Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Security of Information at Cloud Storage in Cloud Environment

Aayushi Priya[*]
Department of CSE
REC, Bhopal (M.P), India

Y. K. Rana
Department of CSE
REC, Bhopal (M.P), India

B. P. Patel
Department of CSE
REC, Bhopal (M.P), India

***Abstract**—Cloud Computing has emerged as a new computational platform in Information Technology (IT) enterprises. Cloud computing is a rent-based service where user can storage space and computing resources or services which are dynamically scalable. It reduces the purchasing cost of computational resources and delivered it as per demand of user and they have to pay for that only for which they want to use. With growing publicity of cloud computing, related vulnerabilities or threats are also increasing because cloud services are often delivered by third party. So, security of the information in the cloud is the major issue for a cloud user. The aim of this paper is to discuss about various security techniques over cloud platform and show analysis of protection by using various cryptographic technique which is most useful for information or data security, especially at cloud storage. A framework is made using various techniques and specialized methods for providing the information security to the cloud information.*

***Keywords**— Cloud Computing, Cryptography, Confidentiality, Decryption, Encryption, Integrity, Security issues.*

I. INTRODUCTION

Cloud computing is a concept of evolving large number of computers connected, virtualized and organized in terms of portable workloads. Cloud computing is an application or service that runs on a distributed network using virtualized resources and accessed over internet.

Cloud = abstraction + virtualization

It abstracts details of system implementation from users and developers i.e. applications runs on physical system is not specified data stored in location is unknown administration of system is outsourced to other. Example: AMAZON WEB SERVICES, AZURE, GOOGLE, etc.Virtualization is applied in cloud model to virtualizes system by pooling & sharing resources. Cloud computing is the computation of various resources which delivers the resources across the network (Internet). Instead of maintaining data on self or updating the application desires in our self can be done around the network (Internet) also. At remote locations it allows the user or an organization to use the hardware or software, which is managed by the third parties. This type of network is called “cloud”. Cloud reference architecture [1] is described in Fig. 1.

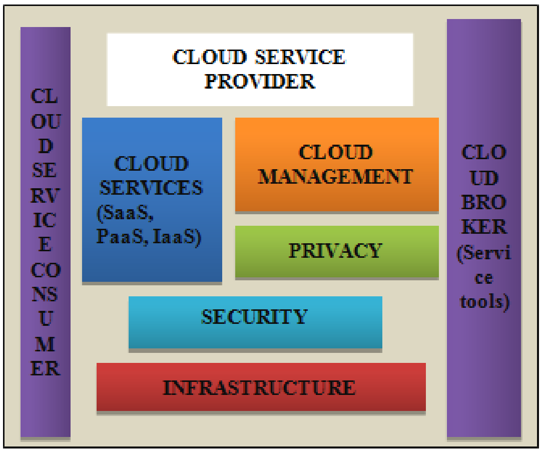

CL OU D SE RV IC E CO NS U M ER
CLOUD SERVICE PROVIDER
CLOUD SERVICES (SaaS, PaaS, IaaS)
CLOUD MANAGEMENT
PRIVACY
SECURITY
INFRASTRUCTURE
CLO UD BRO KER (Servi ce tools)

Fig. 1 Cloud architecture

Resources in cloud can be extended unlimitedly, got anytime and used on-demand. It dynamically delivers everything as a service over the internet on demand of user, such as storage, operating system, software, hardware, and resources.The effectiveness of any computing service ismeasured by its strengths and weaknesses [2]. If advantages owing to computing services are good enough and the overheads occurred are manageable, the acceptance degree of that service is very highand that computing service will be accepted by users. Some advantages and disadvantagesoffered by the cloud are shown in Table I.

Table I: Advantages and disadvantages of cloud computing[2]

