A Secure mechanism for load balancing framework in cloud: An CDAP approach

1.Shikha Pandey
Manager-Learning,
Trans-Neuron technologies
Bangalore, India.
Shikha.p@transneuron.com

2.Ashok Kumar Upadhaya
Member of Technical Staff II,
VMWare private ltd. India,
Bangalore, India.
aupadhaya@vmware.com

3.Dr.C.K. Jha.
Head of Department (Computer Science),
Banasthali University, India.
ckjha1@gmail.com

Abstract: **The traditional network security measures do not properly address the security issues of cloud environment and mostly during the allocation process. Like capabilities, the faults are too inherited, which have worsened more in cloud due to its characteristics. Even being one of the fundamental technology of cloud, the security hindrance is more because of virtualization. Being a multidomain environment different security measures can be applied at independent domains as well as in their functionalities. In this paper we are proposing an efficient security technique based on the privacy homomorphism CDAP (Concealed Data Aggregation) in order to achieve efficient data concealment by using end to end encryption process during the mechanism of suboptimal Load balancing .The load balancing frame work adopts the greedy incremental mechanism for the proper allocation of resources.**

Keywords: Privacy homomorphism; suboptimal mechanism; load balancing; security

I. Introduction

The security issues are paramount impediment in the adaptation and development of cloud computing. The principal concern of any client accessing the services and application of cloud is security and the risk. The application and datum security of the cloud environment depends upon the paradigmatic principle of "CIA" i.e. confidentiality, Integrity and Availability, but implemented in distributed, virtualized and dynamic architectures. ***"Threats and vulnerabilities are also major concern which leads to hindrance in the security".*** The major difference between the two is: -**Vulnerability:** Weakness of the computing environment that can be exploited by the attacker. **Threat:** Probable error or attack by malicious user or computing environment condition. When migrating applications and services in cloud environment vulnerabilities (Session riding, insecure cryptography, internet dependency data protection and portability) and threats (Malicious insider, shared technology use and insecure APIs) are need to be considered. In order to migrate applications successfully prior knowledge of cloud threats and vulnerabilities is a welcome option. Enterprise should avoid relying completely on the cloud provider to address the security issues. [15][16][20][22] In this paper we are proposing an efficient security technique based on the privacy homomorphism CDAP (Concealed Data Aggregation) in order to achieve efficient data concealment by using end to end encryption process during the mechanism of suboptimal Load balancing .The load balancing frame work adopts the greedy incremental mechanism for the proper allocation of resources. The rest of the paper is organized with related work in section 2 followed by concerns in section 3,Section 4 forms the basis of security objectives and the proposed work is articulated in section 5.Section 6 describes the conclusion and future work.

II. Related Work

Sahoo J. and Glitho R. [1] has proposed heuristic to solve the problem of "replica server" placement ,supported by the process of "placement and refinement". Where with placement procedure an initial placement of replica servers on cloud sites are obtained whereas the redundant cloud sites is discarded by the refinement. The mechanism reduces the cost.

Dong N. et.al [2] formulation and "key points of consecutive algorithm (S-Aware)" based on bin packing is discussed in their work. Proposed model is developed to evaluat specific resource in heterogeneous environment with focus on energy conservation and load balancing.

Shani J. and Vidyarthi D [3]They proposed "a level based autonomic Workflow-and-Platform Aware (WPA)" task clustering technique based on the workflow structure and the underlying resource set size . The method reduces the execution time of the workflow and also consolidates the load with minimum possible resources at same time with respect to which wastage is minimized.

Farahmandian. S et al.[4]. Analyzed that since cloud is built on the fundamental of distributed environment, it is easier for an intruder to launch a distributed denial of service (DDoS) attack against available resources and services of a cloud computing environment. Various mechanism for defense is studied in the work.

Barna C.et al.[5] They have implemented, and evaluated a unified approach to enable elasticity and mitigate DoS attack. their work are compromises of an adaptive management algorithm for choosing which portions of a workload need additional resources and which portions represent undesirable traffic and should be mitigated; adapting a layered queuing network (LQN) model for cloud environments in order to enable proactive cost-benefit analysis of the workload; and an implementation and evaluation.

Khalil I et al.[6] Provided a comprehensive survey on the cloud security and privacy concerns. They have investigated and identified the limitations of the current solutions and presented nine general cloud attacks. They have also shown that clouds are more resilient to Distributed Denial of Service (DDoS) attacks.

Gai K. et.al, [7] A "Dynamic Data Encryption Strategy (D2ES)" is proposed by them where the mechanism goals to encrypt data selectively using privacy classification methods with time limits. The proposed work maximizes the privacy protection scope with the use of selective encryption strategy along with the proof of the privacy enhancement Privacy issues.

