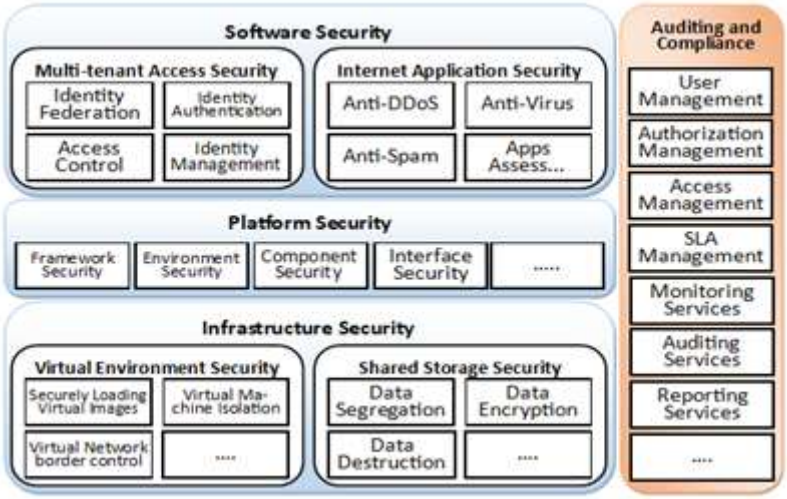

Fig. 4. Cloud computing security architecture

V. PROBLEM STATEMENT

Cloud computing provides services to the organization so that they can use services and the data is going to store in the physical location of vendors out of control of the organization. So the security is playing vital role or this capability of cloud raised the various security issues and questions, for example, confidentiality of the data, integrity, privacy etc. in which every organization needed or demanded a trustworthy cloud computing environment wherein the system or service providers maintain the confidentiality of the data. To induce that type of trust in cloud computing, there is required a system which can perform verification, authentication and encrypted data transmission, therefore that should maintain the confidentiality of the data.

VI. SECURITY MEASURE IN CLOUD COMPUTING

In cloud environment for the security of the data, cryptographic security mechanisms are the best techniques, for protecting data there can be another option which is software encryption, but this method reduces the speed of process which is also less secure. For the security of data during transmission period encryption technique is the best option however there is also the chance of theft of key encryption. In addition, high authentication and data integrity protection should be applied so that it can make sure that your data reach the right place in right from the right path and must not change during transmission. Thus the security is playing a very important role in cloud computing. In cloud computing the security is provided generally by the following services.

- **Virtualization** in virtual environment each tenant might be given a completely isolated virtual environment in orderexecute.
- **Virtual Private Network (VPN)** exchanging of data between cloud provider and the user may be secured by using VPN (Virtual PrivateNetwork).
- **Federated Identity** Federated Identity Federated identity is the ability to port data across security domains using claims and assertions from a digitally signed identity provider [13]. The users who are already authenticated in the organization's the network must be authorized to services of the organization that may be running in the cloud. federated identity service provided this facility, which ties cloud service provider and identity management of the organization together.
- **PolicyServices**Policy Services Defines policies that make an assessment to decide which cloud service provider to choose to depend on factors like security, reliability, etc. [13].

Using the RSA algorithm along with Digital Signature to improve data security in a cloud computing environment, the security of the data, files system, network traffic, host security, backup of data. So here we are proposing an idea of RSA algorithm with Digital Signature, in order to encrypt the data while transmission of data over the network. A digital signature assurance the authenticity of an electronic message or document to provide proof that the document or message is unmodified and original. it is a mathematical scheme for providing the authenticity of digital documents or messages. A valid digital signature gives a receiver a very strong reason to believe that the documents or message was created and send by an identified sender, and during transmission the messages were not altered. And the RSA algorithm is one of the asymmetric cryptography algorithms. Where asymmetric refers that in this type of cryptographic algorithm two different key is used,

Public Key and Private Key. Wherein the public key which is given to anyone and keeping the key private that is a private key. this algorithm is most widely used for securing the data during transmission. The cloud is the complete potential of being top computational technique and is yet to be realized. In future, we feel that state-of-art cryptographic mechanisms and electronic audit will play a vital role in cloud security and have much scope of work and research by academia [15].

Example of the RSA algorithm with Digital Signature is described in some steps of implementation.

1. Suppose John is the sender and Khan is the receiver so a document is taken from the cloud by John and John wants to send that document to Khan.
2. Then the message digest will generate by crunching the document into few lines using some Hash function like (MD5, SHA). used to validate the integrity of the data (i.e. to guarantee that a message has not been altered with, after it leaves the sender but before it reaches the receiver [18]. (Figure 1)

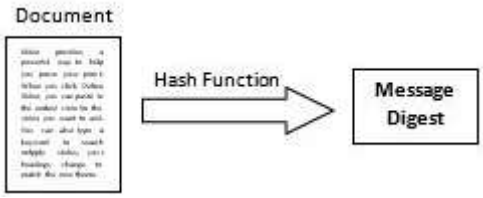

Fig. 1. Message digest process

3. John encrypt the message digest using his private key. Which result or produce the digital signature. (Figure 2).

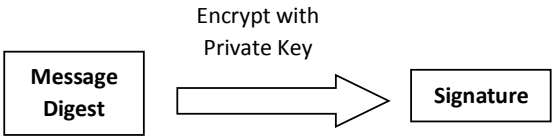

Fig. 2. Message digest process

4. In the last step John uses RSA algorithm in order to encrypt digitally signed signature with Khan public key then the receiver decrypt the decrypted form of text in to the readable form by using his private key and for the verification of signature Khan public key is used.