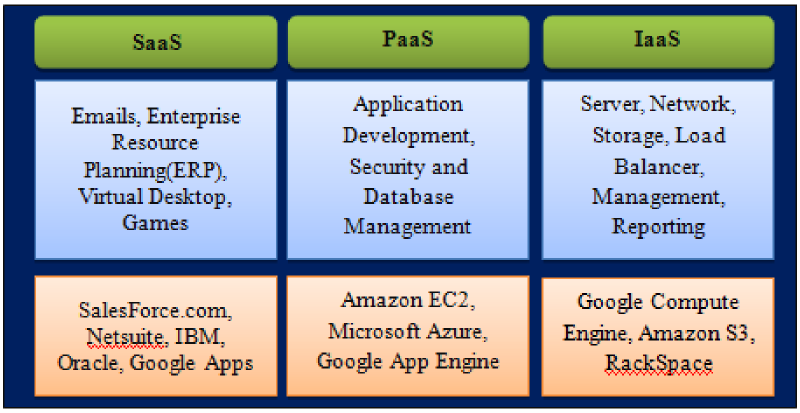
Advantages	Disadvantages
1. Reduced cost. 2. Provides on demand, Scalable and Flexible services on pay-as-you go model. 3. Provides unlimited processing, storage, networking, etc in an elastic way. 4. Easy to backup and recovery of data. 5. Can access the data stored in cloud form anywhere and anytime. 6. Quick deployment.	1. Requires high speed network and connectivity. 2. Security and privacy risks are there. 3. User has external dependencies for critical applications. 4. Requires constantly monitoring and enforcement of Service Level Agreement (SLA's). 5. If cloud loses one's data then user and service provider both get stuck into serious problems.

A. *Delivery Methods of Cloud Computing* [3]*(as shown in Fig.2)*

1) *Software-As-a-Service (SaaS):* In this method, software is provided as a service to the user which they don't purchase for their use. They rent it for their use as pay-per-use model or on subscription. Sometimes service provider delivers these services free for limited use. Example: Gmail, Google Drive, DropBox etc.
2) *Platform-As-a-Service (PaaS):* In this method, cloud provides a platform or environment and related hardware technologies(such as operating systems, virtual servers,storage or development tools) to the user for their applications over Internet. PaaS services are hosted in the cloud and accessed by users simply via their web browser. Customers only subscribe those features that meet their requirements and use them. Example: Google Gears, Microsoft Azure.
3) *Infrastructure-As-a-Service (IaaS)*: In this method, the cloud service provider delivers computing, storage and networking capabilities to the user. A virtual version of infrastructure is given to user but actual physical infrastructure is handled by service providers at remote locations. Example: Amazon Web Services, Google's Compute Engine.

B. *Various Characteristics of Cloud Computing* [3]

1) *On Demand Self-Service:*Cloud providers provide services such as email, applications, network or server services on demand of user.
2) *Broad Network Access:*Cloud services are delivered over network which can be accessed from anywhere such as laptops, mobile phones, etc.
3) *Resource Pooling:*To provide services to the multiple users the resources are pooled together.
4) *Rapid Elasticity:*Cloud services are provisioned with elasticity. Services are quickly scale out and scale in as per user demand.
5) *Measured Service:* Resource usage can be monitored by providing transparency for both the provider and user of the utilized service. Services are charged per usage units – as pay-per-use. There more the utilization the higher user have to pay.



SaaS	PaaS	IaaS
Emails, Enterprise Resource Planning(ERP), Virtual Desktop, Games	Application Development, Security and Database Management	Server, Network, Storage, Load Balancer, Management, Reporting
SalesForce.com, Netsuite, IBM, Oracle, Google Apps	Amazon EC2, Microsoft Azure, Google App Engine	Google Compute Engine, Amazon S3, RackSpace

Fig. 2 Cloud computing services with examples[2]

C. *Deployment Models of Cloud Computing (as shown in Fig.3)* [3]

1) *Private Cloud*:A private cloud is owned and used for particular organization that controls the virtualized resources. It can be inside or outwardly hosted. Example, SOX, HIPAA, SAS 70.
2) *Public Cloud*:Public clouds are owned anddelivered for general public use by a particular organization or company to offer access to computing resources at minimal cost. With public cloud services, users don't need to purchase software, hardware or supporting infrastructure. Example, Rackspace, Amazon Web Services (AWS), Microsoft Azure, Google App Engine.
3) *Community Cloud*: Shared through various organizations or company. Example, Google managed government cloud.
4) *Hybrid Cloud*:Hybrid cloud mean more than two cloud form a single cloud. Goal of such type of cloud is to reduce the change. It takes the advantages in scalability and cost effectiveness. Example, Amazon s3.

