Computing, Information Systems & Development Informatics Journal
Vol. 10 No. 2, June, 2019 - www.cisdijournal.org

Cloud Computing: Security Issues and Challenges Overview

[1]Akanji, W. [2]Abodunrin, G. & [3]Akerele, J.
[1]Department of Computer Science, Lagos State Polytechnic, Ikorodu, Lagos, Nigeria
[2&3]Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria
E-mails: akanjiwasiu2005@yahoo.com; gbengabodunrin@gmail.com; akerele.adennis@gmail.com

ABSTRACT

The Cloud computing today, is one of the branch of IT that is growing at a very fast pace in the network-based technology. This involves linking a large number of computer systems together to provide optimized application technologies used in data and file storage. The Cloud computing works on the principles of pay as you use, an approach where users don't pay for systems, installations and for maintenance. Once any client subscribed to a Service Provider, the client will be able to access freely the services required from cloud as the need arises anywhere in the world on demand basis. Today, in spite of all the benefits that comes with cloud computing, many businesses and organizations are still not willing or reluctant in accepting this technology. Security challenge is a critical factor that is hindering the wider acceptance of using this technology. Releasing of client important data to third party in the cloud can be challenging due to fears of the data being manipulated, theft and the like. This paper gives an overview of issues relating to security challenge that has affected the effective utilization and deployment of cloud computing services. Also, to describe the models for cloud computing and the distribution of cloud computing services.

Keywords: Cloud Computing, Cloud Service Provider, Security, Businesses, Data, Distribution, Services.

CISDI Journal Reference Format
Akanji, W. Abodunrin, G. & Akerele, J. (2019): Cloud Computing: Security Issues and Challenges Overview. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 10 No 2, Pp 111-122. Available online at www.cisdijournal.org.
DOI Affix - https://doi.org/10.22624/AIMS/CISDI/V10N2P9

1. INTRODUCTION

National Institute of Standards and Technology described cloud computing as a paradigm for fast tracking, timely network accessibility to computing devices across wide area network coverage. For examples, software, storage, networks and deliverable services, which can be accessed easily with minimal intervention from the service provider [1]. One of the fastest emerging network-based technologies is Cloud computing, where individuals and businesses use cloud services daily activities in one way or the other without really realizing it, like the use of drop box, yahoo mail and Gmail etc. Many benefits are derived from using cloud services, among which are on-demand accessibility, digital storage of files, wider geographic coverage, reduction in cost of infrastructures for NGOs, private businesses, government, Educational Institutions, hospitals and others.

However, cloud computing is characterized with several issues which include but not limited to data security, lack of resources and expertise in spite of all the merits discussed above. Looking at all the challenges, data security seems to be the most challenging according to IDC report (2009). This paper looks at the data security issues associated with cloud computing. This paper is structured according to the following. Section 2 discusses the existing security research in the cloud, section 3 presents the cloud computing model and distribution of services, section 4 provides an overview of data security issues and approaches to challenges. Section 5 discusses future cloud computing issues.

2. LITERATURE SURVEY

Some proposed methods for addressing security issues in cloud computing have been looked at in the literature survey. Popovi and Hocenski discussed the issues relating to security, its requirements as well as challenges faced by cloud service providers during cloud engineering [4]. Behl looked at the security issues relating to the cloud environment. He also looked at current security measures and their limitations in securing the infrastructure and applications on the cloud [5]. Sabahi discussed security issues, reliability, and cloud computing availability. He has also proposed a viable solution to certain security problems [6].

Mohamed E.M et.al gave a data security model for cloud computing in line with the cloud architecture report. They also introduced tools to enhance the cloud computing Data Security model [7]. Wentao Liu presented some cloud computing systems and analyzed its security issues in and its approach in accordance with the rationale of cloud computing [8]. Mathisen, E, addressed some of the key security threats that cloud computing is likely to face, as well as existing implementations that address these shortcomings [9].

3. CLOUD COMPUTING MODEL

Cloud Computing is a technology maintain applications and data by using central server and the internet. Google services are typical example of Cloud Computing. Without the use of server or software users are able to use the cloud services. These Services are completely managed by the Cloud Provider [2].

3.1 Cloud Computing Characteristics

Cloud model consist of the five characteristics discussed below;

Self-service on Demand. The provision of cloud services such as web applications, storage, processing power, server time and networks can be done automatically without any human interaction if needed by the consumers [3]. Wide connection to network. Standard mechanisms that facilitate the use of multifaceted client platforms (e.g. IT gadgets such as android devices and PCs) are available and accessed over the network [1].

Pooling of Resources. Cloud computing resource providers are pooled by deploying a multitenant model to serve multiple consumers, with different resources being dynamically assigned or reassigned based on consumer demand. This is irrespective of customer's location or service provider but may be able to specify location at a higher level of abstraction (e.g. region, state, or datacenter). These resources are storage, bandwidth compression, memory, and network [1].

