A Research on minimizing security threat in cloud computing by DUN(declining unsecure Node) Technique

Amarbir Kaur
M. Tech Computer Science
Punjab Technical University, India

Nitin Bhagat
M.Tech Computer Science,
Department of CSE

Abstract: Cloud computing has different meaning to different people, the privacy and security issues also differ between a consumer using a public cloud application, a medium-sized Company using a customized Design of business on a cloud platform, and Some Companies are using Platform on Public level which are Public to Public Network The security requirements in cloud computing environment is to find the Security threats in the Structure of clouds To find the security solutions, and finding Reason so that Pre Security Step Should be taken in concerned with security proposed model. In this paper is to build a trusted computing environment for cloud computing system by Combining the trusted computing platform into cloud computing system Which is free from vulnerabilities and threats and system is designed with a model system in which cloud computing system is combined with trusted computing platform and trusted platform models.

Keywords: DDOS, Cloud Computing, Private Cloud, Community Cloud, Hybrid Cloud.

I. INTRODUCTION

The new developments in the field of information technology offered the people enjoyment, comforts and convenience. Cloud computing is one of the latest developments in the IT industry also known as on demand computing. It provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. It is the application provided in the form of service over the internet and system hardware in the data centers that gives these services. This technology has the capacity to admittance a common collection of resources on request. It is proving extremely striking to cash strapped IT departments that are wanted to deliver better services under pressure. When this cloud is made available for the general customer on pay per use basis, then it is called public cloud. When customer develops their own applications and run their own internal infrastructure then is called private cloud. Integration and consolidation of public and private cloud is called hybrid cloud.[2]

DEPLOYMENT MODELS

Cloud services can be deployed in different ways, depending on the organizational structure and the provisioning location. Four deployment models are usually distinguished, namely public, private, community and hybrid cloud service usage. Deploying cloud computing can differ depending on requirements, and the following four deployment models have been identified, each with specific characteristics that support the needs of the services and users of the clouds in particular ways (see Figure 1)[2]

A Private Cloud

The cloud infrastructure has been deployed, and is maintained and operated for a specific organization. The operation may be in house or with a third party on the premises.[2]

Community Cloud

The cloud infrastructure is shared among a number of organizations with similar interests and requirements. This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. The operation may be in house or with a third party on the premises[2]

.

Public Cloud

The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.[2]

Hybrid Cloud

Hybrid cloud is a composition of two or more clouds (private or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources. Since cloud computing can use both internal and external solutions, there is also the option of not going completely on a public cloud, at least not in regards to confidential data[2]

ISSN: 2278 – 1323

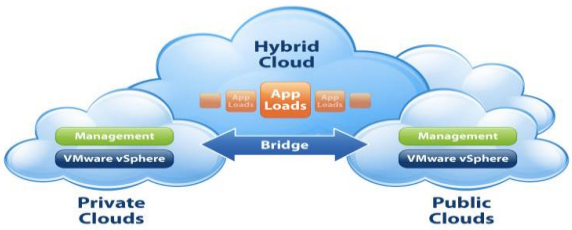

Fig. 1: Cloud Model

OBSTACLES AND OPPORTUNITIES FOR CLOUD COMPUTING

Inspite of being a buzzword, there are certain aspects associated with Cloud Computing a result of which many organizations are still not confident about moving into the cloud. Certain loopholes in its architecture have made cloud computing vulnerable to various security and privacy threats are

1. Privacy and Security
2. Performance Unpredictability, Latency and Reliability
3. Portability and Interoperability[1]

.

II. Related Work

Mobile cloud is a machine-to-machine service model, where a mobile device can use the cloud for searching, data mining, and multimedia processing. To protect the processed data, security services, i.e., encryption, decryption, authentications, etc., are performed in the cloud. In general, we can classify cloud security services in two categories: Critical Security (CS) service and Normal Security (NS) service. CS service provides strong security protection such as using longer key size, strict security access policies, isolations for protecting data, and so on. The CS service usually occupies more cloud computing resources, however it generates more rewards to the cloud provider since the CS service users need to pay more for using the CS service. With the increase of the number of CS and NS service users, it is important to allocate the cloud resource to maximize the system rewards with the considerations of the cloud resource consumption and incomes generated from cloud users. To address this issue[3]

Cloud computing provides a framework for supporting end users easily attaching powerful services and applications through Internet. To provide secure and reliable services in cloud computing environment is an important issue. One of the security issues is how to reduce the impact of denial-of-service (DoS) attack or distributed denial-of-service (DDoS) in this environment. To counter these kinds of attacks, a framework of cooperative intrusion detection system (IDS) is proposed. The proposed system could reduce the impact of these kinds of attacks. To provide such ability, IDSs in the cloud computing regions exchange their alerts with each other. In the system, each of IDSs has a cooperative agent used to compute and determine whether to accept the alerts sent from other IDSs or not. By this way, IDSs could avoid the same type of attack happening. The implementation results indicate that the proposed system could resist DoS attack. Moreover, by comparison, the proposed cooperative IDS system only increases little computation effort compared with pure Snort based IDS but prevents the system from single point of failure attack.[4]

Cloud computing, the next generation architecture of IT enterprises, offers us with a flexible computing environment. In cloud, the virtualized resources are provided as a service over the internet. Typical applications that have already been thought of are SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) etc., which may provide common business applications online that is to be accessed from a web browser. Unlike traditional computing, the cloud moves the application software and databases to a set of networked resources. This enables the data to be accessed from anywhere and anybody simultaneously. Due to the fast growing markets of the cloud and also because of its unique nature, data security in cloud is an important concern. In order to secure the data in cloud, we have to ensure that the data is protected in every level during its flow and also during its storage. In this paper we identify and classify different threats to the data residing in a cloud and also provide separate solutions to these attacks[5].