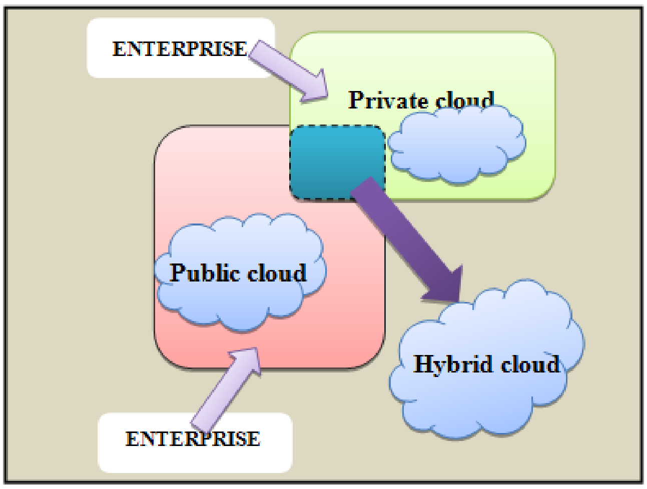
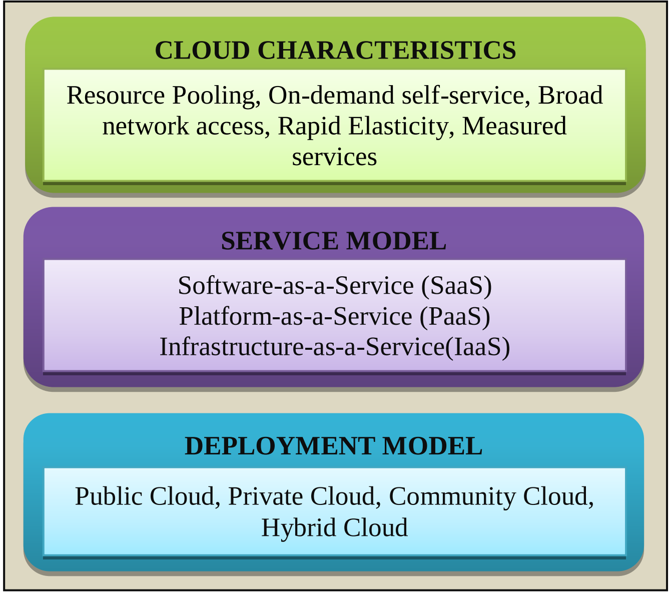


Fig. 3 Cloud computing deployment models

The above mentioned cloud characteristics, services and types according to NIST are shown in Fig 4.


CLOUD CHARACTERISTICS

Resource Pooling, On-demand self-service, Broad network access, Rapid Elasticity, Measured services

SERVICE MODEL

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

DEPLOYMENT MODEL

Public Cloud, Private Cloud, Community Cloud, Hybrid Cloud

Fig. 4 Cloud computing layered architecture

D. Challenges and Issues in Cloud Computing[4,5]

The existing computing paradigms such as distributed computing, cluster or utility computing etc. are basic of cloud computing. With such computing architecturevarious vulnerabilities or issues are associated. Current cloud environment is associated with numerous challenges as shown in Fig. 5 and 6. There are several issues that are of prime concern in cloud computing[4].

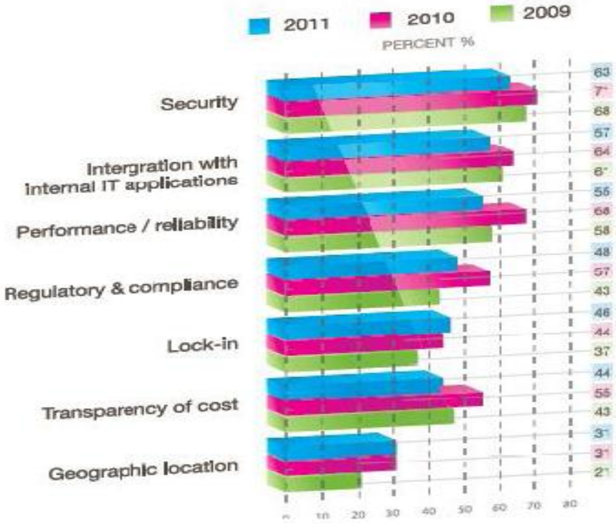


Fig. 5 Biggest barriers to adoption of cloud services[4]

