CLOUD COMPUTING AND ITS SECURITY MEASURES

Chinmayee Sahoo

ABSTRACT

In today's world, Cloud Computing is essentially one of the most well-known and on-demand technologies offered by the IT sectors. Cloud computing operates on hardware and software to remit the services over the web. A cloud computing service offers faster innovation, economies of scope and, useful resources to deliver computing services like storage, database, analytics, servers, networking, intelligence, etc. In the other hand, due to its demand, security in cloud computing is becoming more and more important. In this paper we have made a detail study of the security measures required for the cloud service provider as well as the cloud client.

Keywords- *Cloud, Cloud Client, Cloud Server, Internet Service Provider, Software as a Service, Hardware as a Service, Infrastructure as a Service, Data as a Service*.

Reference to this paper should be made as follows:

Chinmayee Sahoo. *'CLOUD COMPUTING AND ITS SECURITY MEASURES, International Journal of Electronics Engineering and Applications, Volume 8, Issue I, Jan-June 2020.*

I. INTRODUCTION

Institutional data can be stored in our own server our it can be outsourced to the cloud storage which provides enormous benefits due to its characteristics which includes scalability, fault tolerance, pay per use, broad network access, increase productivity. However, outsourcing data not only brings advantage but also raise much concern to its privacy and security. Cloud data may find many types of attack which affect services of cloud storage server and even some of them may compromise data privacy and security. XML Signature Wrapping attacks can take administrative rights of the cloud users and can create, modify and delete the data [1], cross side scripting attack can injects a piece of code into web application to bypass access control mechanism [1], In Flooding attack problem a malicious user can overload server by sending bogus request [2], in denial of service attack, malicious code is injected into web browser to open many windows, so legitimate user can't use the service. The attackers have different motive such as, to steal valuable data so they can get monetary benefits, to cause controversy, some former employees may take revenge by hacking the cloud storage and can steal, modify or in worst case delete the entire data. Therefore, many organizations hesitate to adopt cloud services [3, 4].

Cloud computing poses five key characteristics, Utilizes three delivery model and four deployments Model. Key characteristics: -

On Demand Self-Service: Customer can access /control computing resources automatically as needed. It is on demand of cloud client the cloud server provides the services.

Ubiquitous Network Access: User can access application/data with the help of different type of devices like Computer, Mobile, and Tablet. The main advantage of the cloud architecture the property of mobility. The cloud client and cloud server is totally unknown to each other and in any moment of time the client and server may establish a connection between them.

Resource Pooling: Cloud Service Provider (CSP) can share resources both hardware and software to the different cloud clients based on their needs. User can acquire or release resources as needed. Resources can be pooled out any time and form anywhere.

Rapid Elasticity: User can acquire or release resources quickly and automatically as needed. Cloud Architecture may be useful for different level of applications and for different layers of organization. All type of organization may use the same architecture in their own way. It is just due to the elastic nature of Cloud architecture.

Measured Service: One of the major advantages with the cloud is the cost as per use nature. Uses of the resources on the cloud can be monitored and the user is charged on the basis of the resources used.

The service providers provide the ability to govern the applications and services through a world network. It helps in lowering your operating cost as in this, and you need to pay only for the cloud services that you use. Cloud computing has become the most attractive field of computer research because of cost efficiency and flexibility.

According to NIST, cloud computing is "It is a version for permitting favourable, ubiquitary and on-name for web approach method to a combined pool of contour computing sources that may be promptly provisioned and released with minimum management attempt or service issuer interaction". So, the cloud computing model is considered to be a computational model than technology. It is a service that is delivered over the internet. To enable the cloud services, one only needs to set up an account wit5h any of the cloud providers like Microsoft, Amazon, or Google.