Hong.L and Ge Yufei[8], An " ant colony algorithm (ACA) to solve the VMP problem, named as GACA-VMP" is proposed .The proposed mechanism is in accordance with the "genetic algorithm" in order to solve the issues in which it optimizes the calculation of pheromone in load balancing for the selection.

Batistaa B. et.al [9] They have defined QoS-driven mechanism for cloud environments based on the performance evaluation of a service with different security process. According to them, it is possible to maintain the performance of the service even with the overhead is imposed because of security mechanisms in a cloud environment.

Zhongjin L et.al [10], "A security and cost aware scheduling (SCAS) algorithm" for the heterogeneous tasks of scientific workflow in clouds is proposed based on "particle swarm optimization (PSO)", the coding strategy is devised which minimizes the total execution cost with defined constraints with respect to risk rate and deadline.

III. Concerns

The cloud delivery and deployment model, its defining characteristics, along with the technologies employed the cloud presents different security issues in comparison to traditional computing environment.

Also, the Security measures applied in cloud environment are, for the most part is not different in comparison of the traditional computing environment except due to the above pointed reason.

Maturity, completeness and effectiveness describes the security posture of any organization adopting the cloud and the security controls are implemented in indepently in a layers or at more levels ranging from the physical level, platform and up to the information and applications levels as described by NIST

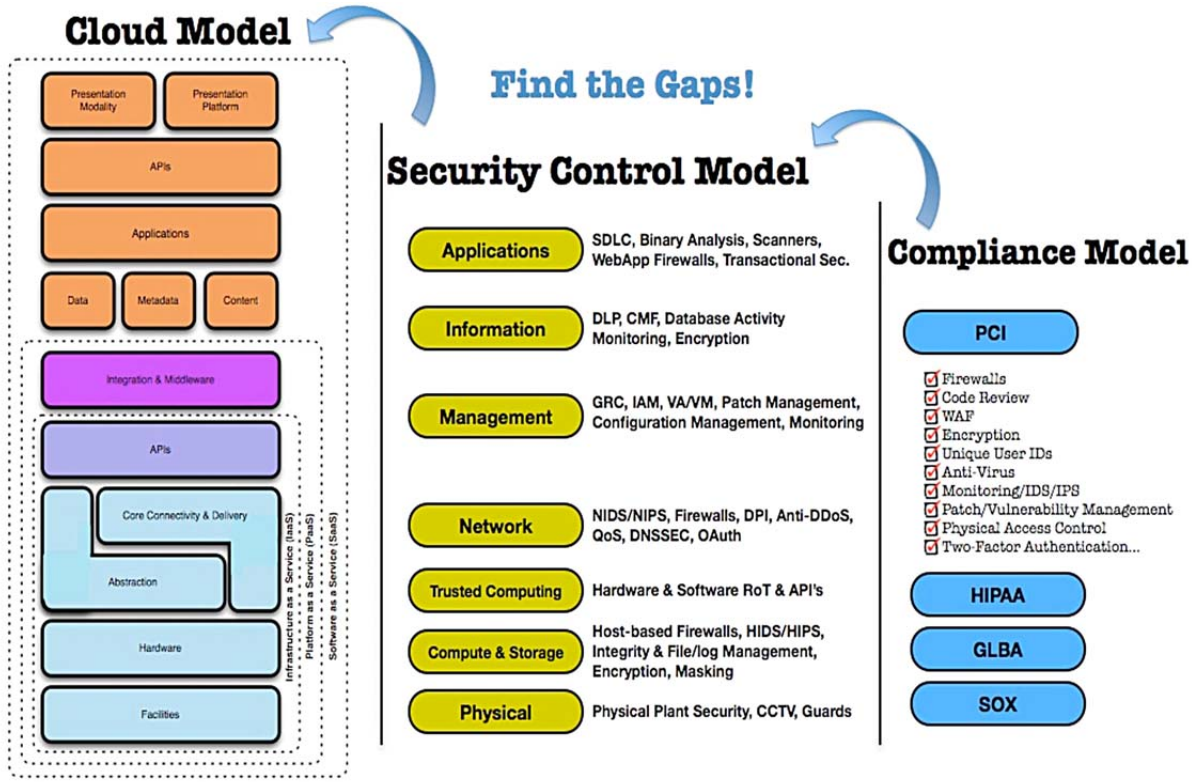

Figure 1: Cloud Security Model (NIST)

Due to the hierarchal architecture, the security risks, analogous of cloud computing services is also inherited between different service layers since cloud has layered architecture. Therefore, its critical to analyze the security issues.[15][16][17][18] . Below is the brief analysis of security concerns in accordance to delivery model.