III. Proposed Work

We Proposed a technique for cloud computing security in Virtual machine monitor can be placed in a virtual environment which will keep track of all the traffic flowing in and out of a virtual machine network. And in case if there is any intruder find doing any wrong activity activity , the corresponding virtual machine may be de-linked or blocked and hence maintaining the security of the virtualized network. The security breach of Twitter and Vaserv.com (via a zero-day vulnerability) last year and the data breach at Son y Corporation and Go-Grid [47], this year, compromising 100 million customers' [38], data have made it quite clear that stringent security measures are needed to be taken in order to ensure security and proper data control in the cloud. Thus we see that the security model adopted by a Cloud service provider should safeguard the cloud against all the possible threats and ensure that the data residing in the cloud doesn't get lost due to some unauthorized control over the network by some third party intruder.

The proposed algorithm for technique for security

Rs Algorithm
$_{ø(n)}$

$a \mod N = 1$

where gcd(a,N)=1

in RSA have:

$N=p.q$

$ø(N)=(p-1)(q-1)$

carefully chosen e & d to be inverses mod ø(N)

hence $e.d=1+k.ø(N)$ for some k

ISSN: 2278 – 1323

Hence :

$C = (M^e)^d = M^{1+k.\phi(N)} = M^1.(M^{\phi(N)})^q = M^1.(1)^q = M^1 = M \bmod N$

Select primes: p=17 & q=11

Compute $n = pq$ =17×11=187

Compute $\phi(n)=(p-1)(q-1)=16\times10=160$

Select e *:* gcd(e,160)=1; choose e=7

Determine d*: de*=1 mod 160 and $d < 160$ Value is d=23 since 23×7=161= 10×160+1

Publish public key KU={7,187}

Keep secret private key KR={23,17,11}

sample RSA encryption/decryption is:

given message M = 88 (nb. 88<187)

encryption:

$C = 88^7 \bmod 187 = 11$

decryption:

$M = 11^{23} \bmod 187 = 88$

can use the Square and Multiply Algorithm

a fast, efficient algorithm for exponentiation

concept is based on repeatedly squaring base

and multiplying in the ones that are needed to compute the result

look at binary representation of exponent

only takes $O(\log_2 n)$ multiples for number n

eg. $7^5 = 7^4.7^1 = 3.7 = 10 \bmod 11$

eg. $3^{129} = 3^{128}.3^1 = 5.3 = 4 \bmod 11$

users of RSA must:

determine two primes at random - p, q

select either e or d and compute the other

primes p,q must not be easily derived from modulus N=p.q

means must be sufficiently large

typically guess and use probabilistic test

exponents e, d are inverses, so use Inverse algorithm to compute the other

the encryption decryption technique are followed by algorithm for security of data in our proposed technique which provide efficient and secured working in cloud computing

IV. Conclusion

Cloud Computing, envisioned as the next generation architecture of IT Enterprise is a talk of the town these days. Although it has revolutionized the computing world, it is pro ne to manifold security threats varying from network level threats to application level threats. In order to keep the Cloud secure, these security threats need to be controlled. Moreover data residing in the cloud is also prone to a number of threats and various issues like confidentiality and integrity of data should be considered while buying storage services from a cloud service provider. Auditing of the cloud at regular intervals needs to be done to safe guard the cloud against external threats. In addition to this, cloud service providers must ensure that all the SLA's are met and human errors on their part should be minimized, enabling smooth functioning. In this paper various security concerns for Cloud computing environment from multiple perspective and the solutions to prevent them have been presented compared and classified.

V. References

[1]. Rohit Bhadauria and Sugata Sanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques" 2009 nternational Journal of Computer Applications. Volume 47

[2]. Rajeev Kumarl, "DATA SECURITY IN CLOUD COMPUTING AND COST ANALYSIS" 2013 International Journal of Computer Applications. Volume 47

[3].

[4]. H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, "Resource allocation for security services in mobile cloud computing," in Proc. IEEE INFOCOM'11, Machine-to-Machine Communications and Networking (M2MCN), pp. 191-195, April 10-15, 2011, Shanghai, China

[5]. Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," ICPPW '10 Proceedings of the 2010 39th International Conference on Parallel Processin g Workshops, IEEE Computer Society, p p. 280-284, Washington DC, USA, 20 10. ISBN: 978-0-7695-4157-0.

[6]. Anindita Saha and Abhijit Das, "A Detailed Analysis of the Issues and Solutions for Securing Data in Cloud" in Proc Journal of Computer Engineering, SSN: 22780661 Volume , Issue5(Sep-Oct 2012)

[7]. CISCO, "Defining Strategies to Protect Against TCP SYN Denial of Service Attacks". September 17, 1996. URL:

ISSN: 2278 – 1323

http://cio.cisco.com/warp/public/707/4.html (4 Jan.2002.

Short Bio Data for the Authors

Amarbeer kaur obtained her B.Tech (computer science & engineering) from College of Engineering and Management, Kapurthala, Punjab, India, pursuing M.Tech (computer science & engineering) from Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. Her area of interest is cloud computing and Security threats in cloud computing.

Nitin bhagat is working as an assist. professor in Department of Computer Science & Engineering, Sai Institute of Engineering and Technology, Manawala, Amritsar, Punjab, India. He obtained his B.Tech (computer science engineering) from Guru Nanak Dev University, Punjab, India, M.Tech (computer science & engineering from Guru Nanak Dev University, Punjab, India.

ISSN: 2278 – 1323