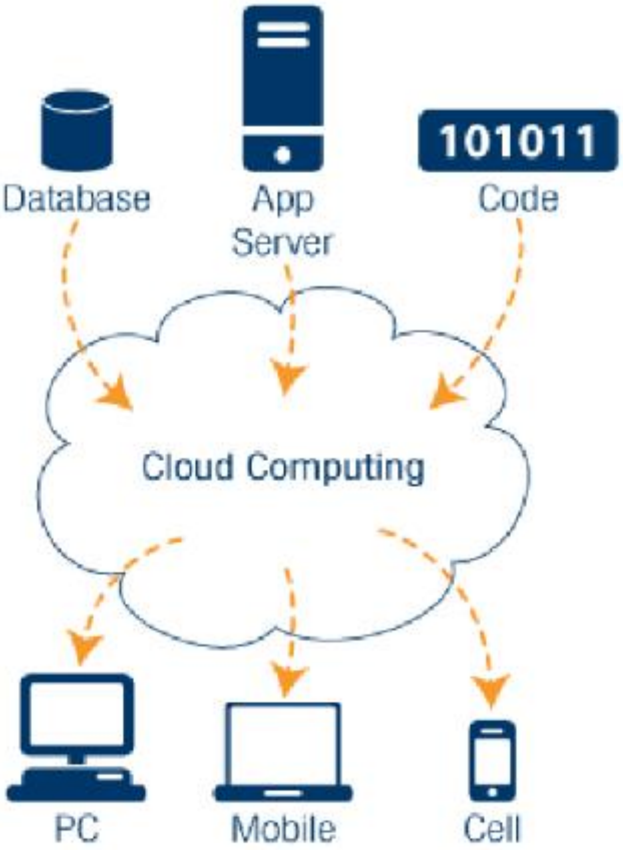


Figure 1. Cloud Architecture.

2. SERVICE MODEL

Cloud computing not only provides a single unit of the product but many other different services. The term service in cloud computing can be defined as using the reusable, fine-grained component across the vendor's web.
It includes the following traits:

1. Low barriers to entry.
2. Device independence allows the user to access the different hardware on the system.
3. Large modularity.

These services include three models:

- Software as a service(SaaS)
- Platform as a service(PaaS)
- Infrastructure as a service(IaaS)

Software as a service

Software as a service is also known as "On-Demand Software." It is a software distribution method in which the applications are hosted by cloud service providers. It also provides the capability to the user to use the form which has been submitted and running on a cloud infrastructure. You can access the application from different client devices through the thin client interface by a web browser or a program interface. The associated data and software are hosted and maintained by the cloud, not by the users. It is hosted remotely, so it needs lees hardware, and the organization does not need to invest in the additional or extra equipment.

Some of the software that is provided as a service through the internet is:

- Customer Resource Management (CRM)
- Accounting
- Web analysis
- Games
- Web content management
- Video conferencing
- IT service management

Software as a service was mainly developed to use web tools such as browsers. This makes the cloud web-native. It provides web-based access to the software which are commercially available.

Platform as a service

Platform as a service provides the virtualized servers for the customer. They can run the existing applications and develop new applications without worrying about the maintenance of the operating system or computing capacity. It provides an environment where you can build, deploy, or test the software application. This service includes application design, testing, hosting, developing, deployment, team collaboration, storage, database, etc.

Some of the well-known platforms as service providers are Microsoft Azure, Salesforce's Force.com, Google Maps, etc.

Infrastructure as a service

Infrastructure as a service is one of the most flexible categories of cloud services. This model provides the storage, processing, networks, and other fundamentals of computing resources to the consumer. In this, the consumer does not have the authenticity to manage or control the cloud infrastructure but has permission to manipulate the operating system, storage, and other deployed applications. You can rent the hardware with Infrastructure as a service (IaaS) instead of buying it.

It saves the time and expanses of capital equipment but does not save cost for the configuration, integration, and management.

Some of the well-known service providers of Infrastructure as a service are Amazon.com, IBM, etc.

Types of cloud

There are three types of clouds for business, organizations, or government agencies. They are:

- Private cloud
- Public cloud
- Hybrid cloud

Private Cloud

A Private cloud is a platform for cloud computing that allows enterprises to implement cloud technologies. You need to create a cloud environment in your data center and provide the self-service access to compute the resources. Without the risk of security and loss of control associated with other cloud infrastructure model, a private cloud offers many benefits of cloud computing. A private cloud includes the utilization of hardware, management of resources, and the virtualization techniques to boost flexibility. The organization itself fully maintains the private cloud infrastructure.

Some of the advantages of a private cloud are:

- The utilization of software and hardware increases by capitulating the more significant ROI for capital expenditure.
- It can bring new services online.
- It provides greater data security, compliances that are specific to industry regulation.