1) *Performance:* A user moves towards cloud computing infrastructure with an objective of better performance which refers towards the efficient capability in running applications over cloud environment. Lack of cloud resources or services such as memory, network connections, lower CPU speed, limited bandwidth, etc. can results in degradation of performance of the system. Effect of degraded performance may results in end of service, loss of customers, reduce revenues generation etc.
2) *Reliability and Availability:* Reliability denotes how often resources are available without any disruption. Availability means the delivery of requested resources at right place on right time whenever they are needed by user or customer. Therefore, reliability and availability of cloud resources should be the most serious area to be considered for its better deployment performance.
3) *Scalability and Elasticity:*Scalability and elasticity provide cloud users facility to use cloud resources according to their needs in unlimited amount as required. Resources available in cloud can be scaled up and down according to wish of user to utilize it.
4) *Interoperability and Portability:* Interoperability is the ability to use the same applications or tools across various cloud platforms. The interoperability can be applied at various levels such as application, service, management and data. Cloud users must be facilitated with the flexibility of either migrating in and out or switching among different clouds whenever they want.Lack of interoperability may results in problem such as vendor lock-in.

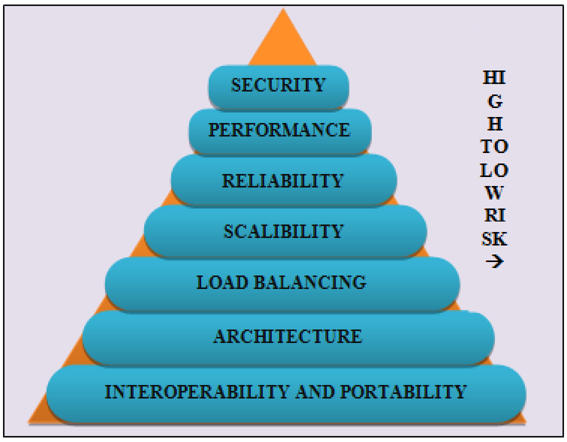


Fig. 6 Classification of threats depend on risk factor

5) *Resource Management and Scheduling:* Resources management can be considered at various levels such as software, hardware or virtualization. Job scheduling is considered as a resource management process in which order of execution of jobs is established in such order to finish job execution. The job scheduling is very critical process that must be decided very carefully. Wrong selection of scheduling method can lead to degradation of performance which may leads to wastage of resources.
6) *Energy Consumption:* Cloud data center consists of thousands of servers. As a result heats are generated due to working of these servers. So, there is need to set up the cooling infrastructure. Working of these cooling infrastructure and servers consumes very large amount of energy and produces green-house gases. So, maintaining such infrastructure is very expensive and energy consuming. To minimize these expenses and energy consumption in optimized and eco-friendly way it is required to design suchsoftware, hardware, job scheduling policies or networking protocols.
7) *Virtualization:*Virtualization is a core technique in computing world that provides a virtualized version of something that are required for computing purpose such as server, hardware platform, operating system or storage. It gives the abstraction of computing resources from physical hardware layer. Virtualization divides the resources of computing into multiple execution environments. Virtualization concept is derived from multitasking and multithreading. It makes multiple operating system and multiple application runningsimultaneously at same time on same machine. It reduces the IT cost and increases the efficiency of computingInstead of these advantages, it has many challenges in cloud computing environment. It has many critical issues to be address such as workloadof Virtual Machines (VMs), security issues in hypervisor based cloud communication, etc.
8) *Security:* According to the survey of International Data Corporation (IDC) the critical challenges in current scenario are security and privacy issues which occur due to movement of information or data or application over the unsecure communication channels. Generally there are two types of security threats such as internal and external. The external threat is posed by individuals or organizations such asattackers or hackers that unable to access to the cloud directly. The internal security threat is posed by official members of cloud providers, current or former employees or individuals that have rights to access to an organization’s information or data, networks and server. In section III, there is discussion of security issues in cloud computing.

II. RELATED WORK

Bhaskar Prashad Rimal et al. [6] described the detailed taxonomy of cloud computing architecture. Further they used this taxonomy to analyze the similarities and differences of architectural approach of existing cloud computing services developed by various projects such as Amazon, Google, Force.com, etc.

Wei-Tek Tsai et al. [7] described the current cloud architecture and issues related to its implementation. They proposed a Service-Oriented Cloud Computing Architecture (SOCCA) for interoperability with each other and to better support multi-tenancy.

Mohammad Sajid et al. [4] presented challenging issues related to various aspects of cloud computing.

Keiko Hashizumeet al. [8] *and Sanjay Dahal* [9] had given a survey detail of different security issues on the cloud and various cryptographic algorithms adoptable to better security for the cloud is presented.

