Indonesian Journal of Innovation and Applied Sciences (IJIAS)
Journal Homepage: https://ojs.literacyinstitute.org/index.php/ijias
ISSN: 2775-4162 (Online)
Research Article

Volume 2	Issue 2	June (2022)	DOI: 10.47540/ijias.v2i2.518	Page: 105 – 113

Cloud Computing and Security

Mansoor Bigdeloo[1*], Mostafa Ramezani[2], Abolfazl Rafat[3]

[1]International Federation of Inventors' Associations (IFIA), Switzerland
[2]Department of Business Administration, Iran
[3]Technical Unit, North Khorasan Towns Company, Iran

Corresponding Author: Mansoor Bigdeloo; Email: ilyacomputer8692@yahoo.com

ARTICLE INFO

Keywords: Cloud Computing, Information Technology, Internet, Massive Data, Security.

Received : 27 April 2022
Revised : 03 June 2022
Accepted : 19 June 2022

ABSTRACT

Following personal computers, one of the most important innovations in the IT industry is cloud computing ad it appeared with the advent of a major revolution in the IT industry. Cloud computing allows organizations to reduce or increase their resources according to operational needs. In fact, cloud computing means the development and deployment of computer technology to provide computational resources through the Internet. Cloud computing is an information space architecture that allows network-based and demand-driven access to a large array of common computing resources at very low cost, high innovation, and development, as well as without spatial and temporal constraints. Cloud computing is one of the most important and powerful tools for securing and managing massive data and allocating resources in the infinity of the Internet.

Introduction

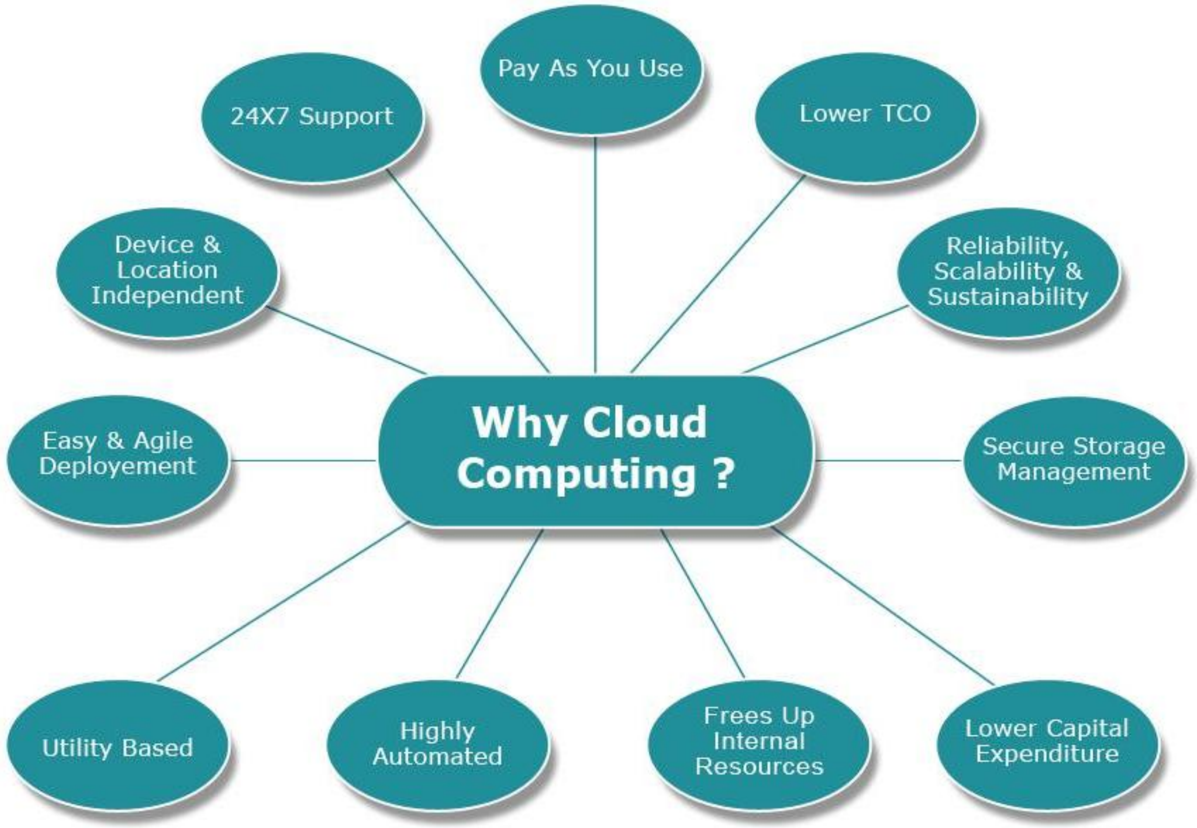
Cloud computing is one of the hottest subjects in today's computer world. Many see the future of the computer in cloud computing, and cloud computing is considered a great strategy to the big problem of speed in computers. Cloud computing is a computational model that emerged in late 2002. This technology is the next generation of computing calculations. Individuals can get whatever they need in the cloud. Cloud is a metaphor for the Internet, based on how it is embodied in computer network graphs, and it is an abstraction for complex infrastructure. This technology is highly extensible and resources can be shared by users. There is no need to install, configure, or specify management for network hardware installation. Cloud allows computing to be much more efficient by concentrating storage, memory, processing, and bandwidth.