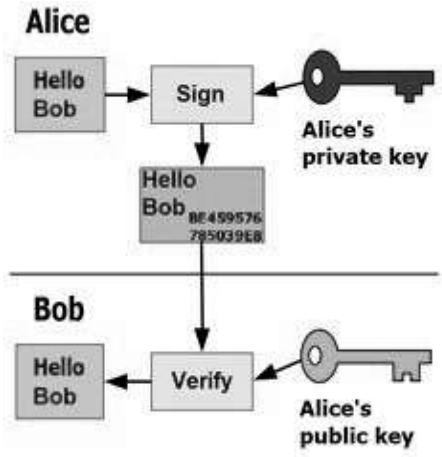

Fig. 3. Encryption of digital signature

VII. CONCLUSION AND FUTURE WORK

Cloud computing model is the newest technology in the computing world. And it becoming most popular nowadays where today small and medium business companies are realizing increasingly that simply by tapping into the cloud area they can achieve fast access to best business applications or drastically enhance their infrastructure resources. Although cloud computing brings a lot of advantages to any organization or company, there are still so many problems that need to be solved and they also need to carefully and know the security

measures which is provided by the cloud service provider. but the best usage of the model we need to remove the current security issues in cloud computing. Based on the above elements which we have described related to the security of the cloud. and we used two cryptographic algorithms RSA algorithm and Digital Signature in order to enhance the security which we have discussed.

Hence in the cloud the security threats are more complex rather than a normal computer network. So It is also depending on the developer side they have to be very cautious about the security of the data. Therefore, every technology has its own pros and cons just like in the case with cloud computing. So the data should be secure in the cloud and the cloud providers should also focus more and more on the security of the cloud which is provided to the customer. This model improves operational efficiency and also reduces costs to customers by streamlining applications maintenance and support to providers.

Future Work Direction:

Since cloud computing is one of interesting technology for businesses. they have to take part in tackling the security genuine issues of cloud computing, mainly protection and security challenges of cloud data (cloud servers) and cloud consumer (cloud clients). There are various models or techniques and various computations for data security, data integrity, data availability, securing those data from being misused, security examination thus on. So we think the need to distinguish these security issues related researches and ways to encourage researchers to identify or detect the research areas in which the new approaches or proposals are projected to characterize the security issues for cloud computing.

REFERENCES

[1]. M. Al Morsy, J. Grundy, and I. Müller, "An analysis of the Cloud Computing Security Problem," ResearchGate, no. December, pp. 7[1] M. Al Morsy, J. Grundy, and I. Müller, "An an, 2010.
[2]. E. Ekonomou, L. Fan, W. Buchanan, and C. Thüemmler, "An Integrated Cloud-based Healthcare Infrastructure," 2011.
[3]. R. Narendula, "Amazon Web Services?: a Case Study Course?: Business Process for IT Services 2012 , EPFL," pp. 1-9, 2012.
[4]. R. R. Chowdhury, "Security in Cloud Computing," vol. 96, no. 15, pp. 1-18, 2014.
[5]. F. Shahzad, "State-of-the-art Survey on Cloud Computing Security Challenges , Approaches and Solutions," Procedia - Procedia Comput. Sci., vol. 37, pp. 357-362, 2014.
[6]. P. Realizzate et al., "Conducibilità elettrica, utile monitorarla nel digestato," pp. 12-16, 2014.
[7]. A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," J. Netw. Comput. Appl., vol. 79, pp. 88-115, 2017.
[8]. P. Barrow, R. Kumari, and P. M. R, "Security in Cloud Computing For Service Delivery Models?: Challenges and Solutions," vol. 6, no. 4, pp. 76-85, 2016.
[9]. C. Stergiou, K. E. Psannis, B. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," Futur. Gener. Comput. Syst., 2016.
[10]. C. Applications, Cloud applications 7. 2018.
[11]. P. Partheeban and V. Kavitha, "A study with security concerns in service delivery models of cloud computing," Int. J. Appl. Eng. Res., vol. 10, no. 21, pp. 42219-42230, 2015.
[12]. H. Wu and C. Winer, "Network Security for Virtual Machine in Cloud Computing," no. 60803057, pp. 18-21, 2009.
[13]. K. Chadha and A. Bajpai, "Security Aspects of Cloud Computing," Int. J. Comput. Appl., vol. 40, no. 8, pp. 43-47, 2012.
[14]. U. Somani, K. Lakhani, and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing," 2010 1st Int. Conf. Parallel, Distrib. Grid Comput. PDGC - 2010, pp. 211-216, 2010.
[15]. R. S. Nejkar, D. V. Patil, and V. S. Patil, "Security aspects in Cloud Computing," Annasaheb Dange Coll. Eng. Technol., vol. 1, no. 6, pp. 1-7, 2013.
[16]. G. Ramachandra, M. Iftikhar, and F. A. Khan, "ScienceDirect ScienceDirect ScienceDirect The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017) A Comprehensive Survey on Security in Cloud Computing A Comprehensive Survey on Security in Cloud Computing," Procedia Comput. Sci., vol. 110, no. 2012, pp. 465-472, 2017.
[17]. D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 1, no. 973, pp. 647-651, 2012.
[18]. S. Deb, "A Message Digest System Using Key Concept and Modulus Operations," vol. 77, no. 9, pp. 30-35, 2013.
[19]. "File_Private key signing."

Ahmad Waleed Salehi" Cloud Computing Security Challenges and its Potential Solution" American Journal of Engineering Research (AJER), vol. 8, no. 10, 2019, pp 165-175