JCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-6, Special Issue-2, March 2018 E-ISSN: 2347-2693

Cloud Computing Security: Multilevel Classified Survey on Attacks and Security Concerns

S.Hendry Leo Kanickam[1*]

SrimadAndavan Arts and Science College
Trichy,India

L. Jayasimman[2]

SrimadAndavan Arts &Scinece College,
Trichy,India

Available online at: www.ijcseonline.org

***Abstract* -** Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network. Today, cloud computing generates a lot of hype; it's both promising and scary. In cloud computing, clouds can be described at different layers, i.e., SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). Although applications for clouds are in development phase, however security requirements for the data and services on the clouds are getting attention of researchers and it has become necessary to consider each layer of a cloud for possible attacks. Thus, it is important to address the security issues and problems in cloud systems, and to find a solution for the widespread acceptance of these solutions. Current system provides the whole security solutions for each and every layer. It leads to waste of energy. We suggested a new mode of security after analysis. The Major idea behind our survey is to concentrate on the particular issues or attacks on the cloud layers instead of focusing whole efforts of security solutions for each and every action. It makes us to build a proper wall against the attackers. Instead of providing all security oriented solutions for all layers, we propose a dynamic security solution according to the corresponding attacks of related layers. It improves cloud service's performance and saves energy of the resources, so that the same can be utilized for more services.

***Keywords* -** Cloud computing security, Layers based Security in Cloud, SaaS, Iaas/Paas, Development Services.

I. INTRODUCTION

In cloud computing, clouds can be described at different layers, i.e., SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). Although applications for clouds are in development phase, however security requirements for the data and services on the clouds are getting attention of researchers and it has become necessary to consider each layer of a cloud for possible attacks. It is worth noting that cloud computing systems have many advantages; however, large organizations are still hesitant to shift their set-ups on the cloud mainly due to security issues and risks. Thus, it is important to address the security issues and problems in cloud systems, and to find a solution for the widespread acceptance of these solutions. However, being a new domain, the research on the requirements and issues regarding security of clouds is still in its early stages. We proposed a new mode of security after analysis. The Major idea behind our survey is to concentrate on the particular issues or attacks on the cloud layers instead of focusing whole efforts of security solutions for each and every action. It makes us to build a proper wall against the attackers. It doesn't mean we didn't provide security for all layers. Instead of providing all security oriented solutions for all layers, we propose a dynamic security solution according to the corresponding attacks of related layers. It improves cloud service's performance and saves energy of the resources, so that the same can be utilized for more services. For Eg: Attack on API should be affect the Saas layers and the attackers focused on to broke SSH, Authentication, Authorization or Publisher credential. It won't be affecting the other kind of services such as platform virtualization, cloud software, computational services in utility computing. So we propose to focus on API oriented security itself.

The analyses took over the past decade proposals on cloud computing proposals and find out the various services provided in cloud computing. It can be around four layers such as Saas, Paas, Iaas and development services.By build a security framework and provide a security solution dynamically for the security concerns related to its layers. So that for API oriented issue such as attack on API the dynamic solution against API attacks can be fetch from security framework. The particular API security package contains as per the fig 1

Some authors in the past decades that the security also provides as a cloud service and it may provide by a vendor, user or customer or any third party. The remaining portion of this paper contains survey from various write-ups, A multilevel classification of security concerns in cloud computing. Finally we conclude with the new suggestion for the survey report.

- **Restrict access to API based on IP Addresses**
- **Rate limit API calls with retry time**
- **Rate limit API calls for Data Batch calls**
- **Data masking of sensitive data from API response**
- **Json threat protection against injection attacks**
- **XML threat protection against injection attacks**
- **Log all API interactions**
- **Threat protection against SQL injection**

Fig 1 . Cloud API Security Solution Package

II. RELATED WORK

In [1] Cloud Computing Open Architecture (CCOA) concept is discussed for clouds in virtual environments. The role and functions of the architecture are discussed according to different infrastructures for IT and business systems. Different types of architectures complicate security management for cloud systems. This architecture provides a solution for different security aspects regarding virtual environments. Authorized users based on the role-based access control can access the sensitive data on platforms. To pre-vent intrusion attacks, cloud service provider blocks the malicious and un-trusted codes enabling digital forensic applications.The application softwares at SaaS are provided with a specific license based subscription, pay-as-go [3]. Platform as a Service (PaaS) caters services for operating system, network capacity, storage and multi-tenancy via the Internet. Infrastructure as a service (IaaS) provides utility computing, automation of administrative tasks, dynamic scaling, desktop virtualization, policy-based services, and Internet connectivity. IaaS provides virtual servers with unique IP address and storage pool as required by customers. Infrastructure and hardware layers may be combined due to intrinsic relationship between hardware and software.