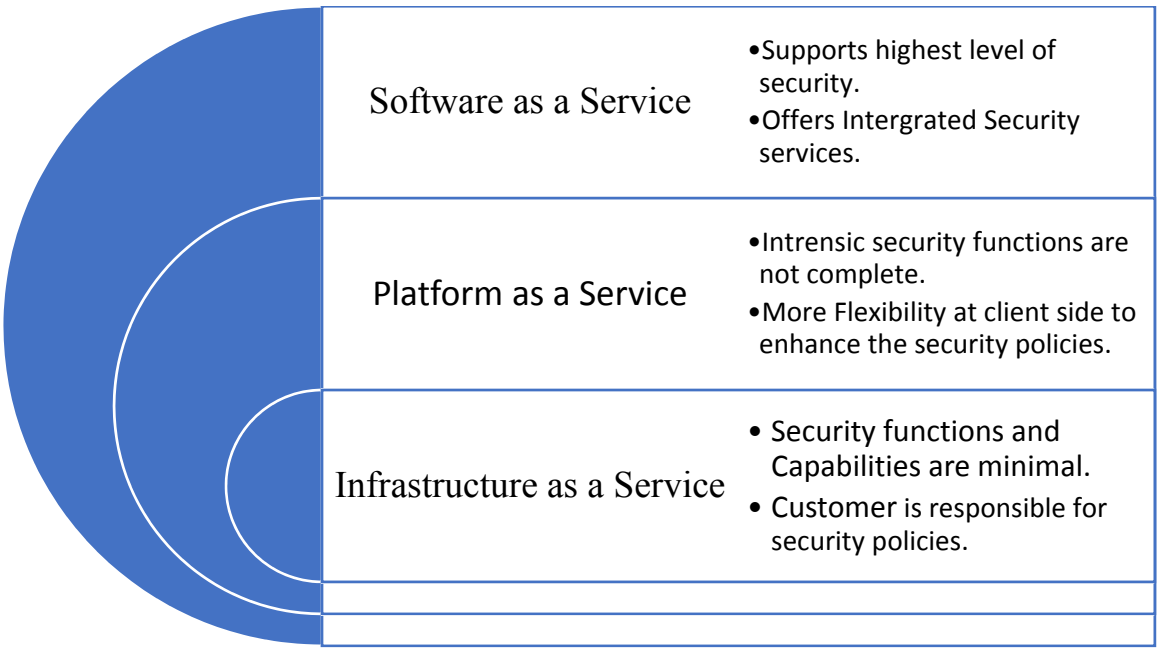

Figure 2: Security concerns in delivery model

The management process and security capabilities of end clients increases down the layer which is one of the critical property in cloud security.[11][12][13][14]

IV. Security objective

According to DACS (Data and analysis center for Software) the properties to be executed for security is:-

Dependability: Predictability of the application in accordance to various conditions.

Trustworthiness: Minimal or less vulnerabilities.

Survivability: Resistant to attacks and ability to recover as soon as possible.

With various benefits and property cloud environment is hindered with different security risks. Security requirements of cloud computing includes-

- Confidentiality
- Integrity
- Availability
- Accountability
- Privacy-preservability [17][18][19][20].

According to CSA, Virtualization vulnerability and Availability are key security issues in cloud environment. Where the vulnerabilities of the environment can be used by the clients to architect parameters that can bypass the standard security measures and access privileged data of other tenants hosted on same machine or in network.

Different cloud platform uses different security mechanism like strong cryptographically Secure Shell (SSH) keys are used by Amazon whereas Microsoft uses Synchronous cookies and connection limiting for mitigation of Distributed Denial of Service (DDoS). Due to cloud, heterogeneous nature, a single security system would overburden in respect to price for other applications [19]

"The need of mechanisms to ensure strong isolation, mediated sharing, and secure communications between VMs is need to be addressed by security mechanism since issues such as trusting the VM image, hardening hosts, and securing inter-host communication are critical areas in IaaS security, privacy, and trust which are inherently non-quantitative" [21].

The cloud service providers often use virtualization technologies which causes dramatic effect on the security levels therefore there is a need of cryptographic approaches to be used .Dynamic encryption policies is taking centerstage in cloud environment and in order to adopt the measures to avoid security especially during the VM migration at time of load balancing[13]A need of proper security mechanism during the process of load balancing and resource allocation is the need of hour, used at the heterogeneous cloud environment[25].

