International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M52-072014

THE EFFECTIVE ALGORITHMIC APPROACH FOR SECURED LOAD BALANCING USING HASH ENCRYPTION IN CLOUD COMPUTING

Rishu
Maharishi Markandeshwar Engineering College,
Maharishi Markandeshwar University
Mullana, Ambala, Haryana, India

ABSTRACT

Cloud computing is model that makes orientation to the two essential concepts: 'abstraction' and 'virtualization' to amplify the capacity and competence of IT by providing on demand network access to shared pool of computing resources without investing in new infrastructure. But as more and more information about enterprises are placed in cloud, concerns about how to secure the cloud environment to keep the data secure are also beginning to grow. So before shifting to cloud computing user must know about various threats present in this new system. In this paper, study about various attacks and vulnerabilities that facade threats to cloud is presented. This paper also concerned with the comparative study of attacks and different security issues arises due to the nature of cloud computing.

Keywords: Cloud Computing; Security; Vulnerabilities; Penetration.

INTRODUCTION

Cloud computing refers to the distributed computing on internet that uses the aspects of various technologies: Grid Computing (Distributed network that provides dependable, consistent and inexpensive access to various computational capabilities), Internet Computing (Provides distributed platform on internet), utility computing (pay-as you-grow), Autonomous computing (system manage themselves without any external interference), Edge computing (for load balancing). Today various small and medium size companies moved towards cloud environment because now they are capable to compete with the larger infrastructure companies by simply gaining fast access to best business application and drastically boost their infrastructure resources at negligible cost. While the cloud offers these advantages there are various issues and risks that reduce the growth of cloud computing.

According to the recent IDC enterprise survey figure 1 shows 74% IT companies has to be taken security as a top challenge prevents the adoption of cloud services.

For resource pooling various steps are included:

- User authentication and login process: In this web browser collects all necessary information about consumer using various

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M52-072014

security technologies/protocols like SSL/SSH/TLS.

- Web browser provides all information to policy manager which authenticate the consumer using public key infrastructure, certification authority and others.
- After that consumer request to browser for required services using Simple Object Access Protocol [XML or REST format + transfer protocols].
- Now web browser delegates the QOS requirements to policy manager, which evaluate the requirements according to service level agreement (SLA). For SLA policy manager also use cloud broker and resources engine.
- For resource discovery cloud broker collects the information about other cloud and their services and resource engine delegates the service requirement to VM schedulers which collaborates the required service from various VM / chunks provider.

Dependency among cloud layers: The application layer and core layer depends upon VMs layer and physical machine layer which further depend upon virtual network layer and physical network layer so damage at any layer also have great impact on other layers.

Complexity of security aspects: When we think about security of organization's core IT infrastructure there is need to provide security at network level, host level, application level and when we talk about data security two aspects are included 'data transmission security and data storage security'.

Security Principles: The fundamental basis for developing secure cloud environment is based on various security principles:

Confidentiality: The prevention of unauthorized disclosure of information that may be intentionally or unintentionally refers to the confidentiality.

Integrity: The concept of cloud information integrity is based on two principles

- Prevention of modification of data from unauthorized users and preventing the unauthorized modification of data by authorised user.

Availability: This Principle ensures the availability of cloud data and computing resources when needed.

Authentication: It refers to the process of testing the user's identity and ensures that users are who they claim to be.

Authorization: It refers to the privileges that are granted to individual or process for enabling them to access any authorized data and computing resources.

Accountability: This is related to the concept of non-repudiation where the person cannot deny from the performance of an action. It determines the action and behaviour of single individual within cloud system.

Analysis of attacks and vulnerabilities in cloud computing environment/system: In traditional on premises deployment model the data of enterprise must resides within its boundary and follow their own access control and security policies. Whereas in cloud computing data reside at distributed data centres of cloud with the lack of control and without the knowledge of how their data resides. Due to the

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M52-072014

nature of cloud system there are many questions that arise as to weather a cloud is secure enough or not.