Sherif El-etriby et al. [10] had presented an evaluation of modern encryption techniques at two independent platforms. A randomness testing using NIST statistical testing in cloud computing environment has been performed on those encryption algorithms to determine most suitable encryption technique among them and analyze their performance.

Hamdan M. Al-Sabri et al, [11] proposed a Cloud Storage Encryption (CSE) Architecture using encryption/ searchable encryption technologies to provide a high level of data protection during data transfer to cloud storage. The presented architecture is composed of seven components (Director generate Keys and privileges, Data Users, The role of users, Encryption Point, Decryption Point, Searchable Encryption , and Cloud Data Storage). The CSE Architecture allows to encrypt data and to index it in a manner that ensures the protection of data during transportation. Also it allows the search process in the form of encrypted data and the retrieval of data in a safe manner.

Neha Tirthani et al.[12] contemplated a design for cloud architecture which ensures secured movement of data at client and server end. They have used the non-breakability of Elliptic curve cryptography for data encryption and Diffie Hellman Key Exchange mechanism for connection establishment. The presented encryption mechanism uses the combination of linear and elliptical cryptography methods.

Chao Yang et al. [13] proposed the data security in cloud data storage. For that a novel triple encryption scheme is presented, which combines HDFS files encryption using DEA and the data key encryption with RSA, and then encrypts the user's RSA private key using IDEA. They implemented the triple encryption scheme in Hadoop-based cloud data storage.

Sengupta N et al. [14] proposed a hybrid cryptography system. In this Hybrid cryptography Vigenere and Caesar Cipher Encryption algorithm are implemented which will prevent the cloud infrastructure in three main places, in client location, in the network and in server. Motive of such type of concept to increase computation time for decryption of cipher text messages for the hackers will be more compared to any single cryptographic system.

Shuaishuai Zhu et al. [15]given a novel secure file sharing scheme based on attribute controlling is presented. In order to design a practical cloud file system with attribute based encryption, they give a systematic definition of attribute computing in cloud computing environment. Based on the definition, they designed a secure and practical attribute based encryption scheme without pairings (CP-ABE-WP) under cloud computing scenarios.

GaidaaSaeed Mahdi[20] proposed to develop a simple, stronger and safer cryptographic algorithm which would not only be a secure one, but also reduces total time taken for encryption and decryption. The modified algorithm MTEA is a new secret-key block cipher of 64 bit that uses good features of Tiny Encryption Algorithm (TEA) and RC6 algorithms.

In ([4], [6]-[15]), hybrid cryptography is developed which is used for security of sensitive data in cloud. These cryptography algorithms may be more secure and effective than any single cryptography system.

III. SECURITY ISSUES IN CLOUD COMPUTING

The Cloud Information Security Alliance’s initial report contains a different cloud taxonomy based on different security domains and processes that need to be followed in general cloud delivery methods. Privacy and security related issues that are analysed as an area of concern for cloud computing are [8,9]:

A. *Governance*

It implies control over policies, standards and procedures needed to be followed by organizational units that provides services for cloud computing to the user.

B. *Compliance*

It refers to operation of services by cloud provider in under predefined laws, rules, regulations, specifications and standards. Specially, security and privacy are main area of attention.

C. *Trust*

It discusses various issues of internal threats caused by multi-tenancy, risk and magnitude of the harm resulting fromunauthorized access, disclosure or modification.

D. *Architecture*

It discusses the issues pertaining to software systems utilized by cloud platform. The issues are hypervisor’s security, virtual network protection, virtual machine images and client side protection.

E. *Multi-tenancy*

Multi-Tenancy is a single instance serves for all customers. Providing efficient use of the resources. Since data from multiple tenants is likely to be stored in the same database this leads towards the risk of data leakage between tenants.

F. *Insecure application programming interfaces (API's)*

Cloud providers supply some kind of software interfaces forclients. Weak and user friendly interfaces are vulnerable to attacks. The remedial methods would be strong authenticationand access control with encrypted transmission.

G. *Malicious insiders*

Higher level of access to an employee can leads to leakage ofconfidential data. The best practices to handle this situation is using access control systems, alarm systems, administer logging, two factor authentication, background checks and visitor access.

H. *Data loss/leakage*

Deletion or alteration of records without proper backups andloss of encoding key make the cloud difficult to recover it back.Unauthorized access in cloud can results in data theft andlosses.

