SECURITY CHALLENGES AND POLICIES IN CLOUD COMPUTING FOR SERVICES

Dattatray B.P[1], Devare A.S.[2]

[1]*PG Scholar, Computer Department, JSPM Narhe, Maharashtra, India*
[2]*Asst. Professor, Computer Department, JSPM Narhe, Maharashtra, India*

Abstract

Cloud computing is becoming most emerging trend in IT industry. With its potential growth and lucrative services cloud computing has acquired mass market in the industry large enterprises running their business on the cloud. A greater acceptance of public cloud by various businesses has given it a wide popularity, strengthening of public cloud security is big milestone. The public cloud acceptance is increasing along with the trust in public cloud at large extent. As the security is most vital factor in the cloud. Handovering data to the cloud service provider keeps cloud user tensed. Different threats have been discovered in recent years. Database security in public cloud raised some critical issues for cloud service provider. This rapid adaptation to the clouds, have increased concerns on a critical issue for successive growth of communication technology and information security. From a cloud security perspective, a number of unexplored risks and challenges are faced by cloud because of migration, causing degradation of the effectiveness of traditional protection mechanisms.

Keywords: *Cloud computing, Cloud DBaaS, public cloud, Cloud Security, Confidentiality, Trust, Encryption.*

***

1. INTRODUCTION

Cloud computing becomes prominent and minimal investment sector for IT businesses. Recent facts about cloud computing has shown the emerging trends and wide acceptance of cloud computing. Near about 75% organizations are now sure in security of information assets in the cloud, inspiring more organizations to accept cloud solutions. During last year, investment in cloud has increased by 10% to an average of $1.5 million a recent study by IDG on cloud computing revealed facts. In upcoming period, over half of the capitalization will be spent on cloud computing. The 61% organizations have computing infrastructure in the cloud at some portion, and 29% organizations operations will be in the cloud within the next five years [1].

Public cloud has acquired larger space in IT services than the private cloud, workload analysis reported massive growth in this sector. The CAGR analysis shows there is rise in workload by 24% from 2013 to 2018, the public cloud workloads will grow by 33% from 2013 to 2018 where private cloud workloads will grow at a steady rate of 21 % from 2013 to 2018[2].

1.1 Cloud Service Models

Cloud service models achieved a major space in cloud computing area. The service model helps to dictates an organization's scope and control with its computational resources, and characterizes a level service for its use.

1.1.1 SaaS

Software-as-a-Service is a service delivery model providing applications and computational resources for use on demand by the service user. Purpose of this model is to reduce the total development cost, including maintenance, and operations. Security is responsibility of cloud provider. The cloud consumer isn't involved in control and management of cloud infrastructure or personal applications, except for priority selections and very less administrative application settings.[3] Workload density will be 59% software as a service, compared to 28% IaaS and 13% PaaS by the end of 2018.

1.1.2 Paas

Platform-as-a-Service is a service delivery model that provides the computing platform and applications can be developed and deployed on it. Motivation behind this model is to minimize cost, complexity of purchasing, hosting, and managing platform, including programs and databases. The development culture is typically provided by cloud provider and supplemented to the design and architecture of its platform[3].

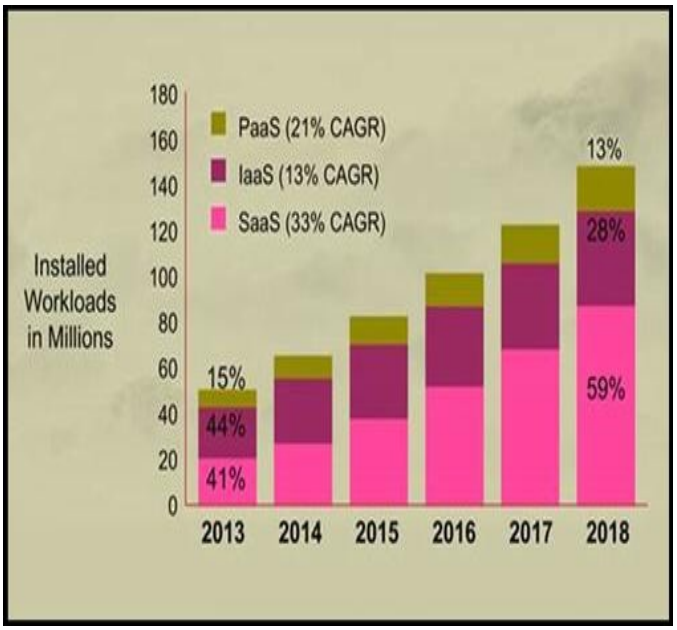

Fig: 1 Global Cloud Index [CISCO][2013-2018].[2]