Before understanding the security management in cloud, it must be necessary to analyse the various possible vulnerabilities and attacks in cloud environment.

Network level attacks: During resource pooling process all data or services flow over the network needs to be secured from following attacks to prevent the leakage of sensitive information or other vulnerabilities:

- *Denial of service/distributed denial of service attack*: This attack can overwhelm target's resources so that authorised user is abstained from getting the normal services of cloud. DDOS is also based on DOS attack which can be distributed for more significant effects. This attack is a cause of failure of availability.
- *Eavesdropping* is an interception of network traffic to gain unauthorized access. It can results in failure of confidentiality.
- *Man in the Middle attack* is also a category of eavesdropping. The attack set up the connection with both victims that makes conversation and making them believe that they talk directly but infect the conversation between them is controlled by attack.
- *Replay attack:* The attacker intercepts and save the old messages and then send them later as one of participants to gain access to unauthorized resources.
- *Back Door:* The attacker gain access to network through bypassing the control mechanisms using "back door" such as modem and asynchronous external connection
- *Impersonation* is vulnerability in which malicious node modify the data flow route and lure the node to wrong positions.
- In *Sybil attack* a malicious user pretends to be distinct users after acquiring multiple identities and tries to create relationship with honest user if malicious user is successful to compromise one of the honest user then attack gain unauthorized privileges that helps in attacking process.
- *Byzantine failure* is a malicious activity which compromised a server or a set of server to degrade the performance of cloud.

CLOUD COMPUTING AND VULNERABILITY ISSUES

Cloud Computing means provides computing over the internet and this word is basically inspired by the cloud. In this, data is stored at remote location and available on demand. It allows clients to use applications without installation the file at any computer with internet facility. By data outsourcing user can get the information from anywhere more efficiently and has no burden on data storage and avoid the extra expenses on software, hardware, information resources and data maintenances and used more efficiently.

Vulnerability means anything which has a capability to harm anybody or absence of security system or exploit the system security policy. Vulnerability means any programming error or misconfiguration

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M52-072014

with the help of which an intruder gain unauthorized access to a system. A Security risk may be classified as vulnerability. Vulnerability is basically run on computer and that helps in unauthorized access of reading, creation, modification or deletion of files anywhere on the network. World is mounting with the emerging technologies. The computer networks and packet transmission systems are also growing in parallel, hence to manage and provide security to packet, a secured system is required. Networks seize or simply intercept is one of the challenges in the fast growing world of Cyber Crime. The network establishments including cloud frameworks and distributed computing systems are facing various types of threats on routine basis. To efficiently transmit information across a network, there is need of an improved and reliable architecture.

Dennis Longley and Michael Shain, Stockton Press, ISBN 0-935859-17-9, defines vulnerability as:

In computer security, a weakness in automated systems security procedures, administrative controls, Internet controls, etc., that could be exploited by a threat to gain unauthorized access to information or to disrupt critical processing.

In computer security, a weakness in the physical layout, organization, procedures, personnel, management, administration, hardware or software that may be exploited to cause harm to the ADP system or activity.

In computer security, any weakness or flaw existing in a system. The attack or harmful event, or the opportunity available to a threat agent to mount that attack.

In cloud computing environment, the most fundamental aspect is how services are delivered? Which mainly dependent on cloud deployment models (provides hosting environment). There are three primary types of cloud computing which are available to service consumer:

PUBLIC CLOUDS

A public cloud is hosted, operated, and managed by third party vendor from one or more data centres. The service is offered to multiple customers over common infrastructure; In a public cloud, security management and day- to- day operations are relegated to third party vendor, who is responsible for the public cloud service offering. Hence, the customer of the public cloud service offering has a low degree of control and oversight of the physical and logical security aspects of a private cloud. There are a few challenges listed below that are preventing wide scale adoption of public clouds.

