International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

Review On Various Cloud Security Algorithm

Himanshu Narang, DCRUST (Murthal); Kavita Rathi, Assistant Professor ,DCRUST (Murthal)

Abstract

Cloud computing is a paradigm which provides various set of services offered to users over the net on a rented base. Cloud computing is becoming very popular because of various reasons such as online data storage and on demand resource sharing. Generally, cloud services are provided by a third-party provider who possesses the arrangement. Cloud computing has several other benefits like flexibility, efficiency, quantifiability, integration, and capital reduction. With disregard to the various characteristics of cloud computing services, the organizations are disinclined towards cloud computing primarily owing to security considerations. Security is one of the major challenge that hinder the expansion of cloud computing. The paper addresses the problems which will arise throughout the preparation of cloud services. Once identifying these issues some steps are explained to mitigate these challenges and solutions to unravel the issues via various encryption algorithms.

Introduction

Cloud computing is emerging technology which basically refers to applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. Cloud has left all other distributed computing techniques far behind both in competition and in terms of popularity and success. The primary reason is that, any service extended based on customer's needs. [1]. Cloud in science means large collection of objects that is visually appearing from distance as cloud. Cloud in cloud computing is metaphor for internet. Cloud computing is the evolution and adoption of existing technologies. The main enabling technology of cloud computing is virtualization.

Virtualization means separating a physical computing into more one virtual device which can be easily maintained [2].

There are many characteristics of using cloud computing over other technologies such as agility, less cost, device and location independence, easily maintainable, multitenacy, on demand services broad network access, rapid elasticity.

There are three types of cloud deployment models. They are private, public, and hybrid. [3]

***Public clouds*:** This is a type of cloud hosting in which the cloud services are delivered over a network which is open for public usage. Public cloud providers like Amazon AWS, Microsoft and Google which offer services over internet.

Private clouds: It is also known as internal cloud; the platform for cloud computing that belongs to the particular corporate organization. Private cloud as it permits only the authorized users, gives the organization greater and direct control over their data.

Hybrid clouds: This kind of cloud could be a combination of the general public and also the non-public cloud and it uses the services that are out there in each the general public and personal house. Management of the cloud is completed by each public and personal cloud suppliers.

Delivery Models: There are three types of cloud delivery models.

Software as a Service (SaaS): In SaaS can be defined as softwares deployed over internet provided as services to the client as per their demand e.g. salesforce.com.

Platform as a Service (PaaS): PaaS permits platform access for purchasers so they will place their own software's and applications on to the cloud. Alternately business produce a number of its custom application used within the corporate.

Infrastructure as a Service (IaaS): IaaS provides customers with the infrastructure like rent process, storage, network capability, and alternative basic computing resources. Additionally permits consumers to manage the operative systems, applications, storage, and network property.

Even with these many characteristics many organization disinclined towards cloud technologies due to many issue. The major multiple issues [4] in cloud computing are:

- Multi-tenancy
- Cloud secure federation
- Secure information management
- Service level agreement
- Vendor lock-in
- Loss of control
- Confidentiality
- Data integrity and privacy
- Service availability
- Data intrusion
- Virtualization vulnerability
- Elasticity

To resolve these issues a new concept of cloud security evolved.

Cloud security is a large set of guidelines, technologies, controls, and methods organized to protect data, applications,

ISSN:2319-7900

infrastructure of cloud computing [3].The main objective of cloud security are:

- To make sure the availableness of data communicated between collaborating systems;
- To maintain the integrity of data communicated between or control at intervals collaborating systems, i.e. preventing the loss or modification of data owing to unauthorized access, element failure or alternative error.
- To maintain the integrity of the services provided, i.e. confidentiality and proper operation.
- To authenticate the identity of communicating partners (peer entities) and wherever necessary (e.g. for banking purposes) to confirm non-repudiation of knowledge origin and delivery; and where acceptable, to produce secure interworking with the non-open systems world.