Simple Elasticity. This is an important feature if the usage experience of an application increases. This does not always have to be fully automated, but if you've expected heavy usage it should be relatively easy to provide additional servers. You can select a base server plan and a payment model to deal with increased demand [4].

3.2 Service Models

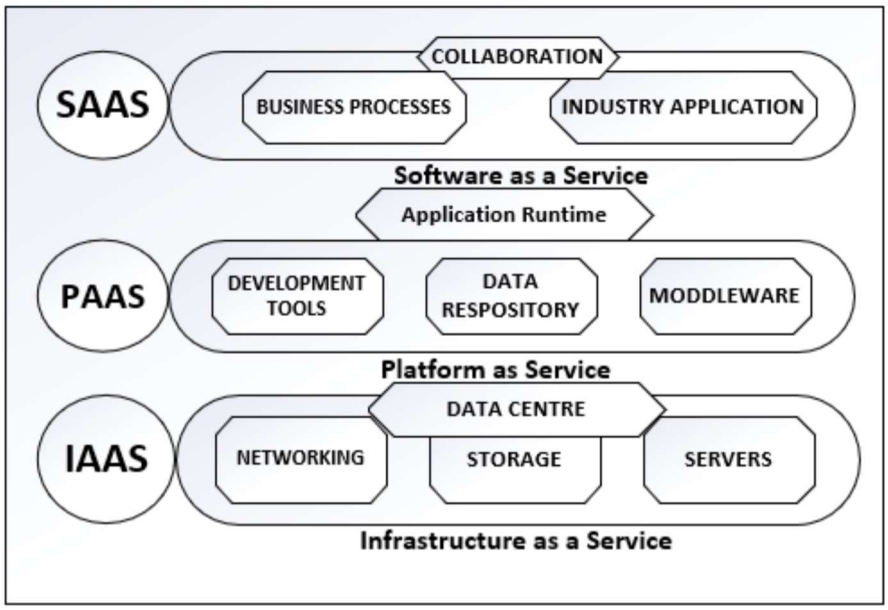

Figure 1: Cloud Service Delivery Model

Measured Service (Pay-Per-Use)–The services used are closest to monitoring and tracking to ensure that there is complete transparency in the cloud provider to resource and deployment customers. The user pays only for a number of resources they use, and is always made aware of any resource anomalies, fluctuations or irregular behavior [4]. In Cloud Computing there are three different service models, which are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) respectively. These service models are completed by end users' layer which encapsulates the end user perspective on the cloud services being provided.

Software as a Service (SaaS). This service allows customers to use cloud-based software directly without the need to install it on their devices. The software can be accessed via the user interface (e.g. e-mail) or the application interface from various clients ' gadgets. The user does not own a cloud system, i.e. servers, networks, operating systems, storage, etc. and may exempt from a limited specific setup of user software [1].

Platform as a service (PaaS). This is a set of development and software tools hosted on the servers of the provider. It is one step below SaaS and restores everything from middleware, operating systems, etc. It provides a built-in system in which developers can press their apps without having to worry about what's happening under the cloud. It provides developers with a service that provides a complete software development life cycle involving planning, design, implementation, implementation, testing and maintenance. Besides that, every other aspect from the developers is abstracted. The cloud platform works similarly to IaaS as a subscription layer which offers an extra rent fee. Customers using PaaS systems transfer costs from capital to operating costs, but they must take into account additional restrictions and perhaps other lock-in thresholds posed by additional layers of feature [6,7].

Infrastructure as a Service (IaaS). The IaaS is one single tenancy cloud layer, which provides a pay-per-use fee to dedicated cloud facilities of the cloud supplier. The cost of providing hardware as cpus, computers and networking devices is greatly minimized by this. This is generally not feasible because it is possible to add or remove computer resources much quicker and more affordable than in an internal data center or with a co-located service [8,10].

3.3. Deployment Models

Cloud service can rely on the organization's nature and need for use in different ways. Models used include private, public, mixed and collective cloud.

Private Cloud. This software is offered by a company or a chosen service provider and provides the elasticity and the flexibility of the cloud computing platform for a single-tenant environment. The physical infrastructure may be part of an organization and operated by the company or service provider selected to extend the organization's management and safety control aircraft [11].

Community Cloud. A particular set of users from joint organizations (e.g. strategy, security requirements, purpose and compliance) are able to make exclusive use of the cloud infrastructure. It may be owned, controlled and maintained by more than one community organization or a third party, or by both the group and a third party, either on or off premises [1].