Public Cloud

Public cloud infrastructure can be used by the general public to provide the provision for open use. It is generally managed, maintained, and operated by governmental bodies, businesses, academic affairs, or any combination. In the public cloud, the service provider provides the application, storage, database, and many more to the general public.

Some of the advantages of the public cloud are:

- Elasticity
- Scalability
- Availability of resources without any extra cost.
- Reduces capital expenditure.

Hybrid Cloud

Hybrid cloud infrastructure is the combination of both public clouds as well as the private cloud. A hybrid cloud allows you to run your applications in the nearest or most appropriate locations.

For example, one can host their website in a public cloud and link it to the highly secured database hosted in the private cloud.

3. ISSUES IN DATA SECURITY ALONG WITH PRIVACY FOR CLOUD

Cloud is one of the most significant sources of storing valuable data. All the data breaches and individuals who possess malicious intent can view this data as a good fortune source. A lot of potentially secured data, along with valuable personal information, has been stored on the computer, stored on the cloud. They are subsequently making it crucial to understand the issues that we face in the security and privacy terms for all cloud platforms. The cloud service provider has to understand all the primary security measures that will make the system robust.
Furthermore, the individuals who stole their data on the cloud shell also take personal precautions to secure their valuable data. Cloud computing security issues depend on many e-technologies such as concurrency control, networks, operating system, resource scheduling, transaction management, load balancing, memory management, process management, and many more. The wearing insights to the issues related to security and privacy of the system need to be applicable to cloud computing.

The security of cloud contains some of the fundamental issues in the security program of a computer, such as sometimes authorized users have been restricted to access, data integrity should be maintained, and the availability of services should be ensured. Virtualization is the core concept of cloud computing, and if the security of virtualization will be on stake, no one will avail services from it. Thus, data security is the utmost requirement. If data from one part of a server could escape into another path, some intrusive activities will show a lack of data security in the virtualization.
When the cloud providers provide service-level agreement (SLAs), the actions are often not sufficient to meet the requirements of any institute or organization. The customers of the cloud platform should often go under an assessment to take the risk for any third-party provider. The organization should increase the utilization of shared assessment before providing the resources to assist in this.

Depending upon the asset, vulnerability risk, threats, breaches, the organization should implement proper security controls. The security concern of any cloud platform can be categorized into numerous dimensions. They can be aggregated into three major areas: security and privacy, compliance management, and contractual or legal issue management.
The claims made by advocates of cloud computing shall be promising in terms that the cloud services will be defining the features of computing belonging from the next era. Cloud security should reach its highest potential peak to save all the vulnerabilities associated with the information. All the information systems should cover a wide range of requirements starting from total protection to complete access with some risk assessment, which will evaluate the organization's trade-off and decide what security level is appropriate and acceptable.

The computer security in the context of cloud computing has added some new layers of the question, making it a somewhat higher complexity level to understand the parameters that will be included in risk assessment. Since then, the computer system and staff from the cloud provider's organization arrange under control of any customer or institution using the cloud services. All the significant users of cloud services entirely rely on the contract and for assurance, a certain amount of trust. All the cloud service providers intend to offer transparency at certain levels, making it an essential part of the organization's efforts to evaluate cloud services.

In this paper, we have concentrated on some of the obtrusive issues of cloud computing.

4. INTRUSION DETECTION SYSTEM

In general, the intrusion is an unauthorized entry to others' property or area. Computer science intrusion is the activity to compromise the fundamental goals of computer security like integrity, confidentiality, and privacy. It is a software or hardware component that allows the intrusion detection process. It is designed to monitor the events which are occurring in the computer system or network and responds to the games with the sign of possible incidents of violations of security policies.

The various intrusion detection methodologies used by the Intrusion detection system are:

- Signature-based intrusion detection
- Anomalies based intrusion detection
- Stateful protocol analysis

Cloud uses these intrusion detection methodologies to detect the harmful events occurring in the network.