- **Security:** The biggest roadblock is the potential security issues due to multitenant nature of public clouds. There are security and privacy concerns with sharing same physical hardware with unknown parties that need to addressed.
- **Reliability and Performance:** Performance and reliability of the applications are important criteria for defining the success of an enterprise's business because organizations lose control over IT environment in some critical applications.
- **Vendor Lock-in:** Cloud computing services offered by different vendors are not governed by any standards as of today.

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M52-072014

Depending on the vendor, the applications have to undergo changes to adapt to the service.

- **Leveraging Existing Investment:** Most large organizations that have already invested in their own data centers would see a need to leverage those investments as an important criterion in adopting cloud computing.
- **Corporate Governance and Auditing:** Performing governance and auditing activities with the corporate data abstracted in the public cloud poses challenges that are yet to be addressed.
- **Maturity of the Solutions:** Some of the PaaS offering like AppEngine offer limited capabilities like only a subset of JDO API.

PRIVATE CLOUDS

To overcome all above challenges enterprises adopt the private clouds which is managed or owned by an organization to provide the high level control over cloud services and infrastructure. In other words private cloud is build specifically to provide the services within an organization for maintaining the security and privacy. As such, a variety of private cloud patterns have emerged:

- **Dedicated:** Private cloud hosted within a customer- owned data center or at a collection facility, and operated by internal IT departments.
- **Community:** Private clouds located at the premises of third party; owned, managed, and operated by a vendor who is bound by customer SLAs and contractual clauses with security and compliance requirements.
- **Managed:** Private cloud infrastructure owned by customer and managed by a vendor.

HYBRID CLOUDS

This model comprised both the private and public cloud models where organization might run non- core application in a public cloud, while maintaining core applications and sensitive data in- house in a private cloud.

DESIGN SCENARIO:

This novel proposed algorithm delivers a better security in the cloud data centers. The major design scenario of such approach is as following.

1. Deployment and Integration of cryptography and secured layered in the proposed algorithmic approach
2. The data centers are accessed by authenticated clients using secured shell and encrypted transmission via brokers

Module 1: System study:

STEP 1: The first step toward the implementation of proposed scheme is the creation of data centers before creating any entities. Because, then data centers are the resource providers. We need at least one before creating any entities. .

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M52-072014

STEP 2: Creation of Cloud Computing Entities: The proposed system is divided up into three parts.

1) **Cloud Service Providers:** That
   - Storage of data in a virtual machines
   - Generate dynamic keys using hybrid approach (MD5+SHA)
   - Distribute the dynamic hybrid keys to the cloud consumers.
   - Perform authentication

2) **Cloud Broker:** negotiation of the relationships between consumers and providers
3) **Cloud Consumers:** that
   - Request for the services with an implemented key by the CSP.

Module 2: Generation of Key by EMG (Encryption Module generation)

STEP 1: Section of random numbers (combination of numbers and characters) for generating first set of dynamic keys. **(dat)**

STEP 2:

1) Selection of random number again including ASIII characters for generating a second set of dynamic keys. **(dat2)**

2) Generation of message digest using MD5 hash function cryptographic algorithm on second set of dynamic keys. It creates a message digest of 128-bit (16-byte) hash value that typically expressed in text format as a 32 digit hexadecimal number in this implementation.

3) After that an encrypted key is appended into the string **(sb)** buffer. If, this step is not performed then will not be added to make the communication more secured.

4) The SHA hash function cryptographic algorithm is applied on the buffered encrypted key to create a message digest that is longer in length. If the length of digest is more the security is more and impossible to break. The SHA-256 is used that creates a message digest of 256 bit(32 byte) hash value that is typically expressed in 64 digit hexadecimal numbers in this work.

4) The string is again buffered to the new string **sb1**.

5) Final key is generated by concatenating first set of random number **(dat),** second set of random number (dat2) and the broker ID (a). The broker is a part of communication channel. So, that any cracking attempt is identified.