Cloud providers have provided customer orders for online ordering and payment through text-based browser applications for the sale of computer tools and the provision of applied services. Hence, one of the most important aspects of cloud computing is e-commerce. The cloud uses virtualization as a key technology. When the end-user sends a request, a virtual machine is created to run the user's specific application. In a host machine, multiple virtual machines can be run to use resources (Spaltro, et al., 2016).

The combination of virtualization technology with cloud computing has become a tradition today. Cloud is a huge container that can integrate various virtualization technologies and applications through the internet. Cloud service delivery models are categorized into three major types: Iaas, pass, and saas. Iaas's delivery model plays a major role in hosting pass, saas, scientific applications, or web applications in cloud data centers. It also provides storage and computing resources for the commercial and scientific use of cloud-based open-source hardware, such as Hadoop, Open Nebula, Eucalyptus, and Nimbus in a dynamic approach. Cloud computing is well developed for HPC applications. HPC applications are mainly focused on scientific applications (Edwards, 2016).

In fact, cloud computing has a three-tier architecture, which in its infrastructure layer, we are faced with resource management in data centers. In the substrate, there are possibilities for developing applications. In the software layer, applications are put to use by the end-user. If we want to improve the way resources are managed in data centers and scheduling tasks, we need to enter the infrastructure layer.

Figure 1. Why Cloud Computing


Pay As You Use
24X7 Support
Lower TCO
Device & Location Independent
Reliability, Scalability & Sustainability
Why Cloud Computing ?
Easy & Agile Deployement
Secure Storage Management
Utility Based
Highly Automated
Frees Up Internal Resources
Lower Capital Expenditure

If we want to work on developing a particular issue publicly, we will enter the substrate, and if we want to focus on how to provide the final service to the user, we need to enter the software layer. With the advancement of IT, we need to do computational work everywhere and all the time. It also requires people to do their heavy computing tasks without having to have expensive hardware and software. Cloud computing has been the latest technology response to these needs. Since this technology is now in its infancy, the definition of a standard scientific that is generally accepted is not yet provided, but most scholars are also in agreement with the definition of this phenomenon. The National Institute of Technology and Standards defines cloud computing as follows: Cloud computing is a model for providing easy access based on the user's demand through the network to a set of configurable and changeable cloud sources such as networks, servers, storage space, applications, and services (which can be accessed or provided free of charge) with the least need for resource management or the need for direct service provider interference (Mell, 2011).