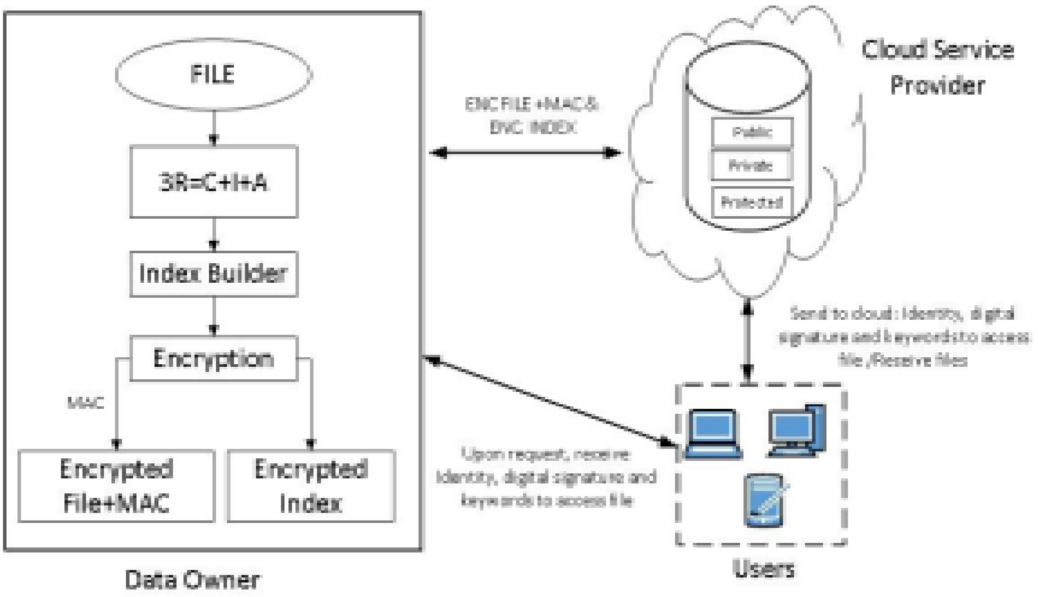

FILE
3R=C+I+A
Index Builder
Encryption
MAC
Encrypted File+MAC
Encrypted Index
Data Owner
ENC FILE +MAC &
ENC INDEX
Cloud Service Provider
Public
Private
Protected
Send to cloud : Identity, digital signature and keywords to access file ,/Receive files
Upon request, receive Identity, digital signature and keywords to access file
Users

Figure 2 Cloud Security Architecture

A. Compliance:

The service provider in public cloud environment normally does not provide the information about the location of user's data stored to the user. The user of public cloud does not have knowledge of where its data is stored. So Cloud service provider must ensure the security of user data through some compliance certificate issued by cloud service provider.

B. Security Management:

Security management is the part of security architecture. Cloud service provider builds trust through security management. Security management is the tool to securely manage the data of cloud user in best possible way. It should have the ability to identify and address the issues related to access control, vulnerability analysis, change control, incident response, fault tolerance, and disaster recovery and business continuity planning.