Module 3: Distribution of key and Encryption of data with a dynamic hash key.

Each time different key is used for encryption. It is similar to one time password. If any one key is compromised that doesn't affect the other keys. It

also solves the problem of key distribution. Because these are distributed once at the starting. It provides a best protection against session hijack and replay attack.

Module 4: Authentication of cloud consumers when they request services. If key matched then cloud service provider approve and cloud broker bind the cloudlets to the specific virtual machine.

Module 5: Report Generation: At the final step, the reports are generated. Here different formulas and techniques are used for the calculation of execution time and security parameter.

CONCLUSION

The cloud environment has scalable, expandable, virtualization and abstraction as basic aspects that makes cloud security become more complex. Various vulnerabilities and attacks discussed in this paper are main threats for cloud that cause many enterprises which have plan to migrate to cloud prefer using cloud for less sensitive data and store important data within enterprise boundary. So as a result, moving towards cloud computing require more safe and secure environment and our further study will also focus on various security schemes or algorithm that helps in providing secure cloud environment.

REFERENCES

[1] Cochavy, Baruch, Method of efficiently sending packets onto a network by eliminating an interrupt, US Patent Issued on August 18, 1998

[2] Dimitris M. Kyriazanos, Neeli R. Prasad, Charalampos Z. Patrikakis, A Security, Privacy and Trust Architecture for Wireless Sensor Networks, 50th International Symposium ELMAR-2008, 10-12 September 2008, Zadar, Croatia

[3] Donna Andert, Robin Wakefield, and Joel Weise, Professional Services Security Practice, Sun BluePrints™ OnLine - December 2002, Trust Modeling for Security Architecture Development

[4] Security, Encryption, Acceleration, http://www.networkintercept.com

[5] Youlu Zheng, Shakil Akhtar, Networks for Computer Scientists and Engineers, Oxford University Press, 2009

[6] Carl Endorf, Eugene Schultz and Jim Mellander, Intrusion Detection & Prevention, McGraw-Hill, 2004

[7] Technical Standard Risk Taxonomy ISBN 1-931624-77-1 Document Number: C081 Published by The Open Group, January 2009.

[8] "An Introduction to Factor Analysis of Information Risk (FAIR)", Risk Management Insight LLC, November 2006;

[9] Matt Bishop and Dave Bailey. A Critical Analysis of Vulnerability Taxonomies. Technical Report CSE-96-11, Department of Computer Science at the University of California at Davis, September 1996

[10] Schou, Corey (1996). Handbook of INFOSEC Terms, Version 2.0. CD-ROM (Idaho State University & Information Systems Security Organization)

[11] Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257 ISBN 978-0-12-374354-1

ISSN (Online) : 2230-8849
Volume 4 Issue 2 July 2014
International Manuscript ID : ISSN22308849-V4I2M52-072014

[12] ISACA THE RISK IT FRAMEWORK (registration required)

[13] Kakareka, Almantas (2009) "23" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 393 ISBN 978-0-12-374354-1

[14] Technical Report CSD-TR-97-026 Ivan Krsul The COAST Laboratory Department of Computer Sciences, Purdue University, April 15, 1997

[15] The Web Application Security Consortium Project, Web Application Security Statistics 2009

[16] Ross Anderson. Why Cryptosystems Fail. Technical report, University Computer Laboratory, Cam- bridge, January 1994.

[17] Neil Schlager. When Technology Fails: Signi cant Technological Disasters, Accidents, and Failures of the Twentieth Century. Gale Research Inc., 1994.

[18] Hacking: The Art of Exploitation Second Edition

[19] Kiountouzis, E. A.; Kokolakis, S. A. Information systems security: facing the information society of the 21st century London: Chapman & Hall, Ltd ISBN 0-412-78120-4

[20] Bavisi, Sanjay (2009) "22" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 375 ISBN 978-0-12-374354-1