When we save images online to your personal computer or use email services or social networking sites, we actually use a cloud computing service or consider an organization that uses an online payment service as an example instead of paying bills for consecutive years; in fact, it employs a cloud computing service. Cloud computing is a computation carried out by a group of many remote servers that are networked together, leading to centralized data storage and online access to services and resources. To put it simply, cloud computing is the acquisition of computing resources through the Internet, and in practice, instead of keeping your information on your hard drive or updating the applications you need continuously, you use the service on the Internet to meet the needs of the aforementioned needs. Cloud computing is a computational model in which a large number of systems are connected either privately or publicly, to provide dynamic and scalable infrastructure for applications, data storage, and files. With the advent of this technology, the cost of computing, hosting applications, content storage, and service delivery has dropped significantly. The idea of cloud computing is essentially based on the “reuse of technology capabilities”.

Cloud computing can be considered an essential tool for the development and growth of small and medium enterprises. The main reason is that based on this fact, cloud computing, IT, business, and services have changed in which the resources were provided by one or more service providers through the Internet as a distributed service in terms of infrastructure. These services are scalable on-demand, and pricing can be based on payment per use. The following is a good description of cloud computing (Laurie, 2017; Mell, 2011)

LITERATURE REVIEW

Cloud computing follows five basic features (Mell, 2011):

1. Self-service request (subscription): The customer can obtain one-way processing facilities such as server and network storage as needed from any provider automatically and without the need for human intervention.
2. Network-wide access: Facilities on the network are available and can be achieved by standardized mechanisms, supporting mechanisms that are used for heterogeneous platforms for weak and strong clients, such as mobile phones, laptops, and PDAs.
3. Resource-based replication. The supply sources of the processing are used to serve all customers through the multimodal model. It is carried out by various physical or virtual resources that are dynamically retrieved according to the customer's request. The customer usually does not have control or knowledge about the exact location of the resources provided, but may be able to determine the location at higher abstract levels (such as country, province, or data center). For example, resources include storage space, processing power, memory, network bandwidth, and virtual machines.
4. Quick Flexibility (in situ): The facilities can be quickly and flexibly developed to be expanded rapidly (scale-free) to quickly reach a smaller scale. From the perspective of the customer, the facilities available to get access are often unlimited and can be purchased at any time and in any amount.
5. Measured service: cloud systems automatically control and optimize resource use. This is accomplished by utilizing the ability to measure at the level of abstraction appropriate to the type of service (such as storage space, processing power, bandwidth, and active users' number). The use of resources can be monitored, controlled, and reported transparently both for the client and for the provider.

Cloud Architecture

Before we dive into the security issues, it is important to understand the cloud definition and architecture. According to Sharma and Trivedi3, cloud computing is a set of resources that can scale up and down on-demand. It is available over the Internet in a self-service model with little to no interaction required with the service provider. Cloud enables new ways of offering products and services with innovative, technical, and pricing opportunities five major actors influence and are impacted by cloud computing, along with its security implications.