I. *Information Security*

Security issues that arise for secure communication during communication between two entities. Generally area of concern while such communications are Confidentiality and Integrity.Confidentiality is associated to all data sent bysomeone (client) should be accessible to only authorized receivers. Integrity refers to all data received shouldonly be sent/modified by authorized senders. Best solutions to these issues are encryption, authentication and secure communication over computer networks.

The above mentioned security risks/threats are depicted in Fig.7.

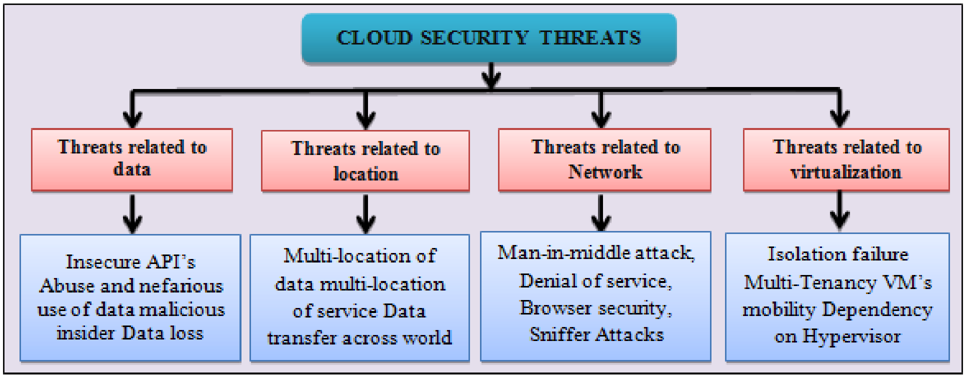

CLOUD SECURITY THREATS
Threats related to data
Threats related to location
Threats related to Network
Threats related to virtualization
Insecure API's Abuse and nefarious use of data malicious insider Data loss
Multi-location of data multi-location of service Data transfer across world
Man-in-middle attack, Denial of service, Browser security, Sniffer Attacks
Isolation failure Multi-Tenancy VM's mobility Dependency on Hypervisor

Fig. 7 Security threats in cloud computing

IV. SECURITY SOLUTION APPROACH

In cloud computing environment there is need of security technologies that are required for providing protection to the resources and virtual machines or virtual servers. Following technologies are used for providing privacy and security in cloud[16]:

A. *Firewall*

To decrease the attack surface of virtualized servers in cloud computing environments, a firewall [17] is deployed on individual virtual machine that controls incoming and outgoing network traffic based on applied rules to prevent unauthorized access to a cloud computing system. It acts as a barrier between secure internal networks to outside network that is not secure.

B. *Intrusion Detection System*

Applying intrusion detection and prevention on virtual machines and Operating system (OS) that detects malicious activity in computer systems and conducts forensic analysis once attack is over.It monitors network resources to detect intrusions or attacks.

C. *Third Party Auditor*

Checks the integrity of data stored at the cloud server and insures cloud user that their data are secure in cloud.

D. *Cryptography*

Using cryptography we can protect the sensitive data in the cloud. In cryptography the sensitive data of the user are encrypted in cipher text which adds a security level over the data. Various types of cryptographic algorithms are discussed below in Fig.8.

Cryptography is most acceptable solution of security by associated companies in cloud computing environment. The first level of security where cryptography can help Cloud computing by making storage secure. Now-a-day's cryptography is referred as a combination of three algorithms, they are Symmetric algorithms, Asymmetric algorithms, and Hashing. In Cloud computing, major area that is to be considered are related to data security, client side security, file system, network traffic, hypervisor security etc. To some extent cryptography can resolve these issues. For instance, in the cloud, customer wants to protect his confidential data then he has to store encrypted form of data in cloud storage. It is advisory not to save an encryption key on the same server where you have stored your encrypted form of data. This will helps us in reducing vulnerabilities caused due to Virtualization. For secure communication between client and server encryption technologies, such as Secure HTTP (HTTPS), encrypted Virtual Private Networks (VPNs), Transport Layer Security(TLS), Secure Shell (SSH), and so on should be used. Encryption will help to prevent threats such as man-in-the-middle (MITM), session hijacking, sniffing attacks, etc.