In [4], security aspects of one of the popular cloud Amazon Elastic Compute Cloud (EC2) have been discussed. It consists of systematic analysis of various crucial vulnerabilities in publicly available Amazon Machine Images (AMIs) and mechanisms to eliminate them. The proposed tool referred to as Amazon Image Attacks (AmazonIA) uses only publicly avail-able interfaces regardless of the underlying cloud infrastructure. The extracted information can be used to initiate botnets, or create back doors to launch impersonate attacks or access source code of a web service available on AMI. Some research groups have worked on the interfaces of both public and private clouds [5]. The public cloud under their consideration is Amazon, while the private cloud is Eucalyptus.

Authors in [6] consider security as a service for cloud-based applications. The architecture considers the existing ser-vices at different levels. It considers user-centric security i.e., users have control over their security permitting them to use security solutions across different clouds. They can subscribe to any security solution provided by any cloud provider and use that particular security solution for their cloud and may also have multiple security solutions for a particular service depending upon its criticality. The multiple security solutions can also be used at different levels.

Authors in [7] address the security and privacy aspects of real-life cloud deployments, while ignoring the malicious cloud providers or customers. Vulnerabilities were discovered in Secure Shell. The extracted information can be further used to create multiple security threats resulting in botnet instances, access of backend services or code of the Web sites through back-doors content.

In [8] authors suggest that security should be provided as a service and propose a model for security as service. Security as a service implies that the security applications and services can be provided by a cloud vendor, or cloud consumer or even by a third trust-worthy party. The security service can be in the form of a cloud-based infrastructure or software. An eXtensible access control markup language (XACML) decision engine that is composed of a context handler, a policy decision point and a policy administration point, can be furnished by reusable com-ponents to augment the security service. Thus, these types of security services, which can be managed and altered by cloud customers, are helpful to build trust of cloud customers on cloud systems.

Research in [9] suggests a trusted computing and attestation system for virtual environments. In virtual environments systems are more prone to threats due to the poor computer communication architectures and hidden network channels.

III. METHODOLOGY

A multilevel classification of security concerns in cloud computing

Cloud systems have a layered architecture of different services and control levels for users. Fig.2 illustrates the classification model of security problems at each layer of the cloud system.SaaS, PaaS and IaaS layers are considered for associated security risks and problems.

A. Security concerns for Software as a Service (SaaS)

SaaS is exposed by attacks on API's, publishers, web portals and interfaces. The attacks on the SaaS are categorized into two broad groups: attacks on development tools and attacks on management tools. Most popular services on SaaS are web services, web portals and APIs. Intruders' attempt un-authorized access and gain of services by attacking web portals and APIs. These attacks affect data privacy. Intruders try to extract the sensitive information of API Keys, private keys, and credentials of publishers via different kinds of attacks and automated tools. Another possibility of attack on this layer is exposure of secure shell for extracting key credentials.

Data protection

In cloud computing applications are deployed in shared resource environments; therefore, data privacy is an important aspect. Data privacy has three major challenges: integrity, authorized access and availability (backup/ replication). Data integrity ensures that the data are not corrupted or tampered during communication. Authorized access prevents data from intrusion attacks while backups and replicas allow data access efficiently even in case of a technical fault or disaster at some cloud location. Hence malicious attackers or intruders can deploy hidden proxy applications between the cloud provider and consumer to scavenge information of login credentials and session details [2]. An intruder can also per-form packet sniffing or IP-spoofing as a middle-party and can access and/or alter the restricted or sensitive information. One possible solution for the data privacy in cloud computing is Cisco Secure Data Center Framework that provides multi-layer security mechanism [2]. Data Breaches are the risk of data breach is not unique to cloud computing, but it consistently ranks as a top concern for cloud customers.**Dataloss**:Data stored in the cloud can be lost for reasons other than malicious attacks, the permanent loss of customer data unless the provider or cloud consumer takes adequate measures to back up data, following best practices in business continuity and disaster recovery.