Figure 1 shows that majority of workload traffic will be covered by SaaS, and Paas will be second fastest growing service.[2]

1.1.3 IaaS

Infrastructure-as-a-Service is a service delivery model services basic computing infrastructure including servers, software, and network equipment provided on-demand service. Platform for developing and executing applications can be established on it. Main motto is to avoid purchasing, and management of software and infrastructure components, and instead get such resources as virtualized objects controllable via a service interface. The cloud user has great freedom for the choice of operating system and development environment to be used. Security is sole responsibility of cloud consumer. [3]

1.1.4 DBaaS

Database as a Service (DBaaS) potentially will be the next big era in IT. It is a service that is hosted by a cloud operator (public or private) and includes applications, where the application team doesn't have any responsibility for old database administration. With a DBaaS, the application developers need not to be expertise in database, and there is no need to hire a database administrator (DBA) to operate and maintain the database.[6] The recent market analysis from 451 research projects shows stunning 86% progressive annul growth rate, with revenues from DBaaS providers rising from $150 million in 2012 to $1.8 billion by 2016.[1] DBaaS is gaining popularity because it eases businesses to setup new databases quickly with high security and at very minimal cost . Database as a Service (DBaaS) offers organizations speed up deployment, elasticity, fair consolidation efficiency, higher availability, and minimal cost and complexity.[2],[4]

Following facts shows why DBaaS will hit the upcoming IT market.

- DBaaS reduces database straggle.
- Supports ease provision.
- Enhance high Security and minimal complexity.

1.2 Cloud Deployment Models

Four deployment models are present for cloud service solutions:

1.2.1 Private Cloud

Infrastructure provided for a private organization. It may be responsibility of organization to manage it or third party can manage it. Existence of such cloud may be on the premise or off the promise.

1.2.2 Community Cloud

Many organizations share the infrastructure and support a distinct community that has general concerns. Organization can manage it or third party can also operate it. Existence of such cloud may be on the premise or off the promise [3].

1.2.3 Public Cloud

This cloud infrastructure is available to public or a large industry group. An organization may own it to sale cloud services [3]. The growth in workload migration from private cloud to public cloud has increased. CISCO reported that workload density for public cloud will increase by 14% by year 2018[2]. The average workload in public cloud will not have more difference than the private cloud.

1.2.4 Hybrid Cloud

Cloud infrastructure is a combination of two clouds i.e. private, community, or public, it doesn't change its properties, but tightened together by standard or proprietary techniques, that enables communication of data and applications.

2. CLOUD COMPUTING SECURITY ISSUES

Data security is an important aspect where quality of service is considered as a prime focus, Cloud Computing undoubtedly raise new security threats for various reasons. Traditional cryptosystems can not directly used because user does not have control over data under Cloud Computing. Checksum for correct data storage in the cloud must be done without knowledge of whole database or data.

2.1 Trust

In cloud trust rely on deployment model as it provides administration of data. Trust is considered as mandatory security policy in old architectures. In public cloud whoever is the owner of infrastructure they have the controls over it. While the public cloud id deployed the infrastructure owner is supposed to take all assurance regarding the suitable security policies so that the risk related to security are reduced. Security is considered about trusting the process or

implementations that are made by owner. Deployment models must differentiate among themselves as the private cloud infrastructure is controlled by private organizations and it do not need any other security policies as organization maintains same trust level.[10]

2.2 Threats

The CSA (Cloud Security Alliance) has discovered various cloud computing threats during last year. The report reflects the current issue among experts around the IT business industry analyzed by CSA , pointing on threats specifically related to shared technology , on-demand service nature of cloud computing[5],[6],[7].

