Security Algorithms in Cloud Computing

Rohini Bhardwaj
M. Tech Scholar
Amritsar College of Engineering & Technology,
Amritsar, India

Tejinder Sharma
Associate Professor
Amritsar College of Engineering & Technology,
Amritsar, India

ABSTRACT
Cloud computing provides services over web with powerful resizable resources. Cloud computing facilities give advantages to the end user in terms of cost and ease of use. Cloud computing services require security during transfer of important data and censorious applications to shared and public cloud environments. To store information on cloud, client needs to exchange their information to the outsider who will deal with and store the information. So it is imperative for any association to secure that information. Information is said to be secured if the classification, accessibility, security is available. Numerous calculations have been use to secure the information. In this paper diverse calculations will examine for security of information in distributed computing.

Keywords
Keywords: cloud computing, security, information, availability, confidentiality, hosts.

1. INTRODUCTION
NIST(National Institute of Standards and Technology) defines cloud computing as "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider's interaction". The above definition clearly defines that cloud computing helps in reducing an organization's cost towards managing resources and maintenance of hardware or software Distributed computing is likewise brought as shared registering over the system i.e. the capacity to run an application or a program on various PCs in the meantime. Cloud makes it attainable to store and get to your information from anyplace and anytime.
Security becomes big issue when we send and store the data on any platform. While sending information it is under danger in light of the fact that any unapproved client can get it, change it, so there is need to secure the information. An information is secure in the event when it fulfills three conditions:

i) Confidentiality
ii) Integrity
iii) Availability

2. CLOUD COMPUTING MODELS

2.1 Software as a Service (SaaS)
It refers to giving an ability to the user to use the software and its functions on demand remotely through internet. Saas removes the responsibility of organizations such as set-ups ,installation, maintenance and daily preservation[3].

2.2 Platform as a Service (PaaS)
This paradigmatic could be depicted as program advancement conditions offered by cloud supplier as a – administration. It is giving the client capacity to decide his application onto cloud's foundation.

2.3 Infrastructure as a Service (IaaS)
It is providing the infrastructure such as servers, hardware, storage, routers and the other networking modules to the users. According to requirement of user, he can use some or all of these infrastructure components and pay for what he have used only[3].

3. CLOUD DEPLOYMENT MODEL

3.1 Public Cloud: A cloud is to be entitled as public cloud when the services are being provided over network that are available publically, anyone can access it[12]. In this manner, the foundation of an open cloud is shared between the clients.

3.2 Private Cloud: The private cloud is more secure and costlier than open cloud. It is devoted to single associations to complete their undertakings, it's works within the alliance and conduct in the same organization[3].

3.3 Hybrid cloud
It's a combination of public and private cloud. It is advantageous when the organization possess some critical data/applications which need large protection to be stored in personal cloud while the others does not require large protection can be located in public cloud[3].

4. CLOUD COMPUTING CHARACTERISTICS

4.1 On Request Self Administrations:
A cloud may separately acquire processing liabilities, according to the utilization of various servers, arrange putting away, as when asked for, without speaking with cloud supplier.

4.2 Wide Network Access:
Administrations are dispatched over the Internet inside a standard system and access to the administrations is conceivable through various client apparatuses.

4.3 Asset pooling:
A numerous model is hired to serve distinctive sorts of customers by creating pools of various assets, according to the interest of clients these have diverse assets which can be doled out and reassigned powerfully.

4.4 Quick Versatility:
Abilities may be flexible, procured or expeditiously freed. From clients see, they gave conceivable outcomes turned out to be boundless and must have the capacity to buy in any amount at any time[4].

4.5 Measured Administrations:
The arrangement obtained by various customers is measurable. The utilization of benefit will be coordinated, evaluated, and charged for supporting and asset[4].

5. CLOUD SECURITY ISSUES
At whatever point we move our information into cloud we need to consider numerous security issues. Both protection and security are the challenges in cloud Computing[3]. Some of security issues are as follows:

5.1 Data confidentiality issue:
Confidentiality appertain to any licensed events having bout to guaranteed information. It implies that customer's information and ciphering should be held esoteric from equally cloud service and different punter[13].

5.2 Data availability issue:
Availability defines as all the data and information continually available at a required level that are requested by customers. So we can say that all machines have to store data and information and deliver or process information when the user need them[18]. Data in the cloud stored at different locations so data availability is a big issue in cloud computing.

5.3 Data integrity issue:
Data integrity assure that the information is absolute and valid. Integrity include controlling the network device and data from the unauthorized access and maintain them strictly[18]. The integrity of data proves its regularity, consistency and validity.

