ISSN 2320-9984

Volume 1, Issue 4, December 2013 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Security Threats in Cloud Computing

Devanshu Tiwari
Assistant Professor
Department of Computer Science & Engineering
Bagula Mukhi College of Technology,
Bhopal (M.P.) [INDIA]
Email :devanshu.tiwari28@gmail.com

Mukesh Kumar Dhariwal
Assistant Professor
Department of Computer Science & Engineering
University Institute of Technology, RGPV,
Bhopal (M.P.) [INDIA]
Email : er.mukesh2008@gmail.com

Abhishek Kesharwani
Assistant Professor
Department of Computer Science & Engineering
University Institute of Technology, RGPV,
Bhopal (M.P.) [INDIA]
Email :abhishek040685@gmail.com

Sanjay Kumar Tehariya
Assistant Professor
Department of Computer Science & Engineering
University Institute of Technology, RGPV
Bhopal (M.P.) [INDIA]
Email : sanjay_tehariya@rediffmail.com

Abstract—*Cloud computing is a network-based environment that focuses on sharing computations or resources. Actually, clouds are Internet-based and it tries to disguise complexity for clients. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and software in the data centres that provide those services. Cloud providers use virtualization technologies combined with self -service abilities for computing resources via network infrastructure. This paper gives brief introduction of the techniques used in cloud computing environment for securing the communication in cloud network. This survey gives idea about the scenario of cloud computing, its security, integrity, threats etc.*

Index Terms:—*Cloud computing, PAAS, SAAS, IAAS, Cloud Ontology.*

1. INTRODUCTION

Cloud computing refers to software and hardware delivered as services over the Internet. The implementation of data mining techniques through Cloud computing will allow the users to retrieve meaningful information from virtually integrated data warehouse that reduces the costs of infrastructure and storage.

Cloud computing is a network-based environment that focuses on sharing computations or resources. Actually, clouds are Internet-based and it tries to disguise complexity for clients. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and software in the datacenters that provide those services. Cloud providers use virtualization technologies combined with self service abilities for computing resources via network infrastructure.

The Cloud, is referred to, involvement of using computing resources – hardware and software – which combinely delivers services over the Internet (Figure: 1). Many companies accepts the third party to host them on its large servers instead of building their own IT infrastructure to host databases or software, so the company would have access to its data and software over the Internet.

The use of Cloud Computing is gaining popularity due to its mobility, huge availability in low cost. On the other hand it brings more threats to the security of the company's data and information. In recent years, data mining techniques are most using technique. Discovering knowledge in databases becoming increasingly vital in various fields: business, medicine, science and engineering, spatial data etc. The Cloud Computing provides its users benefit of unprecedented access. to valuable data that can be turned into valuable insight that can help them achieve their business objectives.

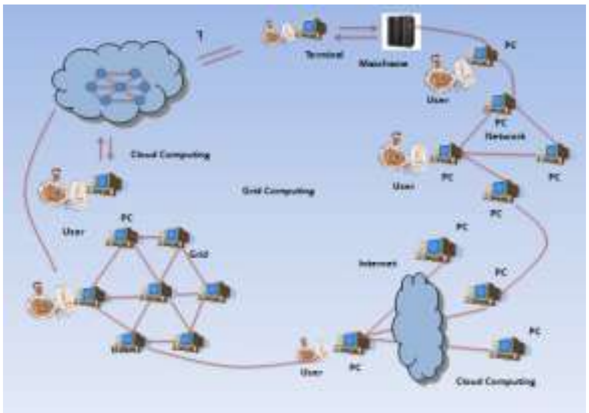

Figure:1 Cloud Computing Scenario

Internet-based online services provides huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the can find this IP addresses as well. In this case, malicious user can find out which physical servers the victim is using then by implanting a malicious virtual machine at that location to launch an attack. Because all of users who use same virtual machine as infrastructure, if a hacker steals a virtual machine or take control over it, he will be able to access to all users' data within it. Therefore, The hacker can copy them into his local machine before cloud provider detect that virtual machine is in out of control then the hacker with analysis the data may be find valuable data afterward [3].

2. RELATED WORK

In 2011, Farzad Sabahi concluded reliability, availability, and security issues for cloud computing (RAS issues), and propose feasible and available solutions for some of them. A cloud application is based on network appliance software. Operating system, running in a virtual machine in a virtualized environment. A virtual appliance faces some management issues in because most of the maintenance, software updates, configuration and other management tasks that they are done by cloud provider which responsible for them. This way for decentralized application and access every time and everywhere to data, occasion and introduce new set of challenges and security problems that must consider before transfer data to a cloud environment and just because the software can run in a Virtual machine it does not mean that it performs well in cloud environment necessarily. That's why cloud faces risks and hidden costs in managing cloud. For successful cloud computing it is necessary to create balance between the business benefits and the hidden potential risks which can impact efficacy [1].