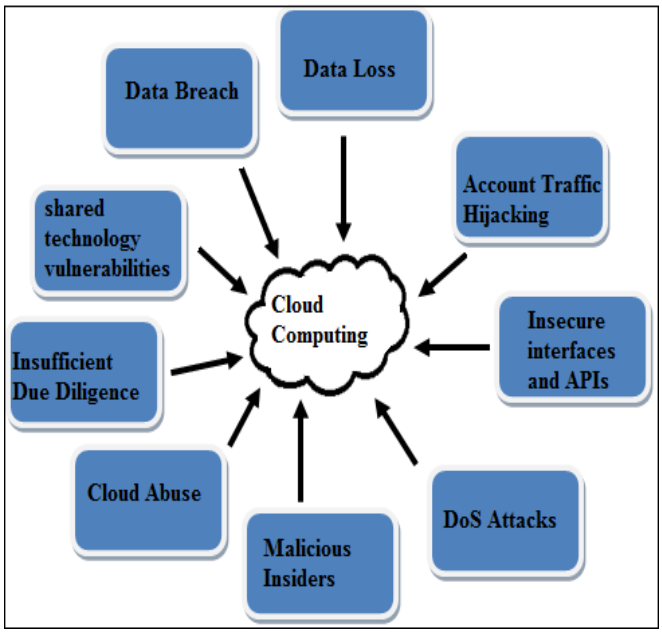

Fig 2: Cloud Threat Model [CSA][2013].[5]

2.2.1 Data Breach

The data breach becomes a serious threat, its presence violated data of near about 110 million individuals targeting on personal and credit data, it took place during the initial processing and storage of information. Cloud computing finds new place of attack CSA reported as a prime threat that attack on targets. The complete security of hypervisor operation and VM operations is still an open research. Question still arises about security existence. Some theoretical assumptions and rare evidences proved that breaches via hypervisors and virtual machines may occur. It's possible for cloud user to listen for activity indication of encryption key on different VM on the same node**. [5]**,[6].

2.2.2 Data Loss

Data is lost when a disk drive crashes and the owner has not created the backup. Data is also lost when the owner loses the key to decrypt the encrypted data. There are few examples shown this data loss due to human operators mistakes (e.g: "remirroring" Amazon EC^2 -2011) [5]. Data loss also may occur due to malicious attacks.

2.2.3 Account Traffic Hijacking

Account hijacking concerns more about account holders credentials and exploitation to personal data can lead to loss of control over user accounts. An attacker can manipulate users data, interfere in transactions, can generate wrong business responses to customers. An account hijacking lets attacker into authorized zone where deployed services may be compromised [5]. In 2009, NASA and Bank of America faced malware attack and in 2010, amazon.com had suffered cross-site scripting attack [2].

2.2.4 Insecure Interfaces and APIs

Organizations may be victim of threats if the service provision is happening with less secure interfaces or API. Interfaces must be developed strong enough to oppose tampering to its services. Authentication , encryption and access control should be secured through high class design of APIs.[7]

Table 1: Threats and their security violations

Sr. No	Type of attack	Security Violations
1	Data Loss	Availability, Integrity
2	Data Brach	Confidentiality, Information Disclosure
3	Account Hijacking	Authenticity, Integrity, Confidentiality, Non-repudiation, Availability, Tampering with Data, Repudiation, Spoofing , Information Disclosure, privilege violation .
4	Insecure Interfaces and APIs	Authenticity, Integrity, Confidentiality, data tampering
5	Denial of Service	Availability, Denial of Service
6	Malicious Insider	Spoofing, Tampering, Information Disclosure
7	Cloud Abuse	Violation to SLA, traffic disruption
8	Insufficient Due Diligence	Authenticity, Integrity, Confidentiality, Non-repudiation, Availability, Tampering with Data, Repudiation, Spoofing , Information Disclosure, privilege violation.
9	Shared Technology	Information Disclosure, privilege violations.

2.2.5 Denial of Service Attacks (DoS)

Denial of service is the traditional disturbance creator for the online operations still they are the threats [5]. Attackers tries to assault quickly and in scattered way before the cloud user get an idea about attack Considering cloud services denial of service attack attacks users services and exploit user authorization without shutting down the

service. Cloud user will be metered for services of all the resources used the period of attack. Continuous DoS attack may make it too critical for running user services [5], [8].

2.2.6 Malicious Insiders

Malicious Insiders is a ordinary threat. If the Malicious Insiders attacker is present in a big cloud organization then the hazards are seen easily. The cloud customer must protect the encryption key in their own place rather than on cloud [5]. The insider attack may poses if the keys are available at the time of use and is not kept with customer. The risk is high when a customer depends totally on cloud service provider for security.

2.2.7 Cloud Abuse

Cloud computing has large scale, flexible services to organizations users and to hackers also. The attacker may take year to crack the encryption key using its own hardware. The attacker may crack it in minutes by using number of cloud services. The hacker can introduce DDoS attack or act as malware or spread the pirated software's. Service provider is responsible for the use of cloud services. Customer must keep track of the services they get from service provider.

2.2.8 Insufficient Due Diligence

Organizations enter into cloud without sufficient knowledge of scope and policies of undertaking. Without an understanding of protection policies, environment of service provision customers tackles about what to expect from cloud service provider. What security policies use, encryption use, incident response; such factors not clearly knowing, organizations forcing themselves to high risk level [7].