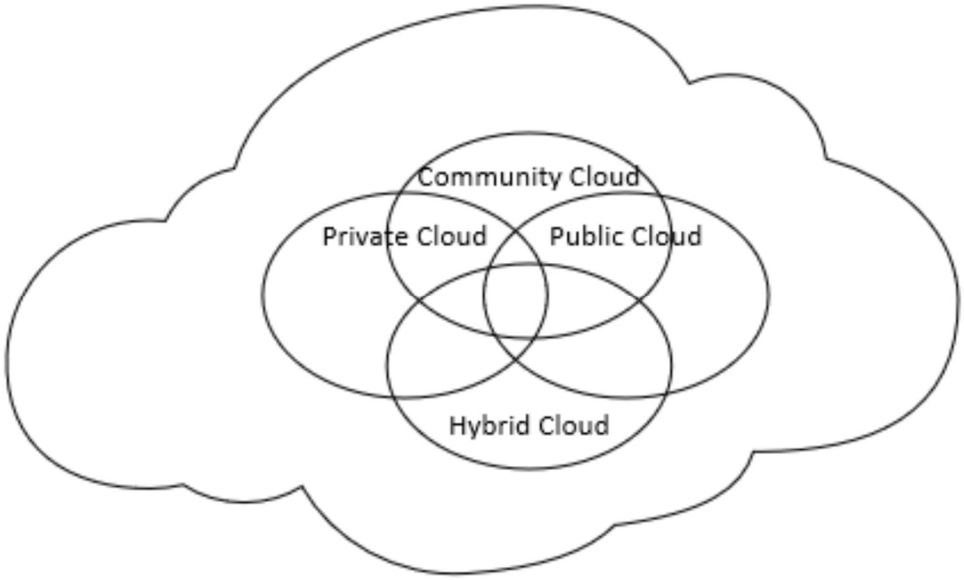

Figure 2: cloud deployment model

Public Cloud. A public cloud is a framework in which users can access the cloud using normal web browsers using interfaces. It is based on a pay-per-use model, similar to a prepaid power measurement or billing system, which is flexible enough to take care of cloud optimization demand spikes. This allows cloud consumers to better match the operating level of their IT costs by reducing their IT infrastructures capital expenditures [8, 9].

Hybrid Cloud. This infrastructure consists of more than one (private, community or public) cloud that retains its features, but is technologically interconnected, enabling data and application portability (e.g., cloud load-balancing) [12,13].

The lack of encryption was the major obstacle to cloud computing adoption. Without a doubt, putting your data on someone's disk and processor, deploying your software, looks risky to many. Threats to the security of the organization's data and software include phishing, data loading and botnet (running on remote machine collection). However, the multi-tenancy model and the pooling of cloud computing resources have created new security issues which require innovative technology. For example, Cloud is used by hackers to build botnet as it provides them with a comparatively cheaper option for secure network resources to launch an attack [9]. Cloud protection is a set of guidelines, enforcement and technology based on regulation, designed to protect cloud-related applications, data and resources. Cloud is used by many companies and related data providers Become a contract priority for adequate security and potentially vulnerable areas. The major problems of shared resources, access control, privacy and identity management are cloud computer security [14]. The following are some of the concerns:

The cloud service providers, employees and contractors can deliberately breaching data confidentiality which results in data security risk.

- Service providers may wrongly modify Cloud-based and are also vulnerable to accidental loss.
- The data may be accessed through insecure API in public network
- The cloud resources are naturally shared among different clients that may be attacked.

However, data security is quite challenging in fact. The safety concerns are addressed briefly in this section:

1. Cloud Storage Security: The acceptance and use of cloud storage facilities has improved over time, causing both the cloud providers and customers many security challenges. IT consultants to warn that even virtual or physical any relatively technical one carries an inherent risk once file-sharing and cloud storage mal-processes are introduced. As a result, customers are not able to keep their information within the cloud, they are passed over to a third party, meaning that the confidentiality of information is beyond the remit of a service provider or business [15]. Customers must ensure service consistency and cloud storage security. The security concerns regarding storage include data leakage, BYOD, snooping, cloud credentials and key management.
2. Cloud Infrastructure Security: Cloud Computing permits the scattered workforce and provides clients with many advantages. It is imperative to learn how to route a cloud infrastructure which ensures secured service deployment, data storage, communications and safe management operations [21]. The rapid implementation of cloud services has resulted in new obstacles to issues (privacy, confidentiality and reliability). The compliance standards, laws, and procedure of the organization’s cloud infrastructure at the device, server and network levels typically are defined by information security practitioners.
3. Software Security: During the entire development process (i.e. from concept to production [16], cloud providers must defend their applications against both internally and publicly threatened threats. Instead of introducing other risks, the security process and software policies should be defined. Both cloud providers and clients are faced with these challenges. Through incorporating glitches, design flaws, overflow buffers, error handling arrangements, program protection can be handled or overcome.
4. Cloud Network Security: It is the responsibility of one cloud service provider to accept legitimate network traffic only and ban all malicious traffic. Server vendors are not used to connect server VMs to their manufacturer network, as are access routers and switches. Consumer affected internal network attacks, including 1) confidential information was not available; 3) access denial or failure. (2) unwanted modification. Network protection has challenges which is both internal and external, since an intruder can theoretically approve it from a separate part of the network. [16].