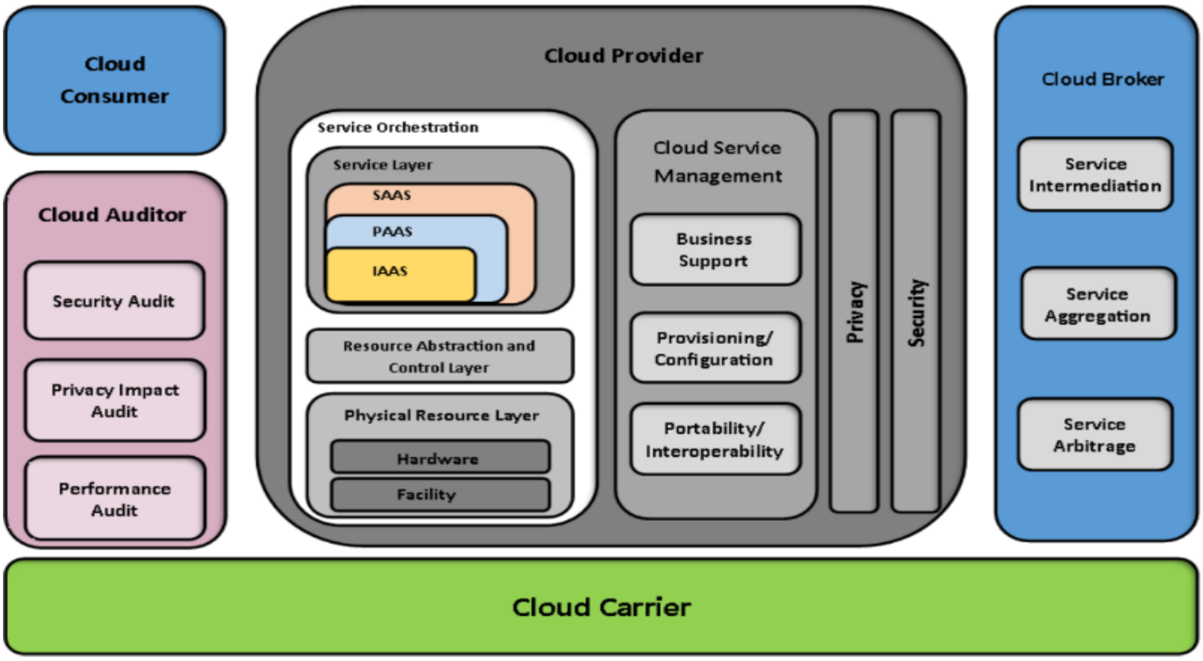
Table 1. Actors in NIST Cloud Computing

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Provider*
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties Cloud Auditor
Cloud Broker	An Entity that manages the use, performance, and delivery of cloud services and negotiates the relationship between *Cloud providers* and *Cloud Consumers*

Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*

The bellow figure is a complete reference architecture for cloud computing. It is important to note that the figure represents an end-to-end reference architecture that addresses all the seven layers of the Open Systems Interconnection (OSI) model, and extends to include the business, commercial, and governance aspects. As it is evident, cloud computing is a comprehensive and complex solution with many areas of vulnerability.

Figure 2. Architecture for Cloud Computing



There are some unique advantages to cloud computing. Some of the key advantages are:

1. Cost of entry for all organizations including small firms
2. Almost immediate access to the resources
3. Reduction in IT barriers to innovation
4. Easy to scale the services
5. Implement and/or offer a new class of application and delivery services.

Cloud computing offers services using the Infrastructure as aService (IaaS), Platform as aService (PaaS), and Software as a Service (SaaS). Cloud users have access to servers and virtual machines through the IaaS service model. The hypervisors execute on the servers to provide virtualization of physical resources. Similarly, using the PaaS service model, the cloud platform provides support for operating systems, runtime systems, databases, or web servers. The SaaS service model provides support for pay-per-use software. The diversity of the service delivery models makes the cloud computing platforms more vulnerable to attacks than any other computing platform. Its vulnerability may be exposed through any of its core components: network, virtual machines, storage, and applications, which are used as a basis for categorization of attack and their implications. For performing comparative analysis, we categorize attacks on a cloud platform based on its components: network (A1), virtual machines (A2), storage (A3), and applications (A4) as elaborated below.

An attack on a cloud may have one or more implications that may deteriorate the provision of data and services on a cloud platform. These implications are categorized as follows:

1. *Violation of data protection*: Data protection is violated when data becomes accessible to users other than owners of data. A large number of threats may violate data protection through different techniques such as data deduplication or third-party clouds.
2. *Malicious manipulation of data*: On cloud computing platforms, the communication

between the user and the cloud services interface involves protocols such as HTTP&SOAP together with scripting languages which are vulnerable to a large number of threats Consequently, an attacker may exploit loopholes in these mechanisms which may result in malicious manipulation of web site data.

3. *Denial-of-service*: An attacker may target the cloud platform to hinder the services being provided to customers. For instance, a malicious insider can occupy the resources so that the requests by other users are responded to with the unavailability of resources.
4. *Theft-of-service*: a few vulnerabilities in the scheduler may result in theft-of-service attacks. For example, an attacker may target the scheduling policy to be able to steal resources or obtain cloud services without proper billing.