Security issues in Cloud Computing

A. Traditional Security Issues

These security problems involve laptop and network attacks or intrusions that may be created attainable or a minimum of easier by moving to the cloud. Cloud suppliers reply to these considerations by dissertation that their safety measures and security processes are big and tested than those of the same old company. Considerations during this class embrace VM-level attacks, Cloud service providers' vulnerabilities, Phishing cloud supplier, expanded network attack surface, Authentication and authorization, Forensics within the cloud.

B. Accessibility issues

These considerations center on knowledge and demanding applications being obtainable. Well-publicized incidents of cloud outages embrace Gmail's one-day outage in period 2008 (Extended Gmail Outage), Amazon S3's over seven-hour period on July twenty, 2008 (Amazon S3 accessibility Event, 2008), and Flexi Scale's 18-17 hour outage on Gregorian calendar month thirty one, 2008 (Flexi scale Outage). Maintaining the period, preventing denial of service attacks (especially at the single-points-of failure) and making certain hardiness of process integrity (i.e. the cloud supplier is genuinely running and giving applicable outcome) are a number of the foremost problems during this class of threats.

C. Third Party knowledge Control

The legal implications of applications and knowledge being control by a 3rd party are advanced and not well understood. There's additionally a possible lack of management and exactitude once a 3rd party holds the info. a part of the message of cloud computing is that the cloud is implementation-independent, however essentially, regulative compliance needs transparency into the cloud. varied knowledge privacy and security problems ar prompting many corporations to create clouds to avoid these problems and nonetheless maintain a number of the advantages of cloud computing. However, considerations like Due diligence, Audit ability, written agreement obligations, Cloud supplier spying, Cloud supplier spying, transitive nature of contracts have to be compelled to be self-addressed properly.

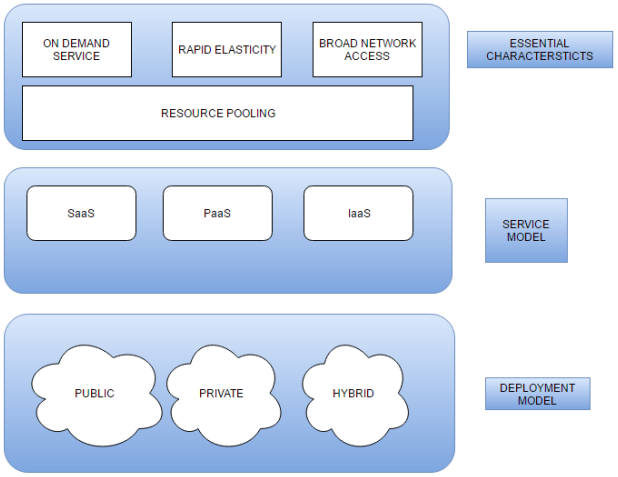

Figure 1. Cloud Security Reference Model

Literature Review

Gartner [5] recognized seven security risks that are essential to be brought before enterprises so that they can build choices relating to the transformation into a cloud computing model [6]. These issues are as follows:

1) *Licensed user access*: The potential risk of exposing structure knowledge over associate external process platform, thanks to the restricted physical, logical and private controls outside the structure boundaries.

ISSN:2319-7900

2) *Agreement to regulations*: process knowledge outside the structure boundaries remains subject to answerability measures, for instance audit by an external third-party house.

3) *Storage space*: Cloud client has no clue regarding the precise location of their knowledge that needs service supplier commitment to suits privacy restrictions.

4) K*nowledge separation*: Clouds hold the customers' knowledge over a shared place wherever knowledge segments aren't keep in successive manner, for that a reliable and well-tested cryptography schemes area unit required.

5) *Recovery*: Service provider must provide some contingency plan to handle disasters and failures.

6) *Investigation*: Breach or intrusion is hard to track because information is dispersed over various servers.

7) *Long-run viability*: If a rare case of service supplier bankruptcy or acquisition happens there ought to be a guarantee of knowledge availability. A corporation has to take care that it will not lose a large quantity of necessary knowledge on the long-term.