3. ISSUES OF SECURITY IN CLOUD COMPUTING

The cloud services systems use the Cloud or the internal network to run on the cloud infrastructure. The faith principle can be applied to as clients pledge the ability of the firm to provide reliable and accurate services. Confidence in focused on the chosen models of application delivery in which applications are assigned and outsourced to the owner's power. Confidence in traditional architecture has needed an efficient and effective security strategy to cope with the technical shortcomings and flows between them [16], [17]. Outside mechanisms bypass the limits on the accessing or monitoring of customer data by targeting services. The group or collective clouds govern the entity to whom the cloud technology belongs in the cloud computing architecture models. When the digital cloud is implemented, management helps the network owner to specifically enforce the appropriate safety policies that guarantees adequate safety operations that reduce hazards and risks. Cloud protection is primarily related to the stability of the owner's computations network and facilities. Within the organization the private cloud infrastructure is managed and operated, there are no additional security problems, so the company retains confidence. It is understood that the transition of data or any entity or network affiliation to the international company opens up possibilities of unlicensed access to information services. [18].

Cloud computing permits the owner of the infrastructure to run, deploy and develop tools that can work effectively without any issues as regards the locations and properties of the primary infrastructure. When data are stored or private data of different companies are transferred and services are gotten from the cloud service owners by accessing the internet resources, there will always be security issues and the privacy of the data involved. In other to secure Cloud Information Systems (IS) which is to identify the threats and the challenges and to be attended to through the implementation of the required countermeasures. In Cloud Computing infrastructure risk assessment will be required in areas like data integrity, data privacy, auditing, reliability and accessibility of data. In general, protection includes important aspects of privacy, secrecy and access to the appropriate security network. In order to secure data, hardware and software, these key safety aspects are needed. In addition, the Trusted Third Party (TTP) discusses cloud computers by allowing trust and encryption [18].

The cryptography is used by trying to address the security vulnerabilities to ensure that the data are authentic, confidential and integral. Customers with unique quality, operational and ethical characteristics are trusted by third parties or cloud providers and contain minimum risk factor acknowledgment. TTP in the IS which offers modular, standard based, end-to-end security services for the different administrative areas, specialty areas and regions. TTP is the optimal protection facilitator in the hybrid cloud environment. Customers or systems belong to different domains without mutual knowledge, so safe interactions are necessary. The following are key safety challenges for the cloud computing infrastructure:

A. Integrity

There is need to ensure prevent unauthorized modification or loss of data. This is usually done by a third party. Hence, there is always the need for integrity. When data is being managed by a third party, then the issue of integrity becomes very paramount. Cloud computing data protection conserves data stored on the cloud server in other to validate that the data has not been not altered or destroyed through the use of third party services. In other to prevent unauthorized access to databases and data integrity, companies will achieve greater confidence [19]. We have greater visibility for those systems in order to determine what information or data can alter or adjust the structure which may influence its credibility. Authorization device is used in the determination of the system level of access to a defined authorized clients should have in other to protect resources controlled through the system. Authorizations are necessary in order to

ensure that only legitimate users can connect or communicate in the cloud-based ecosystem because of the increasing number of access points and customers.
Securing the data includes three key entities; (1) Cloud Storage Service (2) The data owner (3) Data integrity inspector. The auditor may be the data controller or a third party may be responsible [20]. The integrity of the data scheme cycle is described in two steps; which include the preprocessing stage that comprises preprocessed data and some additional metadata that have been generated. During the test process, the auditor submits an application that has problem to the Cloud storage provider which produces data and metadata and sends them to the auditor. The early discovery of any loss of data or manipulation through the use of programs that test the integrity of the data and steps required to recover data.

Computation efficiency: The data can be preprocessed into the cloud storage system, while waiting to be outsourced. Metadata abstraction gotten from big data are sent to the cloud server's storage. This method creates an overhead which reduces performance. While preparation for small data sets does not affect the efficiency of the computation. However, usage of big data sets has an important effect. At the end of the server, the cost to calculate the possession limit of evidence on how the customer can check or ensure the integrity of outsourced data on a regular basis [21]. Primitives are used as metadata for data integrity techniques affecting the calculation of duration.

Efficiency of communication: The communication effectiveness of the data integrity scheme has three main aspects:
1. The data proprietor must face a challenge in order to demonstrate possession.
2. The cloud server storage must respond to a challenge in order of possession for verification to take place.
3) The overhead can take place during the initial metadata transfer. The overhead of complex knowledge exchange comprising of upgrade authentication.