A cloud computing platform provides services using its service delivery model. The attacks on a cloud platform may exploit various components at every layer of its service model to violate data protection and deteriorate the quality of service for malicious purposes. This section discusses and analyzes research work contributing toward revealing attacks on clouds and their countermeasures. We have four categories for attacks including network, VM, storage, and application. Through network-based attacks, the botnets have been successful in exploiting the cloud infrastructure for malicious purposes. For instance, the well-known Zeus botnet was revealed to be using Amazon's Elastic Computing Cloud (EC2) as a command and control server The security of a virtual machine being copied to create another VM may be compromised by modifying its executable code. The worms/viruses may be injected into the original VM before creating a copy of the VM Storage services of a cloud make use of data deduplication to keep a single copy of data.

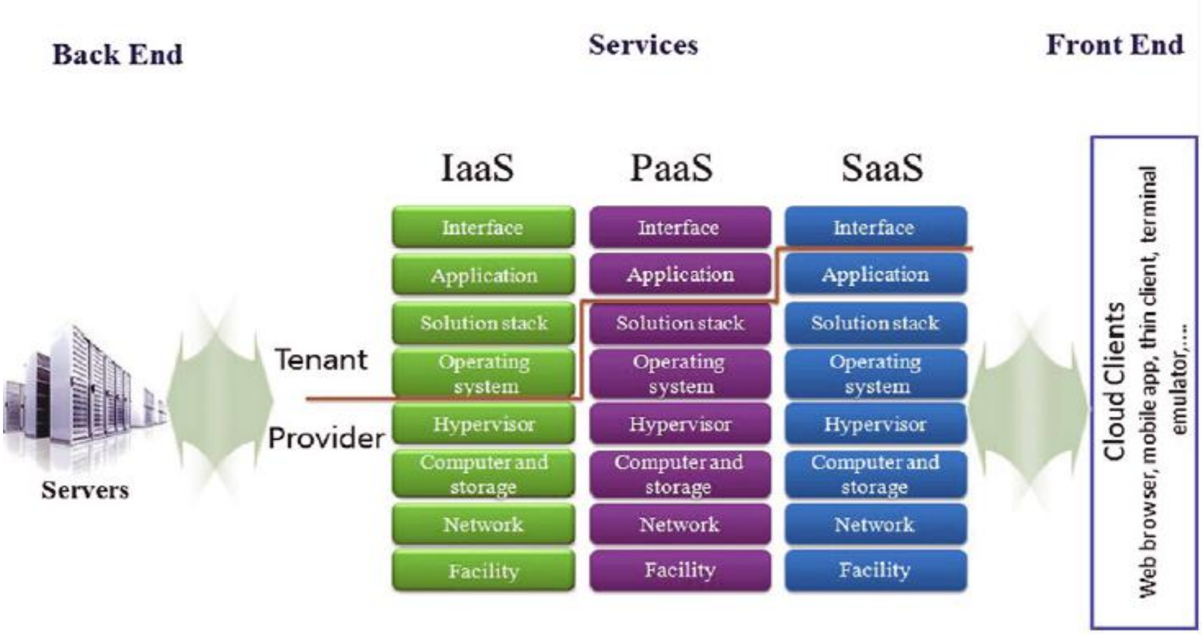
Various security challenges faced due to the elasticity of clouds are described in Owens (2010). The main challenge is the provision for fine-grained access in a cloud environment. Moreover, an anelastic model has to cope with the time and context parameters for restraining various actions. Similarly, the data on a shared architecture may not be secure due to environment access to other users. For steganography attacks, secret data called steganogram can be embedded within normal data exchange which may not be detected by third parties. The secret data may contain malware code which may result in a security breach. For securing cloud computing platforms, the antivirus software may be of great significance as it may monitor and hinder any malicious code to impact the cloud.

Cloud computing implements the virtualization technique is to provide resources efficiently to the end-user. The characteristics of cloud computing include management ability, scalability, and availability. In addition, cloud computing is also economical, on-demand service, expedient, ubiquitous, multitenant, elastic, and stable. Cloud computing offers mainly three service delivery models; Infrastructure as a Service (IaaS), Platform as a Services (PaaS), and Software as a Service (SaaS).