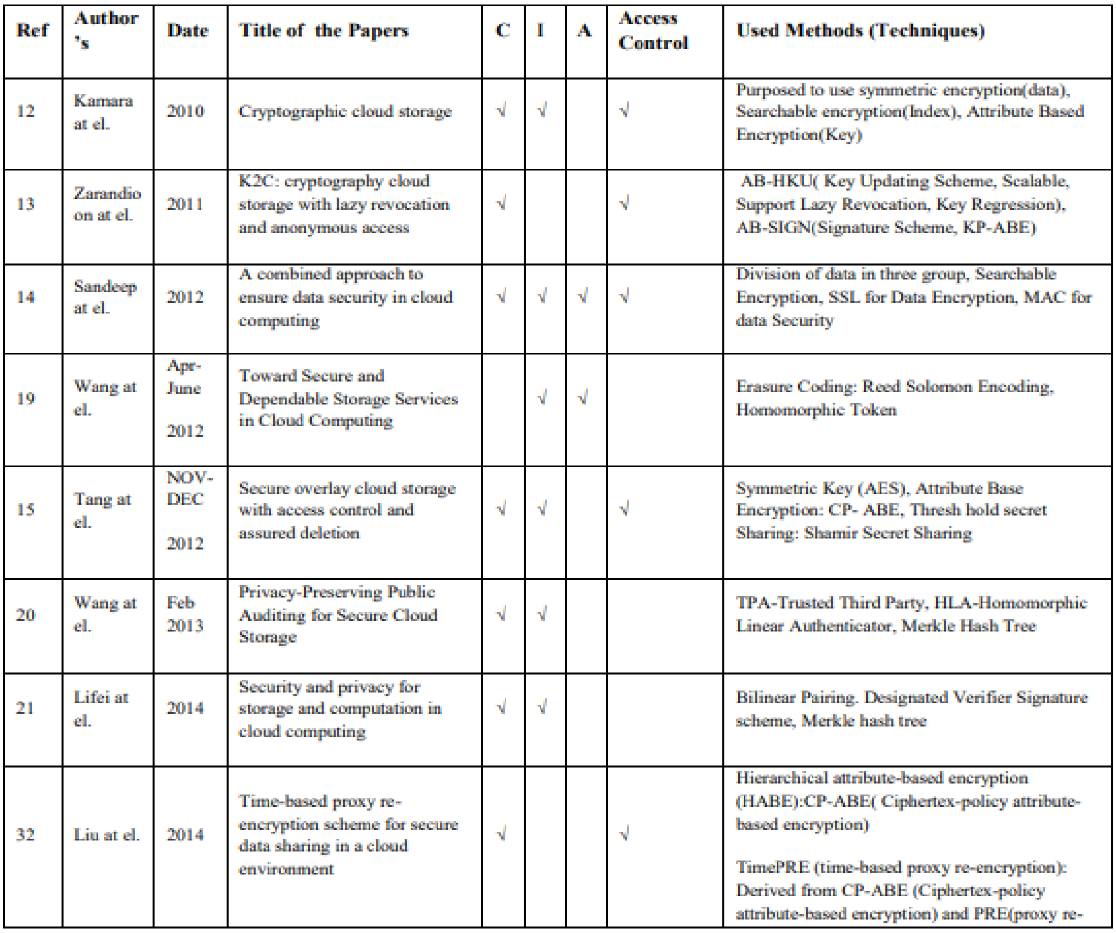
C. Secure Execution Environment:

In a cloud computing environment, there are many applications which run on different servers in a distributed mode. These applications interact with the outside world and other applications and may contain sensitive information. The inappropriate access of this sensitive information would be harmful to a client.

D. Identity Management and Access Control:

Identification and authentication are the most important access control systems. Identification means provision to identify a valid user usually with help of a username or user logon ID to the system. For identity management following methods can be applied a. Finger print scan b. Retina Scan c. Iris Scan d. Hand Geometry e. Voice f. Handwritten signature dynamics.

Table1 : Security Analysis



Ref	Author 's	Date	Title of the Papers	C	I	A	Access Control	Used Methods (Techniques)
12	Kamara at el.	2010	Cryptographic cloud storage	√	√		√	Purposed to use symmetric encryption(data), Searchable encryption(Index), Attribute Based Encryption(Key)
13	Zarandioon at el.	2011	K2C: cryptography cloud storage with lazy revocation and anonymous access	√			√	AB-HKU(Key Updating Scheme, Scalable, Support Lazy Revocation, Key Regression), AB-SIGN(Signature Scheme, KP-ABE)
14	Sandeep at el.	2012	A combined approach to ensure data security in cloud computing	√	√	√	√	Division of data in three group, Searchable Encryption, SSL for Data Encryption, MAC for data Security
19	Wang at el.	Apr-June 2012	Toward Secure and Dependable Storage Services in Cloud Computing		√	√		Erasure Coding: Reed Solomon Encoding, Homomorphic Token
15	Tang at el.	NOV-DEC 2012	Secure overlay cloud storage with access control and assured deletion	√	√		√	Symmetric Key (AES), Attribute Base Encryption: CP- ABE, Thresh hold secret Sharing: Shamir Secret Sharing
20	Wang at el.	Feb 2013	Privacy-Preserving Public Auditing for Secure Cloud Storage	√	√			TPA-Trusted Third Party, HLA-Homomorphic Linear Authenticator, Merkle Hash Tree
21	Lifei at el.	2014	Security and privacy for storage and computation in cloud computing	√	√			Bilinear Pairing. Designated Verifier Signature scheme, Merkle hash tree
32	Liu at el.	2014	Time-based proxy re-encryption scheme for secure data sharing in a cloud environment	√			√	Hierarchical attribute-based encryption (HABE):CP-ABE(Ciphertex-policy attribute-based encryption) TimePRE (time-based proxy re-encryption): Derived from CP-ABE (Ciphertex-policy attribute-based encryption) and PRE(proxy re-