In 2011 Haoming Liang, Wenbo Chen and Kefu Shi proposed a approach which analyses the programming and task scheduling model according to the present-used cloud computing system. It gives examples to explain the process of programming and its modifying directions, as well as the process within which services and resources exchange. It gives explanation of Cloud computing, how social network may increase the Qos through changing the service load will be discussed [2].

In 2011Guannan HU and Wenhao ZHU introduced a dynamic user-integrated cloud computing architecture. This architecture integrates clients with storage capacity and computing competency to data center dynamically, it expands the scale of cloud computing data center. Collaboration of clients with the data center provides services to the other users [3].

In 2009 Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapatham, and Sangoh Jeong proposed the a solution for authentication and secure session management between weblets running device side and those on the cloud. It provides secure migration and authorizes cloud weblets to access sensitive user data via external web services. It gives application integration between private and public clouds in an enterprise environment [4].

Yan Zhu, Huaixi Wang, Zexing Hu, Gail -Joon Ahn, Hongxin Hu, Stephen S. Yau, “Efficient Provable Data Possession for Hybrid Clouds” Proceedings of the 17th ACM conference on Computer and communications security. Migration. It gives the scenario of multiple cloud service providers to cooperatively store and maintain the clients’ data. This scheme gives less overhead and reduces communication complexity [5].

In 2009 Qian Wang, Cong Wang, Jin Li1, Kui Ren, and Wenjing Lou introduced a protocol Which firstly identify the difficulties and potential security problems of direct extensions with fully dynamic data updates and secondly shows how to construct an elegant verification scheme for seamless integration. It manipulates the classic Merkle Hash Tree (MHT) construction for block tag authentication [6].

In 2012 Arash Nourian and Muthucumaru Maheswaran introduced new image encoding scheme that enhances the privacy of the images and allows the clouds to perform certain forms of computations on the images. This encoding scheme uses a chaotic map to transform the image after it is masked with an arbitrarily chosen ambient image [7].

In 2009 Qian Wang, Cong Wang, Jin Li1, Kui Ren, and Wenjing Lou introduced a protocol Which firstly identify the difficulties and potential security problems of direct extensions with fully dynamic data updates and secondly shows how to construct an elegant verification scheme for seamless integration. It manipulates the classic Merkle Hash Tree (MHT) construction for block tag authentication [8].

In 2008 Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn and Farnam Jahanian proposes a new model which gives the concept of possibility to spend bandwidth resources to significantly reduce on-device CPU, memory, and power resources. It shows the in-cloud model enhances mobile security and reduces on-device software complexityandd gives platform-specific behavioral analysis engines. Its benchmarks on Nokia’s N800 and N95 mobile devices show that its mobile agent consumes less CPU and memory while also consuming less power as compared to existing on-device antivirus software [9].

In 2012 Luís Mendonça and Henrique Santos presented the research and tests which define an effective set of traffic parameters capable of modeling both normal and abnormal activity of networks, focusing on botnet activity detection through anomalous and cooperative behavior. It also proposed detection framework prototype which tested using real traffic collected in the University of Minho campi edge [10].

In 2011 Pengfei Sun Qingni Shen, Ying Chen Zhonghai and Wu Cong Zhang proposed a new security load balancing architecture which is based on Multilateral Security (LBMS), when it reaches on peak-load it can migrate tenants’ VMs automatically to the ideal security physical machine. This protocol is based on CloudSim, a Cloud computing simulation. This architecture makes an effort to avoid potential attacks when VMs migrate to physical machine due to load balancing [11].

In 2012 Pragya Jain and Anjali Sardana proposed a novel hybrid scheme that integrates anomaly and signature detection with honeypots. At first level it used Signature based detection for known worm attacks, that makes the system operate in real time. At the second level Any deviation from the normal behavior can be easily detected by anomaly detector and at the Last level is honeypots detects zero day attacks. It gives resource efficient advantage of honeyfarm because it deploys honeypots and both the detectors. The Controller redirects the traffic to the respective honeypots [12].

In 2012 Gaurav Raj and Kamaljit Kaur introduced an protocol which uses the improved Broker Cloud Communication Paradigm (BCCP). It also includes two algorithms first is Secure Optimized Route Cost Finder (S-ORCF) which finds optimum route between broker and cloud on the behalf of cost factor and second is Secure Optimized Route Management (S-ORM) which maintains optimum route. It protocol uses symmetric cryptographic primitives [13].