5.4 Data trust issue:
Trust is moreover a significant concern in spread computing. Trust could be in heart of individual to device, device to individual, individual to individual. Trust is all about affirmation and certainty. In spread computing, customers stores their informative data on spread storage, on consideration of trust on the cloud [4].

5.5 Infected applications:
merchandiser needs to have the plenary siege to the host for checking and preserving, therefore any harmful consumer from importing any infected request to the cloud that will rigorously influence the customer. The programs can be found as something on cloud. Cloud suppliers guaranty that solutions to customers and protected these programs by employing screening and approval techniques for outsourced or manufactured program code[20].

5.6 Data verification:
Things such as tampering, reduction and robbery, while on a nearby device, during transportation, while at sleep at the not known third-party system, or units, and all through distant back-ups. Source solitude assures protection of information throughout handling, by identifying the model caches in electronic devices, and separating these electronic caches from the Hypervisor cache [20].

6. PRIVACY ISSUES IN CLOUD COMPUTING
When the user stores the data on cloud data center many security issue arises. We will discuss some of them as below:

6.1 Loss of control:
As the customer is employ distributed processing then his data is likely to be held by cloud supplier. In the case of customer rapid to alter his expert co-op then there is a probability to debilitate his data, for example, fulmination or get a grip on which as of this moment occur} in the host farm of his present provider [3].

6.2 Invalid storage:
When cloud provider uses the actual storage to store the data of client then provider has to pay for usage of storage that is why the data may be stored on a secondary memory or improper space of cloud provider. So this can be a major concern about data privacy[3].

6.3 Availability and Reliability Issues
Cloud information store are usually as trusted as enterprise information stores or even more so. But},blackout do occur. Also, the cloud is just functional through the Web therefore Web consistency and accessibility is vital [24].

6.4 Legal and Regulatory Issues
The electronic, worldwide character} of spread processing improves numerous genuine and administrative issues. First, move of data out of a jurisdiction may be restricted. If such move is permitted, which jurisdiction's axioms use in case there's discord? And who's liable for blunder such as for example safety breaches? These issues ought to be fixed for almost any sensitive programs of cloud computing[24].

6.5 Perimeter Security Model Broken
Any companies take advantage of a border safety design with solid protection at the edge of the enterprise network. That design has been weakening over with outsourcing and a beastly portable workforce. Cloud computing moves their demise knell. The cloud is unquestionably away from edge of enterprise control but it will now store important data and applications. [24].

7. EXISTING ALGORITHM FOR SECURITY
To give secure transmission of information over the system, encryption calculations have a critical part in distributed computing. Security computation improvements the data in to blended form by applying "the main element" and only customer have the best way to unscramble the data[9]. In Symmetric key security, just simple key is applied to scribe and decode the information. Another program is employing lopsided key security; two keys-private and start keys are utilized. Start

key is employed for security and private key is applied for decoding [9].

Symmetric algorithms:
- DES
- BLOWFISH
- RC5
- 3DES
- AES

Asymmetric algorithms:
- RSA
- DSA
- Diffie-hellman
- EI Gamal
- XTR

7.1 Symmetric algorithms:

7.1.1 DES:

It stands for Data Encryption Standard and it had been developed in 1977. DES has 64 bit key size and 64 bit block size. When employed for connection, both sender and receiver have to know exactly the same key, which is often applied to encrypt and decrypt the information, or even to create and confirm a Message Authentication Code (MAC). The DES can be employed for Single – consumer encryption [8]. That algorithm has become considered as less protected for several applications. It had been created in 1970s by IBM organization, but was later control by the National Institute of Standards and Technology[15]

7.1.2 BLOWFISH:

This is a symmetric key encryption algorithm designed by Bruce Schneier in the year 1993. Blowfish consumes less memory as compared to AES and DES[16]. Blowfish is a variable length key, 64-bit square figure. Different tests and research investigation demonstrated the prevalence of Blowfish calculation over different calculations as far as the organizing time. It is an algorithm which is available free to everyone.

7.1.3 RC5:

Rivest Cipher algorithm is a symmetric-key algorithm which is known because of its simple execution. This algorithm is developed by Ronald Rivest in the year 1994. The speed of this algorithm is slow as compared to other algorithm [5].

7.1.4 3DES:

Triple Data encryption algorithm an improved algorithm for Data Encryption Standard developed in 1998. This algorithm is a symmetric key block cipher, algorithm that implements the Data Encryption Standard (DES) algorithm three times to every block of data. In comparison to DES 3DES shows slow performance in measures of power consumption and output [5]. It needs always more time as compare to DES due to its triple phase encryption characteristics.