1) *Symmetric-key Algorithms:* The most important type of cryptographic algorithm is the symmetric algorithm. Symmetric algorithms are those algorithms which uses the same key for both encryption and decryption. Hence, the key is kept private. Symmetric algorithms have the advantages such as it doesn't consume too much of computing power and its execution speed in high. Symmetric encryption is a type of block cipher which takes a block of input (plain-text) of fixed size and gives cipher-text as an output of same size block. Some popular Symmetric-key algorithms used in cloud computing includes: Data Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES) [8]. Strength and weakness of symmetric key cryptography is discussed in table II.
2) *Asymmetric-key Algorithms:* Asymmetric algorithms are those algorithms that use two different keys for encryption and decryption i.e. Public Key and private Key. The Public key is used for encryption at client end (sender) and the private key is used for decryption of data at server end (receiver). Generally, in cloud computing, asymmetric algorithms are used to generate keys for the process of encryption. The most common asymmetric-key algorithms for cloud are: RSA, ECC, Diffie-Hellman Key Exchange. Strength and weakness of asymmetric key cryptography is discussed in table II.

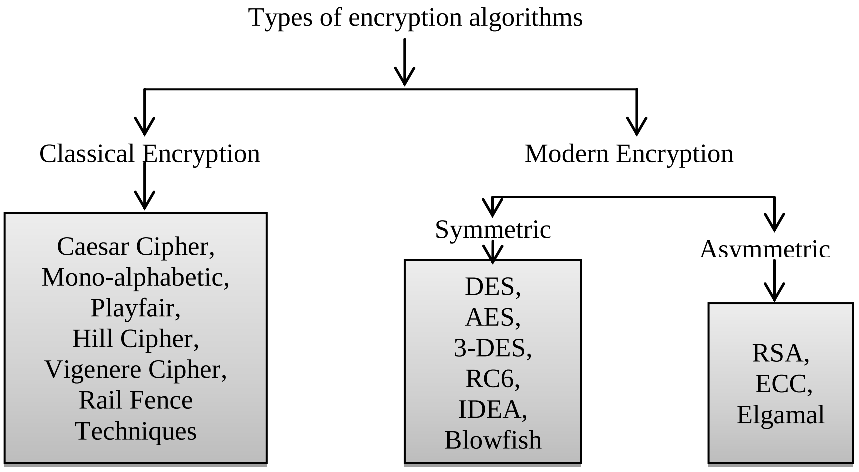

Types of encryption algorithms
Classical Encryption
Modern Encryption
Caesar Cipher, Mono-alphabetic, Playfair, Hill Cipher, Vigenere Cipher, Rail Fence Techniques
Symmetric
Asymmetric
DES, AES, 3-DES, RC6, IDEA, Blowfish
RSA, ECC, Elgamal

Fig. 8 Classification of various encryption methods

Table II: Strength and Weakness of Cryptography Algorithms[3]

Algorithm	**Strength**	**Weakness**
Symmetric key cryptography	Simple, Fast, Encryption and decryption with own key, Uses less computer resources, Prevents message compromise	Need secure channel for key exchange, Management of keys are difficult, Origin and authenticity cannot be guaranteed
Asymmetric key cryptography	Solves the problem of key distribution, Provides message authentication, Detection of tampering, Provides non-repudiation	Slow, Use more computer resources, Public key must be authenticated, Widespread security compromise is possible

A comparison table for various types of cryptographic algorithms used in cloud environment is discussed in table 4.

Table III: comparison able of algorithms used in cloud environment ([4],[18])

Algorithm Name	**Key Size**	**Block Size**	**Security Rate**	**Execution Time**	**Memory Used**	**Problems**
RSA	Based on no. of bits i.e. N=p*q	Variable	Good	Slowest	Highest memory used	Timing attack Cipher text attack Side channel attack
DES	56 bits	64 bits	Not	Slow	More than	Brute force attack

			enough		AES	
3-DES	168,112 bits	64 bits	Adequate	Very slow		
AES	128,192,256 bits	128 bits	Excellent	Very fast	Low RAM needed	Brute force attack, side channel attack
BLOWFISH	32-448 bits	64 bits	Less secure	Fast		Brute force attack
RC6	128,192,256 bits	128 bits	Less secure	Fast		Brute force attack

Table IV: data security metrics based are compared below [19]

METHODOLOGY	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
Keygen algorithm, challenge response algorithm, extract algorithm.		√							
Redistribute algorithm, challenge response algorithm				√					
Database algorithm						√		√	
SOA architecture			√						
Private Information retrieval					√			√	
Symmetric key cryptography	√				√			√	√
Encryption trust mechanism.							√		√
Digital signatures						√		√	√