In 2012 Soumya V L and Anirban Basu proposed a scheme which modifies the BitTorrent protocol for Peer-to- Peer communication. This protocol is used network communication has been discussed and modifications suggested for speeding up file transfer. It improves the performance of cloud [14].

In 2011 Safiriyu Eludiora, Olatunde Abiona2, Ayodeji Oluwatope, Adeniran Oluwaranti, Clement Onime, Lawrence Kehinde introduced a user identity management protocol for cloud computing customers and cloud service providers. This protocol authenticates and authorizes customers/providers to achieve global security networks. The layered protocol design is proposed for cloud computing systems, the physical, networks and application layer. This protocol gives secure data at all levels it protects customers/cloud service providers infrastructure by preventing unauthorized users to gain access to the service/facility [15].

In 2011 Zhuo Hao, Sheng Zhong introduced a protocol which supports public verifiability without help of a third party auditor. In addition, the proposed protocol does not leak any private information to third party verifiers and also gives good performance. It is suitable for providing integrity protection of customers' important data and supports data insertion, modification and deletion at the block level and public verifiability. It is secure against an untrusted server. And also private against third party verifiers. The protocol gives very good efficiency in communication, computation and storage costs [16].

In 2009 Hongwei Li, Yuanshun Dai, Ling Tian, and Haomiao Yang proposed a method based on the identity-based hierarchical model for cloud computing (IBHMCC) and its corresponding encryption and signature schemes. It presents a new identity-based authentication protocol for cloud computing and services. It is more lightweight and efficient than SAP, specially the more lightweight user side. It is suitable for massivescale cloud. It allows the users with an average or low-end platform to outsource their computational tasks to more powerful servers [17].

In 2013 Hongfeng Zhu Tianhua Liu Dan Zhu and Haiyang Li introduced EACS (entangled authenticated cloud storage). The protocol settles the aforementioned typical problem. This scheme has four policies: (i) N-clients can easily "entangle" their files into a single secret c to be store by a cloud storage provider S; (ii) Using secret c, each client may easily recovery their own original file respectively; (iii) If the server alters c in any way, no clients will be able to retrieve its original file (this policy is called all-or-noting-integrity). (iv) All the parties in the entangled scheme should be authenticated. It gives a full specification of this scheme, including how to realize specific policies, how to design the scheme, how to prove the scheme's security [18].

In Yoshiaki Shiraishi and Masami Mohri introduced server-aided computation protocol which uses ElGamal encryption, which is homomorphic. This is secure protocol under the discrete logarithm assumption for passive and active attacks. This protocol is shorter than the original ElGamal encryption [19].

A. *Securing Cloud Service Confidentiality Using Conventional Techniques*

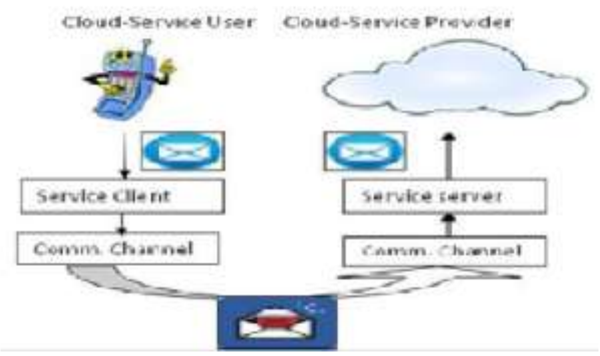

Figure 2: Approach for Maintaining Confidentiality on Cloud -Services

In cloud computing, [19] there are three entities: First is the "cloud service-user"; second is the "cloud infrastructure provider," which runs the data center; and last is the "cloud service-provider," which provides various (compound) services in the cloud. The cloud infrastructure provider and service provider together are called the "cloud provider" It is common in current Web services to secure data on a communication channel to prevent eavesdropping or falsification. SSL/TLS is widely used as the prevention method, but it is not sufficient in the case of cloud services.

B. *Approach for Maintaining Confidentiality on Cloud -Services*

It is desirable [19] that same encryption method be used on the mobile phone as on the desktop PC to improve the convenience for cloud users and expand the viability of cloud-service providers. In the case of a low-spec computer such as a smartphone, the time needed for encryption/decryption must be reduced. Methods to improve the encryption/ decryption speed are as follows: 1) using a high-spec CPU; 2) improving the speed by software programming techniques, and 3) using a server-aided computation method–part of the encryption/decryption processing is done by the server.