V. Proposed solution

The proposed solution aims to guarantee secure mechanism for load balancing of the participating machines. Our proposed mechanism of load balancing was based on the idea to migrate consolidated virtual and physical resource from one cloud site to other at dispersed locations by the use of "Incremental tree approach" which is an optimal way to balance the load. In the framework each overloaded node is connected via a shortest path, where the weight of the edges can be defined in terms link utilization, cost or bandwidth and the process goes on till all the overloaded nodes, depending upon the capacity of underloaded node of previous determined path is migrated through the aggregated node determined from the existing established shortest path. The migration of

resources during the process results into the formation of tree hierarchy, which is generally an "incremental tree".

In this load balancing framework, we can embed the features of privacy homomorphism CDAP (Concealed Data Aggregation) in order to achieve efficient data concealment by using end to end encryption process. Due to the inclusion of homomorphism process, direct operation on cipher texts at time of aggregation and migration process is possible. Though being a simple mechanism, this security technique is suitable for a virtual environment like cloud.It facilitates the aggregation process along with the enhancement of security and obtains a safe end to end transmission between the overloaded and underloaded machines in the cloud system.

Being an encryption transformation mechanism direct calculations on chipper text is possible where a symmetric or asymmetric encryption technique can be applied to obtain chiphertexts. In our work we are using privacy homomorphism based on asymmetric keys because of induced vulnerabilities and disadvantage of symmetric key. We have assumed that entire operations is performed on a set of nodes called TNodes (The underloaded nodes, overloaded nodes and enroute nodes) ,where the privacy homomorphic encryption occurs.

The encryption mechanism is categorized as: End to end encryption: It ensures data privacy and security from one data center to another. Hop by hop: data is encrypted at the aggregator node.Our proposed process is based on End to end encryption.[23][24]

Procedure

The mechanism is made up of following phases:

• Assignment of public key issued by Overloaded node to the TNODEs followed by resources deployment.

• Key sharing (Pair-wise) between the TNODEs of different datacenters or in same datacenters.

• Encryption of data occurs at overloaded nodes by using the symmetric encryption algorithm (RC5) [28]and after which the chipertext is communicated to its closest TNODE in the already established path .

• Decryption of chipher text at Tnodes after which the aggregation function is applied and again the text is encrypted and deployed to the underloaded nodes.

Proposed Algorithm

Let E be the encryption function and D the decryption function.

+ and * respectively indicates the addition and the multiplication functions on the data set R.

Key_{pr} =private

Key_{pu} =public keys possesd by nodes then the transformation encryption is -

Additively homomorphic if:

$m+n= (DKey_{pr}(Ekey_{pu}(m)+Ekey_{pu}(n)))$ *where m, n belong to R.*

Multiplicatively homomorphic if:

$m*n= (DKey_{pr}(Ekey_{pu}(m)*Ekey_{pu}(n)))$ *where m, n belong to R.*

The cipher text (which can be a virtual machines files or resources) are migrated. The TNODEs aggregate incrementally the cipher text during the migration. Only the underloaded nodes can decrypt the aggregated data after the migration using its private key.

The network performance shows tremendous improvement in energy and the bandwidth consumption once migration is secured. Even though the degree of security is increased along with the performance, the use of our security mechanism is hindered by restricted number of allowed aggregation functions. Along with the limited capacity of overloaded machines which can make encryption mechanism non tolerable to some nodes. Though this problem can be addressed by the feature of overcommit exhibited by the machines.

VI. Conclusion and future work

The proposed security mechanism though being a simple technique, but embedding it with the load balancing framework further strengthens the Cloud operations. The proposed paper provides an insight into the cloud security and vulnerabilities along with mechanism to overcome the security issues at the time of load balancing by embedding the poly homo morphism security encryption during load balancing framework.

References

[1] Sahoo J. and Glitho R., "Greedy heuristic for replica server placement in Cloud based Content Delivery Networks" IEEE Symposium on Computers and Communication (ISCC), 2016 ISBN Information: INSPEC **Accession Number:** 16247610, **DOI:** 10.1109/ISCC.2016.7543758 **Publisher:** IEEE ,2016

[2] Dong **N.** et.al,"A Proportional Multi-resource Scheduling Model in SDCloud" Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), IEEE 2016

[3] Shani J. and Vidyarthi D., "Workflow-and-Platform Aware task clustering for scientific workflow execution in Cloud environment", Future Generation Computer System ,Elesvier . 64, Pages 61–74,2016.

[4] Farahmandian S., Zamani M., Akbarabadi A., Zadeh J., Mirhosseini S., Farahmandian S., "A Survey on Methods to Defend against DDoS Attack in CloudComputing", Recent in Knowledge Engineering and Systems Science, ISBN: 978-1-61804-162-3,pp..185-190 www.wseas.us/e-library/conferences/2013/CambridgeUK/.../AISE-29.pdfDDOS.