2.2.9 Shared technology Vulnerabilities

In multitenant cloud environment, infrastructure is shared and inappropriate configuration of application or operating system leads to breach of security or compromises the infrastructure. CPU caches, shared services or shared databases may be compromised [5]. Threat to entire infrastructure can exploit customer's privacy credentials.

3. SECURITY POLICIES IN CLOUD

Cloud providers are emphasizing more on the security in-depth. Cloud services promising customers with standardized security solutions by taking security more seriously. Wide popularity of cloud computing made it hot spot for intruders and attackers to move on. Security discussions have focused some of the prime areas to ensure confidentiality, availability, integrity of data and applications in cloud.

3.1 Data Protection

Data stored in cloud (public or hybrid) placed in shared infrastructure with integration of distributed data from geographically dispersed nodes. Organizations storing data in public cloud infrastructure must protect data by controlling access to data and keep it securely [4]. Data contains everything about user profiles; transaction details make it easy for attacker to exploit cloud data instead of individuals. Cloud applications that include application programs, configurations and scripts also include account information of users. To prevent access to these fields identity based control is provided [8], [10].

3.2 Identity and Access Management

Complexity of managing identities increases along with increment in cloud services by the companies. Organizations sometimes lose control over services. There must be sound policy provision for identity based access. Permission grant to users to get work done and need information must be provided. Organizations using cloud services are restricted by security compliance rules that assure their identity and access management. [7]

3.3 Security Assessment

Cloud users should move forward to the assessment task. Understanding risk is major component of cloud infrastructure security [9]. Assessment in particular beneficial to provide validation while migrating to cloud and will not negate the affection in security perspective and risk assessment. In addition to these, there are some instances that provide extra protections that may be required. Having security assurance and policies integrated together with organizations risk assessment goals can add benefits to both cloud environment and cloud service users [8].

4. CONCLUSION

This survey paper yields some analysis that has an impact on organizations that uses cloud services as a prime choice. Cloud computing services offer different levels of security to its users though it is challenging and complex. The third party trust and cloud service provider's view towards cloud services has a major impact on organizations. However, user should be very curious about to know the security risks and challenges highlighted in utilizing such technologies. Cloud computing is no exception for threats that are major concern in today's world. Security policies in cloud computing now are attracting business enterprises.

ACKNOWLEDGEMENTS

I sincerely thank to A.S. Devare for his continuous and constructive support. I would also like to thank M. V. Borole for encouraging the work on cloud computing. I would also like to thank V.S. Gaikwad for his helpful comments on the paper.

REFERENCES

[1] www.idgenterprise.com/dig-deeper-for-cloud-investment-decisions

[2] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html

[3] W. Jansen and T. Grance, “Guidelines on Security and Privacy in Public Cloud Computing,” Technical Report Special Publication 800-144, NIST, 2011
[4] H. Hacigu¨mu¨ s¸, B. Iyer, and S. Mehrotra, “Providing Database as a Service,” Proc. 18th IEEE Int’l Conf. Data Eng., Feb. 2002
[5] Cloud Security Alliance (2010) Top Threats to Cloud ComputingV1.0.Available:https://cloudsecurityalliance.org/research/top-threats.
[6] http://www.cloudtweaks.com/2012/10/insider-threats-to-cloudcomputing/
[7] http://www.darkreading.com/insiderthreat/167801100/security/news/240146276/cloud-s-privilegedidentity-gap-intensifies-insider-threats.html
[8] Tadapaneni, N. R. Different Types of Cloud Service Models. Available at SSRN 3614630.
[9] Sara Qaisar, Kausar Fiaz Khawaja, “Cloud Computing: Network/Security Threats and counter measures”, Interdisciplinary Journal of Contemporary Research in Business, ijcrb.webs.com, January 2012, Vol 3, N0 9, pp: 1323 – 1329. .
[10] Kandukuri BR, Paturi VR, Rakshit A. Cloud security issues. In: IEEE international conference on services computing, 2009, p. 517–20.
[11] D. Agrawal, A.E. Abbadi, F. Emekci, and A. Metwally, “Database Management as a Service: Challenges and Opportunities,” Proc. 25th IEEE Int’l Conf. Data Eng., Mar.-Apr. 2009
[12] Chauhan, S., & Vermani, S. (2016). Shift from Cloud Computing to Fog Computing. Journal of Applied Computing, 1(1), 25-29.