C. *Conventional Methods of Server-Aided Computation*

When low-spec [19] computer A encrypts its secret to send it to another computer, it needs a lot of processing time. It is possible to shorten A's processing time by asking high-spec computer B (server) to do a part of its calculation without showing A's secret. This method is called server-aided computing.

D. Protocols using homomorphism

Homomorphic encryption [19] is used as the basic encryption technique in future services such as e-voting questionnaires, electronic cash and electronic auctions. We anticipate that many cloud services will appear, which can use the user's encrypted data stored on a cloud server without decryption. In such cases, it is better to have a Web browser compute the encryption process using homomorphism although there are several studies of server- aided computation using RSA encryption, we have never come across a study of it using homomorphism. We propose a protocol for server-aided computation using ElGamal encryption, which is a class of homomorphic encryption.

In Lamia Youseff and Maria Butrico, Dilma Da Silva proposed a new scheme which uses Ontology. The ontology demonstrates a dissection of the cloud into five main layers, and illustrates their interrelations as well as their inter-dependency on preceding technologies [20].

3. THE CLOUONTOLOGY

Cloud computing [20] systems fall into one of five layers: applications, software environments, software infrastructure, software kernel, and hardware. Obviously, at the bottom of the cloud stack is the hardware layer which is the actual physical components of the system. Some cloud computing offerings have built their system on subleasing the hardware in this layer as a service, we discuss in subsection IV-E. At the top of the stack is the cloud application layer, which is the interface of the cloud to the common computer users through web browsers and thin computing terminals.

A. Cloud Application Layer

B. Cloud Software Environment Layer

C. Cloud Software Infrastructure Layer

D. Software Kernel.

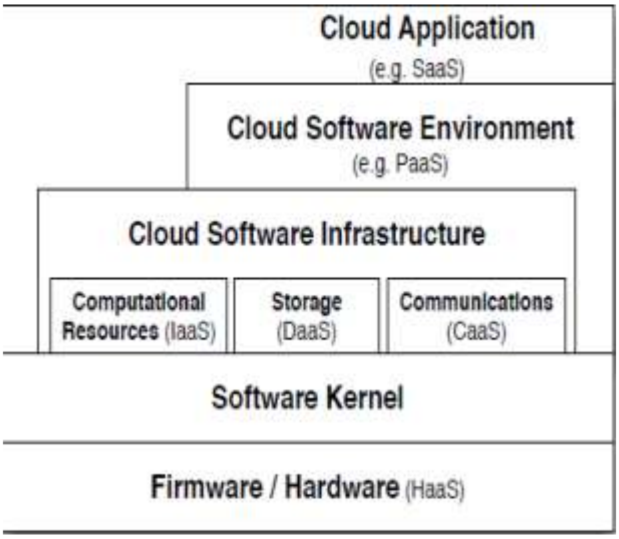
Cloud Application
(e.g. SaaS)
Cloud Software Environment
(e.g. PaaS)
Cloud Software Infrastructure
Computational Resources (IaaS)
Storage (DaaS)
Communications (CaaS)
Software Kernel
Firmware / Hardware (HaaS)

Figure 3: Cloud Environment

In 2011 Narpat Singh Shekhawat and Durga Prasad Sharma defines a hierarchy of natural classes of private cloud applications, and show that no cryptographic protocol can implement those classes where data is shared among clients [21].

4. TRADITIONAL SECURITY

These concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud.

- VM-level attacks. Potential vulnerabilities in the hypervisor or VM technology used by cloud vendors are a potential problem in multi-tenant architectures.

- Cloud provider vulnerabilities. These could be platform level, such as an SQL-injection or cross-site scripting.

- Phishing cloud provider**.** Phishers and other social engineers have a new attack vector.

- Expanded network attack surface**.** The cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases.

- Authentication and Authorization**.** The enterprise authentication and authorization framework does not naturally extend into the cloud.

In 2011 B. Dhiyanesh and A. Thiyagarajan proposed a protocol to maintain the integrity of data in cloud. This can be done by third party auditor (TPA) on behalf of the cloud client to verify the integrity of the dynamic data stored in the cloud. This technique eliminates the interference of Client to check their intactness. It detects the security problems of direct extensions with dynamic data updates and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in our protocol design. To achieve efficient data dynamics, it improve the existing proof of storage models by manipulating the classic Merkle.

Hash Tre construction for block tag authentication. To support efficient handling of multiple auditing tasks, it explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. This scheme is highly efficient and provably secure [22].