Security: The concerns emerging from the fact that data are vulnerable to various attacks during the implementation of data integrity schemes [25], [27]. The ability of a malicious cloud storage provider to tag forgery attempts, attempting to hide customer data breaches to bypass the audit test, is addressed using the following methods.

- The cloud service provider counters the attack to destroy data by creating legitimate proof of ownership with tags that can fully erase the original data.
- In the replace attack, the cloud provider replaces the data blocks of deleted or corrupted pair and respectively tags using another valid pair as the response of challenge with that deceive the verifier.
- The contamination attack determines the correct information to be used in the development of an answer to a question by a deceptive computer, but it creates distorted or worthless blocks during repairs.
- The retrieval of the data stored by a wiretapping perpetrator during the data leak assault.

Data integrity mechanisms may not be simple or the manipulation of the information may not be detected in due time leading to unrecoverable harm. The cloud provider ensured consistency with completeness of the results. Numerous vulnerabilities including multiple intruder assaults on device attributes are clarified by the advent of cloud technology. Intentionally or unintentionally, the integrity of software safeguards it from malicious modification. Cloud service providers provide a series of API or web interfaces to facilitate the integration of cloud services to the user of the services provided. In fact, the reliability of cloud services is concerned with the protection of the app, as the malicious user may gain access to and either erase or tamper with customer information [28] [29]. It is responsible for maintaining the quality of software by the developer or device owner. In order to reach the cloud provider and protect the hardware underlying the production, modification and theft, network and hardware integrity is needed. The key task of keeping data integrity is to provide the cloud service prototypes (IaaS, PaaS and SaaS) with the ability to process data massively. Data storage challenges in the cloud are enhanced if the capacity of the Solid-State Drives (tapes or hard disks) is increased and cannot match the growth of data. The vendors must thus increase their storage by increasing the storage space of solid disk space (hard drives, tapes) and thus either corrupting or losing data, drive or node failure

may be a consequence. In fact, the efficiency of the solid-state disk decreases more and more, though data access cannot be any quicker.

B. Confidentiality

They want to protect secrecy of customer data in the cloud computing environment so that it can only be available for the approved customers and systems [30]. Cloud computing (applications and the necessary infrastructures) mainly includes additional threads on systems in public clouds or applications as compared with the host of private data centers. Therefore, a growing number of applications, customers and technological improvements are the vital requirement as far as keeping customers data secret is concerned. Cloud computing companies are widely involved in two fundamental approaches, for example encryption and physical isolation, to secrecy [31]. Cloud computing provides public network infrastructure and resources and is not segregated physically. The network of virtual LAN and middle boxes should be used for virtual physical isolation, including packet filters and firewalls. Cohesive FT's VPN cubed provides a safety limit for IT systems in the single, multiple, or hybrid cloud data centers. In order to secure the servers and deploy them at Amazon EC2, Vertica offers VPN and a firewall. It allows customers to have full access to a secure system. We establish a VPN connection with business customers, and Vertica is linked to the cloud case. Confidentiality is also improved with encrypted data and TC3 is successfully applied to the solution before transition to cloud storage. There have been many concerns about the security and privacy of applications, the diversity and the reminisce of data [32].

1. Data Remanence: The data will be reflected in the residual data, which can be lost or removed unintentionally because various users are not segregated from hardware and physical drives on a cloud infrastructure are literally isolated, which may unintentionally lead to the exposure of private data application
2. Security and Privacy: The protection of data is related to user authentication. Protecting the customer's account against hackers is a great problem in controlling access to software, devices and memory objects. The electronic screening maintains the customers ' trust. If the customer uses flawed account security, unauthorized cloud access can result. The customer had to focus on the software that the company that manages and holds customer data in a secure way in the cloud computing world. Unauthorized access through the use of sensitive applications or weak identification that pose a privacy and confidentiality issue
3. Multi-Tenancy: Multi-tenancy is the common characteristics of cloud infrastructure. The memory, data, programs and networks are included. The business model of cloud computing is like multiple customers using the same common resources at the client level, host level and network level. Multi-tenancy is analogous to multipurpose jobs, which share common computing tools such as CPU, and is connected with challenges to data confidentiality and privacy.