In [6, 7] the authors examined completely different security and privacy issues associated with cloud computing. They mentioned and printed the risks, their influences, and therefore the opportunities. Adequate levels of reliability, confidentiality, and sensitive knowledge protection area unit samples of several security issues [5].

Clouds as a computing model demonstrate a promising future; at constant time they extremely need serious acts to hide their weak points. The weaknesses and issues come back from unresolved problems within the existing technologies, that area unit wont to build the cloud. Despite the origins or locations of risks and threats, the cloud security as a problem ought to be handled during a comprehensive manner [8, 9]. Service suppliers look for fulfilling security needs over the clouds, however face completely different challenges to ensure high level of security. For that, authors in [10] mentioned the necessity and challenges, conjointly recommended standardization and management approaches to guide cloud engineers and users. Cloud computing as associate approach introduces new risks, influences others, and magnifies some. These risks and their result on security risks and vulnerabilities were explained in [5].

Discussion

The integrated security based mostly model for cloud is making certain security in sharing of resources to avoid threats and vulnerabilities in cloud computing. To confirm security on distribution of resources, sharing of services, service convenience by assimilate cryptanalytic ways. The cloud platform hardware and software system module holds the software system security, platform security, and infrastructure security. The software system security provides identity management, access management mechanism, antispam and virus. The platform security holds framework security and element security that helps to manage and monitor the cloud setting. The infrastructure security create virtual setting security in integrated security based mostly cloud design. The cloud service supplier controls and monitor the privileged user access and regulative compliance by service level agreement through auditing mechanism.

Existing Algorithm on Cloud Security

To provide secure communication over the network, encryption algorithm program plays a significant role. It's the basic tool for safeguarding the information. Encryption converts the information into scrambled form with the help of "the key" and solely users have the key to decrypt the information. Encryption/Decryption process is considered combination of two algorithms

.

1. *Symmetric key algorithm*:-In this algorithm only one key is used for encryption and decryption. Some of examples of this are DES, AES, and BLOWFISH etc.

2. *Asymmetric key algorithm*:-In this algorithm two key used; one for encryption and other for decryption

A. Symmetric Algorithms

i) DES: It stands for Data encryption standard .it was developed in 1977. it was the first encryption scheme suggested by National Institute of Standards and Technology (National Institute of Standards and Technology).It works with 64bit of key and used to encrypt data of 64 bit block size. [11]

Algorithm:
function DES_Encrypt (M, K)
where M = (L, R)
IP (M)←M 1 to 16
do←For round
Ki SK (K, round)← L xor F(R, Ki)←L swap(L, R) end swap(L, R)
IP-1←M
(M) return
M End

ISSN:2319-7900

ii) **Blowfish:** This was developed in 1993. It is developed by Bruce Schneider. Blowfish is a variable length key, 64-bit block cipher. Not known attack till today is successful against this. The main advantage of this algorithm over others is that it has better throughput and power consumption [14].

Algorithm:
Divide y into two 32-bit halves:
yL, yR For i = 1to 16: YL= YL XOR Pi
yR = F(YL) XOR yR Swap YL and yR
Next i Swap YL and yR (Undo the last swap.)
yR = yR XOR P17
yL = yL XOR P18
Recombine yL and yR

iii) **RC5:** It was developed in 1994. The key length if RC5 is MAX2040 bit with a block size of 32, 64 or 128. The disadvantage of this algorithm is that its speed of is very slow.[15]

Algorithm:
X = X + S[0];
Y = Y + S[1];
for i = 1 to r
*do X = ((X Xor Y) <<< Y) + S[2 * i]*
*Y = ((Y Xor X) <<< X) + S[2 * i + 1]*

iv) **AES**: It stands for Advanced encryption technique.it is block ciphers i.e. encrypt data blocks of 128bit. It has variable key length of 128, 192, or 256 bits; and depending on the key size. It has 10, 12 and 14 round . The advantages of this algorithm is that it is fast, flexible can be implemented on various platforms [15][16].