E. Secure Communications:

The application and data moves from from clout to outside in public cloud and within cloud in private cloud, therefore movement of data should be secured. Secure cloud communications involves the structures, transmission methods, transport formats, and security measures that provide confidentiality, integrity, availability, and authentication for transmissions over private and public communications networks.

F. API:

Common vulnerabilities such as weak antivirus software, unattended computing platforms, poor passwords, weak authentication mechanisms, and inadequate intrusion.

5. CONCLUSION

So we can say cloud computing is mainly the delivery of computing services like database, networking, storage, etc. It provides various services to the user with its multiple service model like Platform as a service (PaaS), Software as a Service (SaaS), Infrastructure as a service (IaaS). They also reduce capital costs. Security concerns must be identified to establish trust in cloud computing technology. We even have talked about the intrusion, i.e., the security issues in the cloud-based environment.We have discussed the basics of cloud computing, its service models, types of clouds, security and privacy issues, and then about the Intrusion detection system.

REFERENCES:

[1] Ruhr. "Cloud computing: Gaps in the cloud". NewsRx Health Sci, 2011.

[2] K. Zunnurhain, SV Vrbsky. "Security attacks and solutions in clouds". CloudCom 2010 Poster, 2010.

[3] S. Subashini, V. Kavitha . "A survey on security issues in service delivery models of cloud computing". J. Netw. Comput. Appl. 34, 1–11 ,2011.

[4] Abu Salim, Rajesh Kumar Tiwari, Sachin Tripathi. "Addressing Security Challenges in Cloud Computing". International Journal of Computer Engineering and Applications, Vol. II, Issue II, Pages 1-13, April 2013.

[5] J. Li, G. Zhao, X. Chen, D. Xie, C. Rong, et al. "Fine-grained data access control systems with user accountability in cloud computing". IEEE second international conference on cloud computing technology and science(CloudCom), pp 89–96, 2010.

[6] G. Zhao, C. Rong , J. Li, F. Zhang, Y. Tang. "Trusted data sharing over untrusted cloud storage providers". IEEE second international conference cloud computing technology and science(CloudCom 2010), pp 97–103, 2010.

[7] S. Tu, S. Niu, H. Li, Y. Xiao-ming, M. Li. "Fine-grained access control and revocation for sharing data on clouds". IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) , pp 2146–2155, 2012.

[8] DH Tran, HL Nguyen, W Zha, WK Ng. "Towards security in sharing data on cloud based social networks". 8th International conference on information, communications and signal processing (ICICS) , pp 1–5, 2011.

[9] D. Xin, Y. Jiadi, L. Yuan et al. "Achieving an effective, scalable and privacy preserving data sharing service in cloud computing". Computers and Security 42, 151–164, 2014.

[10] KS Bharath, E. Yousef, H. Gerry, KM Sanjay. "A secure data sharing and query processing framework via federation of cloud computing". Inf. Syst. J. 48,196–212, 2015

[11] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, Accessed on 13.03.16.

[12] https://www.certicom.com/index.php/the-next-generation-of-cryptography, Accessed on 13.03.16

[13] V. Goyal, O. Pandey, A. Sahai, B. Waters. "Attribute-based encryption for fine-grained access control of encrypted data". 13th ACM conference on computer and communications security (CCS '06) , pp 89–98, 2006.

[14] M. Blaze, G. Bleumer, and M. Strauss. "Divertible protocols and atomic proxy cryptography". In EUROCRYPT. Springer-Verlag, 1998.

[15] G. Ateniese, K. Fu, M. Green, and S. Hohenberger. "Improved Proxy Reencryption Schemes with Applications to Secure Distributed Storage". In NDSS, 2006.

[16] Elgamal Taher . "A Public key Cryptosystem and A Signature Scheme based on discrete Logarithms". IEEE Transactions on Information Theory 31 (4):