C. Availability

Including software and their resources, cloud computing is available to ensure approved clients are always able to access the network properties on demand. The cloud computing frameworks (IaaS, PaaS and SaaS) provide clients with connectivity at all levels to resources and software. Cloud machine vendors provide the VM-based cloud platform and services. S3, EC2, which is based on the Skytap VM, are offered in Amazon and Xen offers the virtual lab administration app (Xen, VMware and Microsoft Hyper-V) which depends on a hypervisor. The Xen virtual machine supported by Amazon is able to offer separate storage, virtualization of ram, virtualization of a computer / CPU, etc., for example. Therefore, on the basis of the usage expense in each unit, Amazon providers can split up resources (memory, capacity, saving, CPU cycle) on demand. The cloud vendors offer platforms and VM infrastructures (Skytab, Amazon), but these services are not equal to the network security inspections for mainly cloud companies, providing the ability to filter and block traffic based on port and IP address for secure systems. Cloud merchants (such as Google and Amazon) provides geographic idleness in their cloud and thereby allowing high availability on an individual provider. The cloud system has capacity to carry procedures even when there are possibilities security cracks or

authorities misbehave [33]- [35]. Cloud service displays a heavy dependance on the network and infrastructure resources present at any given time.
The information system architecture validates the uniqueness of many organizations that meet the required shared security parameters and assess the unique data security and data protection standards. The various distributed framework indicates security challenges based on the physical, technological or device level of the user. The main reason for the system safety distributed are given below; To ensure the data confidentiality among the participating systems.

- When physically adding or deleting resources, maintain exactly the same level of security.
- Ensure that no data leakage occurs across systems in the cloud at simulated level during process isolation and processing.
- To maintain or preserve the integrity, such as secrecy and accurate operations of facilities.
- To provide the world of non-open systems with the right secure networks.
- To check different identities of exchanging consumers and, where appropriate, to ensure non-repudiation of the data source and origin for the purpose of banking. To ensure the availability of data or systems communicated among the participating systems.
- Software or data integrity shall be protected by prohibiting any alteration or damage from unauthorized access to participating systems.

D. Trusted Third Party (TTP)

Trusted cryptographic third parties help facilitate interaction between the two parties and review all key activities between them. The cloud computing world has demanded TTP resources to create the fundamental level of confidence, providing an ideal solution for ensuring that correspondence and data are accurate, essential and confidential. TTP may generate a trustworthy security environment with a standard security cap clearly missed. It is an organization which provides confidence in electronic transactions without partiality through commercial and technical security features. [18]. TTP facilities, together with scientific, operational, financial and legal instruments, are manufactured and distributed. This is linked operationally to the trust chain (certificate paths) in order to provide a network assurance to create the Public Key Infrastructure (PKI) framework. PKI provides legally acceptable and technically reasonable methods for applying data integrity, protection, authorization, effective authentication, and non-repudiation. PKI profits from combining the directory with a centralized information system, which contains a number of objects which are hierarchically and functionally ordered with the same attributes.

The Lightweight Directory Access Protocol is a key protocol that supports the Certificate Revocation List (CRL) access of PKI directory services and is used for authentication by web services [36]. User certificate, for example an end-user certificate, must also be acquired by email. PKI is connected to a directory that can be used to distribute: 1) application certificate such as end-user certificate need to obtain using email before the transfer of encrypted message 2) certificate status information (CRL); and 3) private key, If the consumers don't use the same computer each day, the system requires portability. The directory containing the hidden encryption or private key is decrypted with the customer's password on the remote working platform.

PKI is used with the Single-Sign-In (SSO) system which is suitable for cloud computing, where clients work across the multiplicity of cross-cutting boundaries. In the SSO system, the user does not have to enter the password again and again in order to access various services over the network. SSO is used in tandem with PKI that enhances the security and authorization of the entire infrastructure between the obvious technical problems because the reliability is reasonably guaranteed. The following methods can be used by TTP: Client-Server Authentication: The licensing body must validate the organizations or applications involved with cloud computing activities, including the registration of virtual servers, network devices, electronic users and servers and physical infrastructure. For remotely or physically

involved organizations in cloud security protection, the PKI Certification Authority provides the requisite solid certification with specific limits.
The digital signature integrating Ldap and SSO, which allows user versatility and consistency, is the most powerful verification process in distributed environments [37]. Customer authentication is performed with a private key to other users across the network simply and automatically. Cloud computing platform is giant, where each service requires safe authorization and verification. The use of the appropriate SSO approach is crucial among the logical limits of outsourced or own services. Shibboleth is open source middleware which enables SSO to share information such as user and named attributes across organizational boundaries and trust third parties or cloud providers. [38]. Authorization may be carried out without caring about divulging personal information on the resource registry following successful verification in which consumers share their attributes.

Low or high-level confidentiality: Delivery of data throughout the network is a problem because the danger of data disruption or modification continues to rise. Due to the deficiency in conventional physical connections, the complexity in the cloud computer environment increases, so that it requires not only cloud traffic protection but also between the cloud host IPSec, allows you to forward or receive protected packets such as UDP, TCP, ICMP etc. [18], [39]. To order for the client to boost scalability, IPSec can authenticate itself with the PKI certificate through previously issued CA certificates. SSL Protocol allows interface between End-to-End Encoding applications, and TCP / IP protocols allow encoded communication and Client-Server authentication. The unique characteristics of cloud computing include coordination to secure servers, users and host-to-host. SSL and IPSec are selected in this regard on the basis of the security requirements and different criteria.