NIST defines a four-development model of the cloud: Public, private, hybrid, and community. Cloud computing uses a cloud server stack where the client or user is on the front end and the server on the backend. Services reside in the middle ware of the stack as shown below. At the top level resides the application, which directly delivers the outsourced software to the client and eliminates sophisticated software. Customers do not need to expend money to install software, only they pay for their usage. NIST is responsible for developing guidelines and standards to provide security in a cloud environment. Here we define the cloud architecture as a fourfold, which is composed of:

1. Cloud computing concept and characteristics
2. Cloud deployed models
3. Cloud service delivery models
4. Cloud security concept

Figure 3. The Characteristics of Cloud Computing



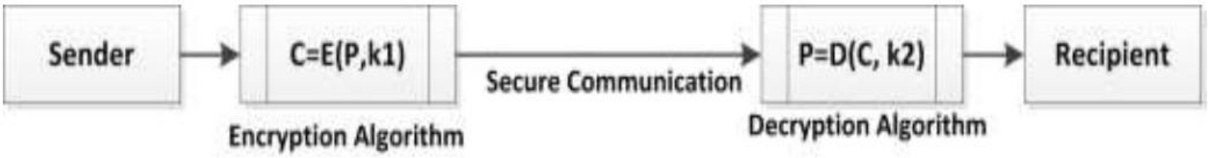
Security Algorithms for Cloud Computing

Imagine two people who share critical secret information have to split up. This requires them to share and communicate their data and information from a distance, even as there lays a threat of an eavesdropper having the ability to stop, interfere or intercept their communications and seeks that same information. They decide to lock their information in a box using a lock that only the other knows the combination to and has the key to open it. The box is locked and sent over to the other user who uses the combination key to unlock the box and read its contents.

In simple terms, Cryptography can be seen as a method of storing and disguising confidential data in a cryptic form so that only those for whom it is intended can read it and can communicate information in the presence of an adversary and the security algorithms mitigate security issues by use of cryptography, authentication and distributing keys securely (Cloud Security Alliance, 2015). Cryptography is thus the science of making data and messages secure by converting the end-user data to be sent into cryptic non-readable form and encrypting or scrambling the plaintext by taking user data or that referred to as clear text and converting it into cipher text and then performing decryption which is reverting back to the original plain text. With this ability, Cryptography is used for providing the following security:

1. Data Integrity: information has value only if it is correct, this refers to maintaining and assuring the accuracy and consistency of data, and its implementation for computer systems that store use data, processes, or retrieve that data.
2. Authentication for determining whether someone or something is, in fact, who or what it is declared to be.
3. Non Repudiation: is the assurance that a party, contract, or someone cannot deny the authenticity of their signature and sending a message that they originated.
4. Confidentiality: relates to loss of privacy, unauthorized access to information, and identity theft.

Figure 4. Encryption and Decryption Process



Cryptography is the science of using mathematics for making plain text information (P) into an unreadable cipher text (C) format called encryption and reconverting that cipher text back to a plain text called as decryption with the set of Cryptographic Algorithms (E) using encryption keys (k1 and k2) and the decryption algorithm (D) that reverses and produces the original plain text back from the cipher text. This can be interpreted as Cipher text C = E {P, Key} and Plain text C = D {C, Key}

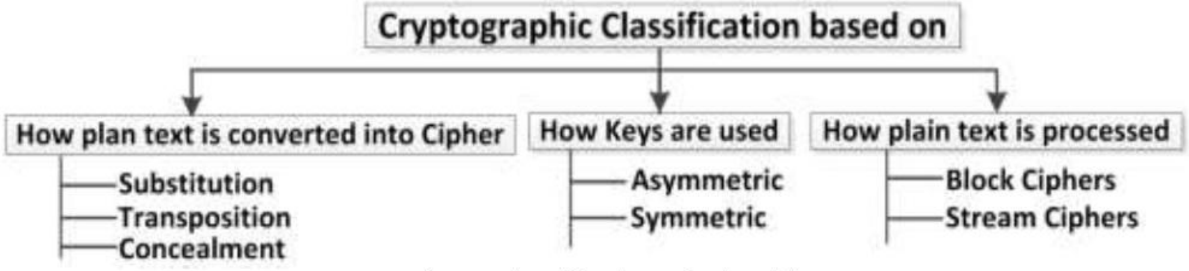
1. The plaintext is the original intelligible source information or data that is input to algorithms.
2. Cipher text is the scrambled message output as a random stream of unintelligible data.
3. Encryption Algorithm substitutes and performs permutations on plain text to cipher text.
4. The decryption Algorithm is encryption run in reverse by taking the secret key and transforming the cipher text to produce the original plain text.
5. Keys are used as input for encryption or decryption and determine the transformation.
6. Sender and Recipients are persons who are communication and share the plaintext With respect to Cloud computing, the security concerns are end-user data security, network traffic, file systems, and host machine security which cryptography can resolve to some extent and thus helps organizations in their