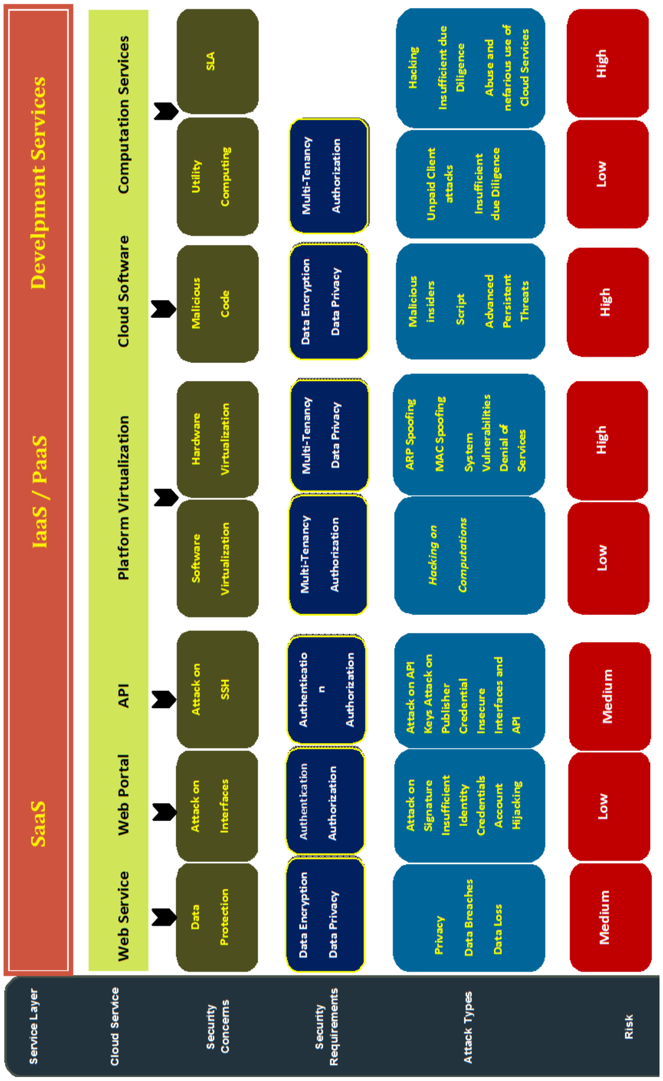
Service Layer
Develpment Services
IaaS / PaaS
SaaS
Cloud Service
Computation Services
Cloud Software
Platform Virtualization
API
Web Portal
Web Service
Security Concerns
SLA
Utility Computing
Malicious Code
Hardware Virtualization
Software Virtualization
Attack on SSH
Attack on Interfaces
Data Protection
Security Requirements
Multi-Tenancy Authorization
Data Encryption Data Privacy
Multi-Tenancy Data Privacy
Multi-Tenancy Authorization
Authenticatio n Authorization
Authentication Authorization
Data Encryption Data Privacy
Attack Types
Hacking Insufficient due Diligence Abuse and nefarious use of Cloud Services
Unpaid Client attacks Insufficient due Diligence
Malicious insiders Script Advanced Persistent Threats
ARP Spoofing MAC Spoofing System Vulnerabilities Denial of Services
Hacking on Computations
Attack on API Keys Attack on Publisher Credential Insecure Interfaces and API
Attack on Signature Insufficient Identity Credentials Account Hijacking
Privacy Data Breaches Data Loss
Risk
High
Low
High
High
Low
Medium
Low
Medium

Fig 2 . Classification model of security problems at each layer

Attacks on interfaces

A successful attack on the cloud interfaces can result in a root level access of a machine without initiating a direct attack on the cloud infrastructure. Two different kinds of attacks are launched on authentication mechanism of clouds. The control interfaces are vulnerable to signature wrapping and advanced cross site scripting (XSS) techniques. First kind of attack is referred to as signature wrapping attack or XML Signature Wrapping attacks. Second type of attacks exploits the vulnerability in XSS. The particular vulnerability attack steals username and password pair information. Insufficient identity, credential, and access management these can enable unauthorized access to data and potentially catastrophic damage to organizations or end users.

Account Hijacking

Account Hijacking or service instances might become a new base for attackers. With stolen credentials, attackers can often access critical areas of cloud computing services, allowing them to compromise the confidentiality, integrity, and availability of those services.