1) Cryptographic data separation: In the cloud computing world, which is a key element in the effective implementation of the SaaS platform, sensitive data security is essential. Included or protected is the cryptographic technique that is invisible to other entities and protects data privacy, confidentiality and dignity. Cryptographer isolation is disguised or secret. The two encryption methods (symmetric and asymmetric) are used together to provide good performance and date security. [40], [41].

4. CONCLUSION AND FUTURE CHALLENGES

Although cloud computing may be viewed as a new technology that can change our use of the Cloud, a great deal must be safeguarded. Most modern developments grow exponentially, each with technological improvements that promote people's lives. Nevertheless, it is important to note the security risks and challenges presented by these developments. No cloud computing separately. The report discussed the key safety concerns in the cloud. Cloud computing continues to be a pioneer in the development of a distributed, secure and economically viable IT solution.
Mainly the security and privacy of cloud data is an issue. Cloud issues. Data systems such as openness, resource sharing, multi-tenancy, virtualization, Enterprise Cloud Computing and the Cyber Security Agreement (SLA). The paper presents the challenges and methods of data security to solve these issues. loud computing also has developed new technologies, such as container as a service (CaaS), software-defined networking (a concept to build and manage network systems which eliminate applications from the underlying networks), software-specified storage (respects conceptual storage and functionality from the underlying hardware) and Cloud of Things (CoT) (a concept that incorporates cloud computing). These new developments pose new and important challenges in cloud computing. As new technologies emerge, existing security strategies must always be checked to secure and safeguard records.

REFERENCES

1. Peter Mell, and Timothy Grance, "The NIST Definition of Cloud Computing",30-9-13, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909616.
2. Fauzi the Annual Azila ,Herawan Tutut, Noraziah A. ,Noriyani Mohd .Zin , On Cloud Computing Security Issue, Springer-Verlag Berlin Hiedelberg 2012
3. Olive Christopher, Cloud Computing Characteristics Are Key, White Paper, General Physics Corporation 2011.
4. Carlin Sean, Curran Kevin , International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No.2, June 2012, pp. 59~65 ISSN: 2089-3337
5. Zissis Dimitrios , Lekkas Dimitrios , Addressing cloud computing security issues , Elsevier journal Future Generation Computer Systems 28 (2012) 583–592
6. Global Netoptex Incorporated. — Demystifying the cloud. Important opportunities, crucial choices. ll pp4-14. Available: http://www.gni.com [Dec. 13, 2009].
7. Ahmed E. Youssef, Exploring Cloud Computing Services and Applications, Journal of Emerging Trends in Computing and Information Sciences, VOL. 3, NO. 6, July 2012.
8. A Platform Computing Whitepaper Enterprise Cloud Computing: Transforming IT', Platform Computing, pp6, viewed 13, March 2010.
9. Brodkin J, 2008, _Gartner: Seven cloud-computing security risks', Infoworld, viewed 13 March 2009, from http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0 .
10. Kuyoro S. O., Ibikunle F. , Awodele O., Cloud Computing Security Issues and Challenges , International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011.
11. Ramgovind S, Eloff MM, Smith E , The Management of Security in Cloud Computing , 978-1-4244-5495-2/10, IEEE 2010.
12. National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.
13. Vemulapati Jyanti,Neha Mehlotra and Dangwal Nitin ,SaaS Security Testing: Guidelines and evaluation framework ,11th annual International Software testing conference 2011.
14. Z. Gou, S. Yamaguchi, and B. B. Gupta., "Analysis of various security issues and challenges in cloud computing environment: A survey," Handb. Res. Mod. Cryptogr. Solut. Comput. Cyber Secur. IGI Glob., pp. 393–419, 2016.
15. T. C. Nguyen, W. Shen, Z. Luo, Z. Lei, and W. Xu, "Novel data integrity verification schemes in cloud storage," Comput. Inf. Sci., pp. 115–125, 2014.
16. C. Eric, D. Chris, E. Mike, and G. Jonathan, "Security for cloud computing 10 Steps to ensure success," Cloud Stand. Cust. Counc., pp. 1–35, 2015.
17. S. Paquette, P. T. Jaeger, and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," Gov. Inf. Q., vol. 27, no. 3, pp. 245–253, 2010.
18. K. Karaoglanoglou and H. Karatza, "Resource discovery in a Grid system: Directing requests to trustworthy virtual organizations based on global trust values," J. Syst. Softw., vol. 84, no. 3, pp. 465–478, 2011.
19. N. Iltaf, M. Hussain, and F. Kamran, "A mathematical approach towards trust based security in pervasive computing environment," Proceeding Int. Conf. Inf. Secur. Assur., pp. 702–711, 2009.
20. S. Rizvi, K. Cover, and C. Gates, "A trusted third-party (TTP) based encryption scheme for ensuring data confidentiality in cloud environment," Procedia Comput. Sci., vol. 36, pp. 381–386, 2014.
21. S. Aldossary and W. Allen, "Data security, privacy, availability and integrity in cloud computing: issues and current solutions," Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 4, pp. 485–498, 2016.
22. F. Zafar, A. Khan, S. U. R. Malik, M. Ahmed, A. Anjum, M. I. Khan, N. Javed, M. Alam, and F. Jamil, "A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends," Comput. Secur., vol. 65, pp. 29–49, 2017.