Reluctant acceptance of Cloud Computing

Various security issues arise in the Cloud:

1. Ensuring Secure Data Transfer: In a Cloud environment, the physical location and reach are not under end-user control of where the resources are hosted.
2. Ensuring Secure Interface: integrity of information during transfer, storage, and retrieval needs to be ensured over the unsecured internet.
3. Have Separation of data: privacy issues arise when personal data is accessed by Cloud providers or boundaries between personal and corporate data do not have clearly defined policies.
4. Secure Stored Data: question mark on controlling the encryption and decryption by either the end-user or the Cloud Service provider.
5. User Access Control: for web-based transactions (PCI DSS), web data logs need to be provided to compliance auditors and security managers. Security Algorithms are classified broadly as:
6. Private Key/Symmetric Algorithms: Use a single secret key is used for encrypting a large amount of data and are have a fast processing speed. These algorithms use a single secret key that is known to the sender and receiver. RC6, 3DES, Blowfish, and 3DES are some prime examples of these algorithms. Public Key/Asymmetric Algorithms: Use a key pair for the cryptographic process, with the public key for encryption and the private for decryption. These algorithms have a high computational cost and thus slow speed if compared to the single key symmetric algorithms. RSA and Diffie Hellman are some types of public-key algorithms.
7. Signature Algorithms: Used to sign and authenticate use data are single key based. Examples include RSA and DH.
8. Hash Algorithms: Compress data for signing to a standard fixed size. Examples include MD5 and SHA.
9. Some other ways of classifying Algorithms based on their processing features as below.

Figure 5. Classification of Algorithms


Cryptographic Classification based on
How plan text is converted into Cipher
Substitution
Transposition
Concealment
How Keys are used
Asymmetric
Symmetric
How plain text is processed
Block Ciphers
Stream Ciphers

Background

The basic concepts of cloud computing date back to the 1960s. This concept, which was presented by John McCarthy, the founder of AI, was later explored further. Cloud computing will be organized as a public utility In 1966, Hill Douglas

Park in a book titled as "The Problem of the Public Computer Industry" pointed to issues such as the illusion of unlimited access, elastic procurement, the provision of facilities to the public through private, governmental and associative services. But the words that were used in the 1960s did not have the concept of the cloud today, and it was literally used as a public industry. In 1969, the idea of a galactic network or an intergalactic network that is now called the Internet came up by J.C.R. Licklider and after a while, the American Research Institute developed the ARPANET network to allow anyone to access programs and information from across the network. In the 1970s, virtualization software, such as VMware, were introduced and they were able to put multiple operating systems in a host operating system and serve each one individually.

The first known definition of cloud computing was done in 1997 by Professor Ramnath Chlapapa in Dallas. "A computational instance where the maximum computational power is located will soon be beyond the frontier of the economy and will not be able to calculate alone, and it must pass through technical constraints", he said in a speech. To put it simply, it's easier to say that he meant some processes are currently out of the responsibility of a server in some software and services, and the processor's ability to process is not more than that and there must be several servers to process and deliver services. In the late 1990s, a company called Salesforce.com began operating and its field of activity was the transformation of comprehensive applications for organizations into the web. The company's activity was a start-up for organizations to focus their activities on a platform (Internet)by software. Cloud computing technology peaked in the 2000s. Where in 2003 Xen developed the Virtual Machine Monitor software.