Attacks on SSH (Secure Shell)

Attacks on Secure Shell (SSH), the basic mechanism used to establish trust and connection with cloud services, are the most alarming threat that compromises control trust. According to Ponemon 2014 SSH security Vulnerability Report [10], 74 % organizations have no control to provision, rotate, track and remove SSH keys. Cybercriminals take full advantage of these vulnerabilities and use cloud computing to launch different attacks. An organizations cloud workload can be used host botnets if SSH access has been compromised. Attackers have hosted the Zeus botnet and control infrastructure on Amazon EC2 instances [11]. The different types of attack on SSH include attacks on API keys, attacks on user credentials, and attacks on publisher credentials.

B. Security issues for Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)

IaaS and PaaS layers area unit overlapped within the model as a result of their mutuality on each other. The attacks on these layers area unit classified into 3 types: attacks on cloud services, attacks on virtualization, and attacks on utility computing. The protection issues for IaaS and PaaS area unit mentioned below.Insecure interfaces and application programming interfaces (APIs) are Cloud providers expose a set of software user interfaces (UIs) or APIs that customers use to manage and interact with cloud services.To protect against accidental and malicious attempts to circumvent policy.

Hardware virtualization

The VMs interconnectivity is that the biggest security concern within the planning of cloud computing platform. VMs area unit coupled victimization bridge and route virtual network configuration modes. The bridge mode works as a virtual hub shared among all the VMs, which can end in sniffing the virtual network by a compromised VM. Within the route mode, wherever route works as a virtual switch, every VM is connected employing a dedicated virtual interface. Any network trespasser in an exceedingly LAN section of a network will access virtual environments by address resolution protocol (ARP) spoofing and waterproof spoofing. Hans Arp spoofing alters the Hans Arp tables and management interfaces and systems [8]. The attacks and exploitation of virtual environments area unit terribly diversified and that they can increase in future since platforms area unit growing in variety and quality. Therefore, a mechanism for sleuthing attacks beside preventions is important.

System vulnerabilities are exploitable bugs in programs that attackers can use to infiltrate a system to steal data, taking control of the system or disrupting service operations.(DoS) are designed to prevent users of a service from being able to access their data or applications. system resources such as processor power, memory, disk space, or network bandwidth, attackers can cause a system slowdown.

Software virtualization

A software package virtualization attack could examine the VM pictures to launch AN attack or steal of knowledge, particularly targeting development pictures, that area unit accidentally free [16]. It's conjointly attainable to produce a VM image having malware to cloud computer system leading to thieving and corruption of information.

Cloud software

Multi-tenancy in clouding up computing needs multiplexing the execution of VMs from completely different shopper on identical physical server [12]. Software deployed on guest VM stay susceptible to attack and compromise. A malicious code in VM could interfere with the hypervisor or different VMs. Shortcomings in programming interfaces and process of directions area unit the most targets to uncover vulnerabilities [13]. A malicious insider such as a system administrator can access potentially sensitive information, and can have increasing levels of access to more critical systems and eventually to data. APTs are a parasitical form of cyber attack that infiltrates systems to establish a foothold in the IT infrastructure of target companies, from which they steal data.

C. Utility computing

Utility computing is that the thought that emerged from grid com-puting, and it combines computation, storage and information measure to produce services on the demand through payment by the client. It conjointly provides 2 basic blessings of price reduction and measurability. Security risk related to utility com-putting is access by attackers United Nations agency need to utilize resources while not paying [3]. The common use of public cloud includes e-commerce, web-application and information processing system hosting creating these services susceptible to variety of attacks on possession, credibleness, and integrity and utility. A compromised shopper could perform a dishonorable Resource Consumption (FRC) attack by victimization the metered information measure of web-based service that leads to a monetary burden on the cloud shopper [14].Insufficient due diligence areOrganizations that rush to adopt cloud technologies and choose providers without performing due diligence expose themselves to a number of risks.