7.1.5 AES:

In cryptography, the Advanced Encryption Standard (AES) symmetric-key encryption standard. All these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. AES algorithm assures that the hash code is encrypted in a very protected manner.AES includes a fixed block size of 128 bits and works on the key size of 128 bits[8]. Both AES and DES are square figures. It's variable key length of 128, 192, or 256 bits; standard 256. It scrambles data bits of 128 bits in 10, 12 and 14 circular contingent upon the key size [9]. AES encryption is quickly and flexible; it could be actualized on numerous stages particularly in small devices.

7.2 Asymmetric algorithm

7.2.1 RSA:

Rivest-Shamir-Adleman is the most simple and common execution asymmetric algorithm. This algorithm is used for encryption as well as decryption of digital signature. It is an algorithm for public-key cryptography [11]. It is the initial algorithm regarded as suited for signing along with encryption[25]. By the usage of the private key unscrambling is held prime secret and isn't regular standard to everybody. The inspiration behind obtaining data is that solitary accepted customers may reach it. Following encryption data is held in the cloud [10].

7.2.2 DSA:

This algorithm is used for processing digital data. It was proposed by NIST in august 1991. With DSA, the entropy, mystery, and uniqueness of the arbitrary mark esteem k is basic. It is critical to the point that restrict any of those three necessities can uncover the whole private key to an assailant. Utilizing a similar esteem twice (even while keeping k mystery), utilizing an anticipated esteem, or releasing even a couple of bits of k in each of a few marks, is sufficient to break DSA [9].

7.2.3 Diffie-hellman:

It is the earlier asymmetric data encryption standard algorithm, developed in 1976. This algorithm permits same users for interchanging a secret key on the insecure medium without any earlier discrepancies . This is a strategy for trading cryptographic keys by first setting up a mutual mystery key to use for the entomb correspondence and not for encryption or decoding. This key trade prepare guarantees the two gatherings that have no earlier learning of each other to mutually build up a common mystery key over unsecure web [6].

7.2.4 EI Gamal:

It is used for public key cryptography. This algorithm is based on the agreement of Diffie-Hellman algorithm. This algorithm is the predecessor algorithm of DSA [5]

7.2.5 XTR:

This is a asymmetric public key encryption algorithm is its fast key generation speed, small key sizes, and speed [5].

Table 1. Review of different techniques of security

Ref. no.	Author	Year	Technique	Features
1.	N.Jayapandian, Dr.A.M.J.Md.ZubairRahman, S.Radhikadevi and M.Koushikaa	2016	DSA and RSA algorithm	Prevent the information from eavesdroppers in cloud

2.	G.PrabuKanna and V.Vasudevan,	2016	Hybrid encryption using (RSA with ECC)	Enhanced the security of outsourced data
3.	Punam V Maitri and ArunaVerma,	2016	LSB technique and SHA1 HASH algorithm	Accomplish key information security and data integrity
4.	Vijay Kumar Pant, JyotiPrakash andAmitAsthana	2015	Cryptography and Stegnography	Provide more security on data in cloud computing
5.	Sakinah Ali Pitchay, Wail Abdo Ali Alhiangem, Farida Ridzuan and MadihahMohd Saudi	2015	RSA and AES using USB devices	Security and personal privacy is highly maximized
6.	Mr.Prashant Rewagad and Ms.YogitaPawar,	2013	Diffie Hellman algorithm, Digital signature, AES	Protection of authentication, data security, verification at same time.
7.	Ashutosh Kumar Dubey, Animesh Kumar Dubey, MayankNamdev and Shiv Shakti Shrivastva,	2012	RSA, MD5	Provide secure cloud framework
8.	Wenjun Fan and Xudong Chen,	2010	Port RSA to CUDA architecture	Realize performance improvement which lead to optimized results.

8. CONCLUSION:

Cloud computing seems very helpful service for lots of people; every individual is applying cloud in numerous ways. Because of its mobility, several people are moving their information to cloud. Cloud computing demonstrate a really effective application for organisations. Since organisations have massive amount of data to keep and cloud offers that space to their user and also enables their user to gain access to their data from everywhere any time easily. As folks are preserving their particular and crucial data to clouds, so that it becomes an important concern to keep that information safely.Security plays an important role in distributed computing. So there is need to ienhance the security of the cloud.

9. REFERENCES

[1] Er Ashima Pansotra and Er Simar Preet Singh "Cloud security algorithms" International Journal of Security and Its Applications vol 9, Issue no.10, pp 353-360, 2015.

[2] Mohammad Ubaidullah Bokhari, QahtanMakkiShallal, YahyaKordTamandani "Security and privacy issues in cloud computing" International Conference on Computing for Sustainable Global Development (INDIACom), pp 896-900,2016.

[3] Manpreet kaur, Hardeep singh "A review of cloud computing security issue" International Journal of Advances in Engineering & Technology, vol 8, Issue no.3, pp 397- 403, june 2015.