5. CONCLUSION

This survey paper simply presents the recent developments, architecture and security issues in the field of Cloud Computing in a simple and collective manner. This paper also provide an overview of the cloud computing and its application.

REFERENCES:

[1] Farzad Sabahi "Cloud Computing Security Threats and Responses" 2011 IEEE, 2011.

[2] Haoming Liang, Wenbo Chen and Kefu Shi "Cloud Computing: Programming Model and Information Exchange Mechanism" Proceedings of the 2011 International Conference on Innovative Computing and Cloud Computing (ICCC '11), PP:10-12, 2011.

[3] Guannan HU and Wenhao ZHU, "A Dynamic User- integrated Cloud Computing Architecture" Proceedings of the 2011 International Conference on Innovative Computing and Cloud Computing (ICCC '11), pp: 36-40, 2011.

[4] Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjitha, patham, and Sangoh Jeong, "Securing Elastic Applications on Mobile Devices for Cloud Computing" Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW '09), pp:127-134, 2009.

[5] Yan Zhu, Huaixi Wang, Zexing Hu, Gail-Joon Ahn, Hongxin Hu, Stephen S. Yau, "Efficient Provable Data Possession for Hybrid Clouds" Proceedings of the 17th ACM conference on Computer and communications security (CCS'10),pp: 756-758, occtober 2010.

[6] Qian Wang, Cong Wang, Jin Li1, Kui Ren, and Wenjing Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing" Proceedings of the 14th European conference on Research in computer security (ESORICS'09). pp: 355- 370,2009.

[7] Arash Nourian and Muthucumaru Maheswaran, "Towards Privacy Enhanced Limited Image Processing in the Clouds" Proceedings of the 9th Middleware Doctoral Symposium of the 13th ACM/IFIP/USENIX International Middleware Conference (MIDDLEWARE '12), Article No. 5, 2012.

[8] Jean Bacon1, David Evans1, David M. Eyers1, Matteo Migliavacca2, Peter Pietzuch2, and Brian Shand3 "Enforcing End-to-End Application Security in the Cloud" Proceedings of the ACM/IFIP/USENIX 11th International Conference Middleware (Middleware '10), pp: 293-312,2010.

[9] Jon Oberheide, Kaushik Veeraraghavan, Evan Cooke, Jason Flinn and Farnam Jahanian, "Virtualized In-Cloud Security Services for Mobile Devices" Proceedings of the First Workshop on Virtualization in Mobile Computing (MobiVirt '08),pp: 31-35,2008.

[10] Luís Mendonça and Henrique Santos, "Botnets: A Heuristic-Based Detection Framework" Proceedings of the Fifth International Conference on Security of Information and Networks(SIN '12),pp: 33-40,2012.

[11] Pengfei Sun Qingni Shen, Ying Chen Zhonghai and Wu Cong Zhang, "POSTER: LBMS: Load Balancing based on Multilateral Security in Cloud" Proceedings of the 18th ACM conference on Computer and communications security (CCS '11), pp: 861-864, 2011.

[12] Pragya Jain and Anjali Sardana, "Defending against Internet Worms using Honeyfarm" Proceedings of the CUBE International Information Technology Conference (CUBE '12), pp: 795-800,2012.

[13] Gaurav Raj and Kamaljit Kaur "Secure Cloud Communication for Effective Cost Management System through MSBE" 2012 International Journal on Cloud Computing: Services and Architecture (IJCCSA),Vol.2, No.3, June 2012.

[14] Soumya V L and Anirban Basu "Modified Bittorrent Protocol And its Application In Cloud Computing Environment" 2012 International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol.2, No.5, October 2012.

[15] Safiriyu Eludiora, Olatunde Abiona2, Ayodeji Oluwatope, Adeniran Oluwaranti, Clement Onime, Lawrence Kehinde. " A User Identity Management Protocol for Cloud Computing Paradigm" 2011 Int. J. Communications, Network and System Sciences, pp: 152-163 March 2011.

[16] Zhuo Hao, Sheng Zhong, Nenghai Yu "A Privacy- Preserving Remote Data Integrity Checking Protocol with Data Dynamics and Public Verifiability" 2011 IEEE Transactions on Knowledge and Data Engineering, Volume:23, Issue:9, Page(s): 1432 – 1437, Sept. 2011.

[17] Hongwei Li, Yuanshun Dai, Ling Tian, and Haomiao Yang "Identity-Based Authentication for Cloud Computing"2009 Springer-Verlag Berlin Heidelberg, pp. 157–166, 2009.