Algorithm:
Cipher(byte[] input, byte[] output)
{
byte[4,4] State; copy input[] into State[]
AddRoundKey for (round = 1; round < Nr-1; ++round)
{
SubBytes ShiftRows MixColumns AddRoundKey
}
SubBytes ShiftRows AddRoundKey copy State[] to output[]
}

B. Asymmetric Algorithms:

RSA: This algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption. The major advantage of this algorithm is that it can solve problem of authentication and non-repudiation [11].

Algorithm Key Generation:
KeyGen(p, q) Input: Two large primes – p, q
Compute n = p . q φ (n) = (p - 1)(q - 1)
Choose e such that gcd(e, φ (n)) = 1
Determine d such that e . d ≡ 1 mod φ (n)
Key: public key = (e, n)
secret key= (d, n)
Encryption: c = me mod n where c is the cipher text and m is the plain text.

RSA has a multiplicative homomorphism property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product.
Given ci = E(mi) = mi e mod n,
then (c1 . c2) mod n = (m1 . m2) e mod n

Conclusion

Inevitably cloud computing can support a surplus of knowledge systems because the advantages outnumber its shortcomings. Cloud computing offers preparation design, with the power to handle vulnerabilities recognized in traditional information system however its dynamic characteristics are ready to deter the effectiveness of traditional countermeasures. During this paper we've known generic style principles of a cloud surroundings that stem from the need to manage relevant vulnerabilities and threats. Security during a cloud surroundings needs a general purpose of read, from that security are created on trust, mitigating protection to a trusty third party. Cloud computing managing the integrity, confidentiality, accessibility of information and communications, the answer, presents a horizontal level of service, accessible to any or all involved entities, that realizes by data security algorithm as explained in this paper.

References

[1] Wikipedia, http:// en.wikipedia.org/ wiki/Cloud Computing.

[2] Virtual PC vulnerability. http://www.microsoft.com/technet/security/bulletin/ms07-049.mspx.

ISSN:2319-7900

[3] "Study on the security models and strategies of cloud computing" JianhuaChea*, YaminDuanb, Tao Zhanga, JieFanaa 2011 International Conference on Power Electronics and Engineering Application

[4] Security Alliance. Top Threats to Cloud Computing, 2010.http://www.cloudsecurityalliance.org [accessed on: March, 2010].

[5] RuWei Huang, Si Yu, Wei Zhuang and XiaoLin Gui, "Design of Privacy-Preserving Cloud Storage Framework" 2010 Ninth International Conference on Grid and Cloud Computing

[6] Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp. 571-575.

[7] Cong Wang, Qian Wang, KuiRen and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", In Quality of Service, 2009. 17th International Workshop on, page 19, 2009.

[8] Cong Wang, Qian Wang, Kui Ren and Wenjing Lou "Ensuring Data Storage Security in Cloud Computing." IEEE 2009.

[9] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, "Cloud security issues" In Services Computing, 2009. IEEE International Conference on, page 517520, 2009 no. 3, pp 220-232, 2011.

[10] Kashish Goyal, Supriya Kinger" Modified Caesar Cipher for Better Security Enhancement" International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013.

[11] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing (v2.1). Decemeber,2009.

[12] Greveler U, Justus b et al. (2011). A Privacy Preserving System 2.for Cloud Computing, 11th IEEE International Conference on Computer and Information Technology, 648–653.

[13] CLOUD SECURITY ALLIANCE (CSA)'s The Notorious Nine: Cloud Computing Top Threats in 2013 Available Online at: http://www.cloudsecurityalliance.org/topthreats.

[14] John Harauz, Lorti M. Kaufinan. Bruce Potter, "Data Security in the World of Cloud Computing", IEEE Security & Privacy, Co published by the IEEE Computer and Reliability Societies, July/August 2009

[15] Cong Wang, Kui Ren, Qian Wang and Wenjing Lou "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, vol 5.

[16] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed AnisulHoque, Dr. M. M. A Hashem A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.

[17] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[18] Mr. Gurjeevan Singh, , Mr. Ashwani Singla and Mr. K S Sandha " Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August