This system allowed a large number of guest operating systems to run on multiple servers and use shared server resources. So far, we've outlined how to form some services over the years, and by putting together this puzzle, you'll find out what the idea and technology of cloud computing is all about. In 2006, Amazon Company modernized its Datacenter and it is one of the first companies which expands cloud computing to today's concept so other companies such as Microsoft and Google can tend to cloud computing. At first, Amazon introduced its cloud service, Elastic Compute Cloud, which allowed its users to use their software on servers. After a while, Amazon established a service called Simple Storage Service to share information storage space. And today we see a lot of hosting spaces like OneDrive, DropBox, Google Drive, and more. After Amazon in 2007, Google and IBM started with some large-scale research projects in the field of cloud computing. In 2013, the cloud computing market grew dramatically, and in 2014, the trend went so far as most companies came to this service. It is anticipated that in the year 2020, all cloud services will be available on Cloud. The following graph shows the history of cloud computing (Spaltro, et al., 2016).

Conclusion

Cloud computing is increasingly being adopted by a wide range of users starting from commercial entities to consumers. A survey by Right Scale1 found that an average user runs at least four cloud-based applications and at any point in time is evaluating another four. The survey also found that 41% of commercial entities run a significant workload on public clouds. With so much of our workload moving to the cloud, security in cloud computing is under increased scrutiny. This assessment is also supported by the 2017 report by Forbes2, which says that in 15 months, while 80% of all IT budgets will be committed to cloud solutions, 49% of the businesses are delaying cloud deployment due to security skills gaps and concerns. The problem appears to be multi-dimensional, with a lack of skilled resources, lack of maturity, conflicting best practices, and complex commercial structures to name a few. Adaption of the cloud has reached a tipping point and it is expected that more workloads will move from traditional local storage to the cloud from not just average Internet users, but also from most if not all commercial entities.

While many problems need identifying, analyzing, and addressing, this document attempts to survey the security in cloud computing and reports on various aspects of security vulnerabilities and solutions. Some questions that need urgent answers are (a) Privileged User Access Management, (b) Regulatory Compliance, (c) Data Location, (d) Data Segregation, (e) Data Protection and Recovery Support, (f) Investigative Support, and (g) Long-term Viability. It is highly recommended that these questions, along with other risks, are assessed and addressed. Some of the assessments could be as follows: (a) Organization capability and maturity, (b) Technology & data risks, (c) Application migration and performance risk, (d) People risks, (e) Process risks, (f) Policy risks, (g) Extended supply chain risks.

REFERENCES

1. Beloglazov, J. Abawajyb, R. Buyya. (2012). Energy-aware resource allocation heuristics for efficient management of data centers for Cloud computing, *Future Generation Computer Systems*, 22: 255– 262.
2. Cloud Security Alliance (CSA). (2015). Security Guidance for Critical Areas of Focus in cloud computing V3.0. CSA 2015.
3. Edwards, Justin. (2016). Cloud computing services: Professional obligations and ethics, *Brief*, 43 (3): 32-34.
4. Laurie A. Schintler, Connie L. McNeely. (2017). Cloud Services, *Springer International Publishing*, pp 1-4.
5. Leena Khanna, Anant Jaiswal. (2013). Cloud Computing: Security Issues and Description of Encryption Based Algorithms to Overcome Them, *IJARCSSE*.
6. Marios Savvides. (2011). Introduction to Biometric Recognition Technologies and Application. *International Journal of Computer Applications*, (0975-8887), 15 (3).
7. Mell P, Grance T. (2011). *The NIST Definition of Cloud Computing*. Maryland, US: The National Institute of Standards and Technology.
8. R. P. Padhy and G. P. Rao. (2011). *Load Balancing in cloud computing Systems*. Bachelor Thesis, Rourkela Orissa India.
9. Spaltro, Dan Di Alex Polvi, Logan Welliver. (2016), Methods and systems for cloud computing management, *Patent Citations*, Nov 22.
10. V. Ankita. (2013). A Survey on Various Resource Allocation Policies in Cloud Computing Environment, *IJRET*, Vol. 2, pp. 760-763.
11. Wayne Jansen, Timothy Grance. (2011). Guidelines on Security and Privacy in Public Cloud Computing, *National Institute of Standards and Technology* 2011.