D. Service Level Agreement (SLA)

SLA is a best manner for guaranteeing security and trust. The implementation of SLA leads to a well-designed contract of responsibilities between parties that may enhance security level. In cloud atmosphere, SLA is combined with the net service level agreement (WSLA) for mitigating security risks [3]. SLA defines the various levels of security and their complexity supported the services for the higher understanding of the safety policies to a cloud shopper. The prevailing cloud storage systems don't give security guarantees in their SLAs affecting the difference of cloud services. A cloud storage service could leak non-public information, come inconsistent data or modify the info as a result of bugs, hacking, crashes, or mis-configurations. This security issues need correct SLA guarantee models like Cloud Proof [15].Abuse and nefarious use of cloud services providespoorly secured cloud service deployments, free cloud service trials, and fraudulent account sign-ups via payment instrument fraud expose cloud computing models to malicious attacks.

IV. CONCLUSION AND FUTURE SCOPE

The above analyses took over the past decade proposals on cloud computing proposals and find out the various services provided in cloud computing. It can be around four layers such as Saas, Paas, Iaas and development services. By build a security framework and provide a security solution dynamically for the security concerns related to its layers. It improves cloud service’s performance and saves energy of the resources, so that the same can be utilized for more services. While the energy of the resources saves the price of the services also reduced. So the above said solution is optimum for economical also. In future it leads for new innovative approaches and turn into the products.

REFERENCES

[1] S.S. Yeo, J.H. Park, Security considerations in cloud computingvirtualization environment, Grid Pervasive Comput. LectureNotesComput. Sci. 7861 (2013) 208–215.

[2] H. Yu, N. Powell, D. Stembridge, X. Yuan, Cloud computingand security challenges, in: Proc of the 50th Annual SoutheastRegional Conference (ACM-SE12), ACM, New York, USA,2013, pp. 298–302.

[3] P. Arora, R.C. Wadhawan, E.S.P. Ahuja, Cloud computingsecurity issues in infrastructure as a service, Int. J. Adv. Res.Comput. Sci. Softw. Eng. 2 (1) (2012) 1–7.

[4] S. Bugiel, S. Nurnberger, T. Poppelmann, A.R. Sadeghi, T.Schneider, AmazonIA: when elasticity snaps back, in: Procofthe 18th ACM Conference on Computer and CommunicationsSecurity (CCS11), ACM, 2011, pp. 389–400.

[5]J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N.Gruschka, L.L. Iacono, All your clouds are belong to us:security analysis of cloud management interfaces, in: Proc. of the3rd ACM workshop on Cloud Computing Security Workshop(CCSW11), ACM, 2011, pp. 3–14.

[6] M. Hussain, H. Abdulsalam, SECaaS: security as a service forcloud-based applications, in: Proc. of the Second KuwaitConference on e-Services and e-Systems (KCESS11), ACM,2011, pp. 1–4.

[7] R. Laborde, F. Barre`re, A. Benzekri, Toward authorization as aservice: a study of the XACML standard, in: Proceedings of the16th Communications & Networking Symposium, Society forComputer Simulation International, 2013, pp. 1–7.

[8]G. Pek, L. Buttyan, B. Bencsath, A survey of security issues inhardware virtualization, ACM Comput. Surveys 45 (3) (2013) 1–34ACM.

[9]M. Pearce, S. Zeadally, R. Hunt, Virtualization: issues, securitythreats, and solutions, ACM Comput. Surveys 45 (2) (2013) 1–39ACM.

[10]L. Ponemon, Ponemon 2014 SSH security Vulnerability Report Retrieved from http://www.venafi.com/collateral/wp/ponemon-2014-ssh-security-vulnerability-report2014.

[11]Zeua, Zeus Botnet Controller Retrieved from http://aws.amazon.com/security/zeus-botnet-controller/2009.

[12]T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Get off of mycloud: exploring information leakage in third-party computeclouds, in: ACM Conference on Computer and CommunicationsSecurity, ACM, 2009.

[13]Zeua, Attacks on Virtual Machine Emulators, White Paper Symantec Corporation http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf2007.

[14]J. Idziorek, Exploiting Cloud Utility Models for Profit and RuinGraduate Theses and Dissertations, Lowa State University,2012.

[15]R.A. Popa, J.R. Lorch, D. Molnar, H.J. Wang, L. Zhuang,Enabling security in cloud storage SLAs with CloudProof, in:Proc. of the 2011 USENIX Conference on USENIX AnnualTechnical Conference, 2011, 31-31.

[16]J. Wei, X. Zhang, G. Ammons, V. Bala, P. Ning, Managingsecurity of virtual machine images in a cloud environment, in:ACM Cloud Computing Security Workshop (CCSW?09),ACM, 2009.