[4] Tanvi Agrawal, S.K.Singh "A Review of cloud computing security issues" International Conference on Computing for Sustainable Global Development (INDIACom),pp 106-8, 2016.

[5] Akashdeep Bhardwaj, Dr. GVB Subrahmanyam, Dr. Vinay Avasthi, Dr. Hanumat Sastry "Security Algorithms for Cloud Computing Environment" 2015.

[6] Shakeeba S. Khan, Prof.R.R. Tuteja "Security in cloud computing using cryptographic algorithm" International Journal of Innovative Research in Computer and Communication Engineering, vol 3, Issue no.1, pp148-154, jan 2015.

[7] Varun Gandhi, Sanchit Bansal, Raveesh Kapoor, Aakarsh Dhawan " Cloud computing security architecture implementing DES algorithm in cloud for data security" International Journal of Innovative Research in Engineering & Science, vol 9, Issue no.2, pp 11-19 sep 2013.

[8] Randeep kaur, Supriya kinger " Analysis of security algorithm in cloud computing" International Journal of Application or Innovation in Engineering & Management (IJAIEM)vol.no.3, Issue 3, pp 171-176 march 2014.

[9] S.Manjula, Dr.M.Indra Devi, and R.Swathiya, "Division of data in cloud environment for secure data storage", International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE), pp. 1-5, IEEE. 2016.

[10] Jaspreet singh, Sughandha Sharma " Review on Cloud computing security issues and encryption techniques" International Journal of Engineering Development and Research vol 3, Issue no.2, 2015.

[11] Akshita bhandari, Ashutosh Gupta, and Debasis Das, "Secure algorithm for cloud computing and its application" 6th International Conference on Cloud

System and Big Data Engineering (Confluence), pp. 188-192, IEEE. 2016.

[12] G.Prabu Kanna and V.Vasudevan, "Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 3688-3693, IEEE.2016.

[13] Punam V Maitri and ArunaVerma, "Secure file storage in cloud computing using hybrid cryptography algorithm" International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1635-1638 IEEE.2016.

[14] N.Jayapandian, Dr.A.M.J.Md.ZubairRahman, S.Radhikadevi and M.Koushikaa, "Enhanced cloud security framework to confirm data security on asymmetric and symmetric key encryption" World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), pp. 1-4. IEEE. 2016.

[15] Vinay Pal Bansal and Sandeep Singh, "A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs" 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS),. pp.1-5. IEEE.2015.

[16] Majda Omer Elbasheer and Dr.Taring Mohammed, "Signing and verifying certificates by NTRU and RSA algorithm" International Conference on Cloud Computing (ICCC), pp. 1-4. IEEE.2015.

[17] Vijay Kumar Pant, Jyoti Prakashand Amit Asthana, "Three step data security model for cloud computing based on RSA and Stegnography techniques" International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 490-494. IEEE. 2015.

[18] Sakinah Ali Pitchay, Wail Abdo Ali Alhiangem, Farida Ridzuan and MadihahMohd Saudi, "A proposed systemconcept on enhancing the encryption and decryption method for cloud computing"17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim), pp. 201-205. IEEE. 2015

[19] Mr.Rupesh R Bobde, Prof.AmitKhaparde and Prof.Dr.M.M.Raghuwanshi, "An approach for securing data on cloud using data slicing and cryptography" 9th International Conference on Intelligent Systems and Control (ISCO), (pp. 1-5). IEEE. 2015.

[20] PreetiGarg and Dr.Vineet Sharma, "An efficient and secure data storage in mobile cloud computing through RSA and hash function",International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp. 334-339. IEEE. 2014.

[21] Vishwanath S Mahalle and Aniket K Shahade, "Enhancing the data security in cloud by implementing hybrid(RSA & AES) encryption algorithm", International Conference on Power, Automation and Communication (INPAC), pp. 146-149. IEEE. 2014.

[22] Mr.Prashant Rewagad and Ms.Yogita Pawar, "Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance security in cloud computing" International Conference on Communication Systems and Network Technologies (CSNT), pp. 437-439. IEEE.2013.

[23] Ashutosh Kumar Dubey, Animesh Kumar Dubey, MayankNamdev and Shiv Shakti Shrivastva, "Cloud user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment", Sixth International Conference. pp. 1-8. IEEE. 2012.

[24] Wenjun Fan and Xudong Chen, "Parallelization of RSA algorithm based on compute unified device architecture", 9th International Conference. pp. 174-178. IEEE.2010.

[25] Iuon-Chang Lin and Hsing-Lei Wang, "An improved digital signature scheme with fault tolerance in RSA", Sixth International Conference. pp. 9-12. IEEE.2010.