[5] Barna C. , Shtern M., Smit M. , Ghanbari H. and Litoiu M," Model-driven Elasticity and DoS Attack Mitigation in Cloud Environments", Proceedings of the11th International Conference on Autonomic Computing (ICAC '14). Philadelphia, PA, ISBN 978-1-931971-11-9, pp. 13-24,June 2014

[6] Khalil I., Khreishah A., Azeem M. , "Cloud Computing Security: A Survey", computers, ISSN 2073-431X, www.mdpi.com/journal/computers Computers 2014, 3, pp.1-35, doi:10.3390/computers3010001,2014.

[7] Gai K. et.al, "Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing" ,2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), **ISBN:** 978-1-5090-0946-6,2016.

[8] Hong.L and Yufei G.GACA-VMP: Virtual Machine Placement Scheduling in Cloud Computing Based on Genetic Ant Colony Algorithm Approach, IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), 16158285 ,2015

[9] Batistaa B. et.al, "A QoS-driven approach for cloud computing addressing attributes of performance and security", Future Generation Computer Systems ,Volume 68, , Pages 260–274 ,Elsevier ,2017

[10] Zhongjin L et.al," A security and cost aware scheduling algorithm for heterogeneous tasks of scientific workflow in clouds" Future Generation Computer Systems,Volume 65, December 2016, Pages 140–152,Special Issue on Big Data in the Cloud,Elesvier

[11] Sevcik P and WetzelR," About Seeing Through the Fog: Managing Application Performance in the Cloud" February 2011.

[12] Wu Li et.al, "SLA-Based Resource Provisioning for HostedSoftware-as-a-Service Applications inCloud Computing Environments", IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 7, NO. 3, pp 465-485,2014

[13] Antonio C.et al,"VM consolidation: A real case based on OpenStack Cloud",FUTURE GENERATION COMPUTER SYSTEMS ,2014.

[14] Rodrigues G.et.al, "Monitoring of Cloud Computing Environments: Concepts, Solutions, Trends, and Future Directions", SAC 2016 ACM Proceedings of the 31st Annual ACM Symposium on Applied Computing, pp 378-383, ISBN 978-1-4503-3739-7 ,2016.

[15] S. Subashini n , V. Kavitha, "A survey on security issues in service delivery models of cloud computing" ,Anna University Tirunelveli, Tirunelveli, TN 62700, Journal of Network and Computer Applications 34 (2011) 1–11,Elesvier

[16] Hassan Takabi and James B.D. ," Security and Privacy Challenges in Cloud Computing Environments", THE IEEE COMPUTER AND RELIABILITY SOCIETIES , 2016,IEEE , pp 24-31

[17] Yan Q. et.al,"Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges",IEEE Communications Surveys & Tutorials ,Volume: 18, Issue: 1, 2016

[18] Yadav P. and Sujata , "Security Issues in Cloud Computing Solution of DDOS and Introducing Two-Tier CAPTCHA", International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.3,pp.25-39, June 2013.

[19] Srivastava R. et.al, " MAS based framework to project cloud computing against DDOS attack", International Journal of research in engineering and Technology,EISSN:2319-1163,vol.02,issue12,2013

[20] Logashree R. and Rajakumari S. , "Secured Load Balancing Model based on Cloud Partitioning using Round Robin Algorithm for the Public Cloud in Cloud Computing",International Journal of Science, Engineering and Technology Research (IJSETR), ISSN: 2278 – 7798,vol. 3, Issue 4, , pp.861-867, 2014

[21] " Security guidance for critical areas of focus in Cloud Computing", https://cloudsecurityalliance.org/guidance/csaguide.v3.0,v4.0.

[22] Krutz R. and Vines R., Cloud Security: A Comprehensive Guide to Secure Cloud Computing, ISBN:978-0-470-58987-8, pp 384 , 1st edition, Wiley publishing, July 2010

[23] X.W. Zheng et.al, "A Multi-Objective Virtual Network Embedding Algorithm in Cloud Computing," Journal *of Internet Technology*, vol. 17, Issue 4, pp. 633-642, Jul.,2016

[24] Cheng T. et.al, "An approach to identifying cryptographic algorithm from ciphertext" 8th IEEE International Conference on Communication Software and Networks (ICCSN) , pp:19 – 23

[25] Ismail B. et.al, "Cloud-centric multi-level authentication as a service for secure public safety device networks" , IEEE Communications Magazine ,Vol.: 54, Issue: 4, pp: 47 – 53, 2016