23. L. Chen, “Using algebraic signatures to check data possession in cloud storage,” Futur. Gener. Comput. Syst., vol. 29, no. 7, pp. 1709–1715, 2013.
24. E. Esiner, A. Kachkeev, S. Braunfeld, A. Kupcu, and O. Ozkasap, “FlexDPDP: Flexlist-based optimized dynamic provable data possession,” Cryptol. ePrint Arch. Rep. 2013/645, pp. 1–40, 2013.
25. G. Ateniese, R. Burns, and J. Herring, “Provable data possession at untrusted stores,” Proc. 14th ACM Conf. Comput. Commun. Secur., pp. 598–610, 2007.
26. Y. Yu, J. Ni, M. H. Au, H. Liu, H. Wang, and C. Xu, “Improved security of a dynamic remote data possession checking protocol for cloud storage,” Expert Syst. Appl., vol. 41, no. 17, pp. 7789–7796, 2014.
27. K. Yang and X. Jia, “Data storage auditing service in cloud computing: Challenges, methods and opportunities,” World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.
28. Y. Zhu, H. Hu, G.-J. Ahn, Y. Han, and S. Chen, “Collaborative integrity verification in hybrid clouds,” Proc. 7th Int. Conf. Collab. Comput. Networking, Appl. Work., pp. 191–200, 2011.
29. S. K. P and R. Subramanian, “An efficient and secure protocol for ensuring data storage security in cloud computing,” J. Comput. Sci., vol. 8, no. 6, pp. 261–275, 2011.
30. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling public auditability and data dynamics for storage security in cloud computing,” Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, 2011.
31. M. Armbrust, A. Fox, R. Griffith, A. Joseph, and RH, “Above the clouds: A berkeley view of cloud computing,” Univ. California, Berkeley, Tech. Rep. UCB, pp. 7–13, 2009.
32. M. F. Mushtaq, S. Jamel, and M. M. Deris, “Triangular coordinate extraction (TCE) for hybrid cubes,” J. Eng. Appl. Sci., vol. 12, no. 8, pp. 2164–2169, 2017.
33. Cloud Security Alliance, “Top threats to cloud computing,” Cloud Secur. Alliance, pp. 1–14, 2010.
34. F. S. Al-Anzi, A. A. Salman, N. K. Jacob, and J. Soni, “Towards robust, scalable and secure network storage in cloud computing,” Proceeding 4th Int. Conf. Digit. Inf. Commun. Technol. Its Appl., pp. 51–55, 2014.
35. K. D. Bowers, A. Juels, and A. Oprea, “HAIL: A high-availability and integrity layer for cloud storage,” Proc. 16th ACM Conf. Comput. Commun. Secur. - CCS ’09, vol. 489, p. 187, 2009.
36. A. Bessani, M. Correia, B. Quaresma, F. André, and P. Sousa, “DEPSKY: Dependable and secure storage in a cloud-of-clouds,” ACM Trans. Storage, vol. 9, no. 4, pp. 1–36, 2013.
37. S. Boeyen and T. Moses, “Trust management in the public-key infrastructure,” Entrust seucring Digit. identities Inf., no. January, pp. 1– 36, 2003.
38. A. Levi and M. U. Caglayan, “The problem of trusted third party in authentication and digital signature protocols,” Proc. 12th Int’l Symp. Comput. Inf. Sci., 1997.
39. M. S. E. H. Tebaa, “Secure Cloud Computing Through Homomorphic Encryption,” Int. J. Adv. Comput. Technol., vol. 5, no. 16, pp. 29–38, 2013.
40. M. F. Mushtaq, S. Jamel, K. M. Mohamad, S. Kamal, and A. Khalid, “Key generation technique based on triangular coordinate extraction for hybrid cubes,” J. Telecommun. Electron. Comput. Eng., 2017.
41. A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi, and H. Sastry, “Security algorithms for cloud computing,” Procedia Comput. Sci., vol. 85, pp. 535–542, 2016.