A : Cost , B : Error rate , C : Reliability , D : Code Redundancy , E : Integrity , F : Processing time for cpu , G : Locality , H : Response time , I : Security

V. CONCLUSION

As per the above given comparison, it is concluded that, data protection, integrity check and authentication are major security parameters that are preserved by applying cryptographic algorithms and such security algorithms are currently used in a cloud computing environment. A comparison Table. 4 describe various cryptographic algorithms used in cloud security with their features and their security level. Another comparison table 5 states the data security metrics and various types of algorithm that work on these security metrics. While keeping in mind thesesecurity metrics, more advance and more efficient algorithms can be developed which can increase the security level in the cloud environment. In future we will suggest an encryption algorithm for a cloud environment which focuses on one of these security metrics.

REFERENCES

[1] Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf, " NIST Cloud Computing Reference Architecture" *US Department of Commerce*, Gaithersburg, MD, 2011.

[2] Yashpalsinh Jadeja, Kirit Modi, "Cloud Computing- Concepts, Architecture and Challenges", *Intenational Conference on Computing, Electronics and Electrical Technologies [ICCEET]*, 2012 IEEE.

[3] P. Mell and T. Grance, "The nist definition of cloud computing, special publication 800-145," *US Department of Commerce*, Gaithersburg, MD, 2011.

[4] Mohammad Sajid, Zahid Raza, "Cloud Computing: Issues & Challenges", *International Conference on Cloud, Big Data and Trust* 2013, RGPV.

[5] Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing", *IEEE,* 2010.

[6] Bhaskar Prashad Rimal, Eunmi choi, Ian Lumb, "A Taxonomy and Survey of Cloud Computing System", *IEEE* 2009.

[7] Wei-Tek Tsai, Xin Sun, Janaka Balasooriya, "Service-Oriented Cloud Computing Architecture", *Seventh International Conference on Information Technology, IEEE* 2010.

[8] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, Eduardo B Fernandez "An analysis of security issues for cloud computing", *Journal of Internet Services and Applications, Springer*, 2013.

[9] Sanjay Dahal, "Security Architecture For Cloud Computing Platform", 2012.

[10] Sherif El-etriby, Eman M. Mohamed, "Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing", *ICCIT* 2012.

[11] Hamdan M. Al-Sabri, Saleh M. Al-Saleem "Building a Cloud Storage Encryption (CSE) Architecture for

Enhancing Cloud Security" *IJCSI International Journal of Computer Science Issues*, Vol. 10, Issue 2, No 1, March 2013 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784

[12] Neha Tirthani, Ganesan R "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography"[online], Available: http://eprint.iacr.org/2014/049.pdf

[13] Chao Yang ; Weiwei Lin ; Mingqi Liu "A Novel Triple Encryption Scheme for Hadoop-Based Cloud Data Security" *Fourth IEEE International Conference on Emerging Intelligent Data and Web Technologies (EIDWT),* 9-11 Sept. 2013 Page(s):437 – 442 Print ISBN:978-1-4799-2140-9

[14] Sengupta, N., Holmes J. "Designing of Cryptography Based Security System for Cloud Computing" *IEEE International conferences on Cloud & Ubiquitous Computing & Emerging Technologies (CUBE),*15-16 Nov. 2013 Page(s):52 – 57 Print ISBN:978-1-4799-2234-5 INSPEC Accession Number:14030210

[15] Shuaishuai Zhu ; ; Xiaoyuan Yang ; Xuguang Wu "Secure Cloud File System with Attribute Based Encryption" *5th IEEE International Conference on Intelligent Networking and Collaborative Systems (INCoS)*9-11 Sept. 2013 Page(s):99 - 102INSPEC Accession Number:13848474

[17] Wesam Dawoud, Ibrahim Takouna, Christoph Meinel, "Infrastructure as a Service Security: Challenges and Solutions", *IEEE*, 2010.

[18] Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", *International Journal of Engineering Research and Applications (IJERA)*, Jul-Aug 2013

[19] Venshila SanthaKumar, Jeno Lovesum" Survey on Data Security in Cloud Computing Using Combined Approach" *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 12, December 2013.

[20] GaidaaSaeed Mahdi, "A Modification of TEA Block Cipher Algorithm for Data Security (MTEA)", *Engg.& tech. Journal*, vol 29, No.5, 2011.