Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/5398
DOI URL: http://dx.doi.org/10.21474/IJAR01/5398

RESEARCH ARTICLE

AN ANALYSIS OF CLOUD COMPUTING MULTITENANCY SECURITY CHALLENGES.

Amira Hosni.
Arab Academy for Science and Technology and Maritime TransportCairo, Egypt.

Manuscript Info

Manuscript History

Received: 11 July 2017
Final Accepted: 13 August 2017
Published: September 2017

Key words:-
Cloud Computing, Multitenancy, Security, Threats.

Abstract

Cloud computing is becoming the trend of information technology computational model and the cloud security is becoming a major issue in adopting the cloud for large customers [28]. Such concerns are driven by the multitenancy situation where more than one tenant are utilizing the same physical computer hardware and sharing the same software and data [1]. This has associated risks where confidentiality and/or integrity can be violated [28]. Therefore in order to propose effective security solutions and strategies a good knowledge of the current cloud implementations and practices must be acquired [28]. Such knowledge is needed in order to recognize attack vectors and attack surfaces [28]. This paper explores the specific risks in cloud computing due to multitenancy and the measures that can be taken to mitigate those risks. Before that a clear understanding of multitenancy and its benefits are demonstrated.

Introduction:-

Multitenancy is the practice of placing multiple tenants on the same physical hardware to reduce costs to the user by maximizing the advantage of economies of scale [1]. Tsai defines a tenant as an instance of a virtual machine in the cloud or a human being [4]. In the multitenancy model, many users' data and resources are located in the same cloud and controlled and identified by the use of tagging of resources owned by an individual user [2]. In a typical multitenancy situation, the users are the tenants and are provided with a level of control to allow them to customize and tailor software and hardware to their needs [2].

The cloud service providers offer multitenancy to gain advantage of the economies of scale which translate into savings for the end user [1]. Moreover multitenancy is a popular way to reduce the cloud services providers total cost of ownership of their IT infrastructure [6]. However, multitenancy introduces a unique set of security risks which has yet to be fully acknowledged by policy makers and cloud service providers [2]. This paper exploits the security threats associated with multitenancy and some of the measures to mitigate them.

The paper is organized as follows section two is the related work, section three are the security risks, section four are the countermeasures and section five is the conclusion.

Related Work:-

Multitenancy has been identified as a security issue by several researchers such as [11] who conducted a survey on security issues in service delivery models and stated that multitenancy is a major characteristic that may lead to confidentiality violation. Ref. [12] identified also multitenancy as a major threat to both confidentiality and privacy.

Corresponding Author:-Amira Hosni.
Address:-Arab Academy for Science and Technology and Maritime Transport Cairo, Egypt.

Moreover, [13] highlighted shared technology vulnerabilities as one of the top threats to cloud computing in a survey done on the existing literature. In addition, [14] recognizes multitenancy as a new source of threat in cloud computing infrastructure.

Ref. [15] links between multitenancy as a form of shared environment and the attraction of malicious activities in the cloud. Intel IT Center [16] generated a document of best practices on building secure clouds and clearly highlights multitenancy and shared technology as security challenges for a cloud environment. Ref. [17] in his work proposed a layered security approach for cloud computing and states that virtualization is one of the servers issues where competitors will have separate virtual machines in the same physical machine; hence multitenancy.

In [18] under data governance the writer highlighted that multitenancy arrangements are raising questions about data segregation. NIST developed a report titled "Guidelines on Security and Privacy in Public Cloud Computing"; they identified multitenancy as a downside in the cloud [18]. Ref. [19] interviewed five leading scientists from the cloud community, the chief scientist for Search and Cloud Platforms at Yahoo! was one of them. His response to the question what would you say are the key fundamental challenges of cloud computing that should be addressed by new research in the field? Included multitenancy as a fundamental challenge of cloud computing. Ref. [20] raised questions in how cloud computing affecting security, privacy and trust and he identified multitenancy as one of the security issues.

Cloud Security Alliance (CSA) released a document titled "Security as a Service" [21] that tries to define categories for services. They raised the question of data isolation in multitenant environment. In addition, CSA in the same document stated that multitenancy is creating new targets for intrusion. In a study by [22] to identify the challenges of security and privacy in cloud computing, multitenancy is recognized as one of unique implications of security and privacy in cloud computing. Ref. [23] defines multitenancy as a major characteristic of cloud computing and a major dimension in the cloud security problem that needs a vertical solution from the SaaS to the IaaS. Ref. [24] highlight that multitenancy may enable information leakage and increase attack surface. Moreover [25], [26], and [27] considered multitenancy as a serious issue in cloud security.

Multitenancy Security Threats:-

The security issue with multitenancy is the very premise, in which multitenancy is based on; that is multiple tenants sharing the same computer hardware, software and data [1].One of the main challenges of this multiple services is ensuring data isolation as several users will be using the same data and resources but all require privacy and confidentiality [2]. Moreover lack of network isolation among tenants make the cloud vulnerable to attacks [3].In addition, lack of efficient bandwidth and traffic isolation makes multitenancy in cloud computing vulnerable as malicious tenants may launch attacks towards tenants on the same cloud data center [3].

Additionally access control on clouds does not scale well to multitenancy requirements as they are based on individual IDs [4]. By its nature multitenancy has increased security risks due to the sharing of software and data by multiple tenants [1]. If the barriers between the tenants are broken down, one tenant may access another tenant's data or interfere with their applications [1].Yet, the cloud providers are the one responsible for not allowing a tenant to break into another tenant's data and applications [4].

Side-channel attacks based on information obtained from bandwidth monitoring or other techniques pose significant risks in cloud computing environment [1]. Side-channel attacks occur due to covert channels with flawed access control policies that allow unauthorized access [5]. Another security risk associated with multitenancy is interference between tenants because of tenants' workloads [1]. For example an overload created by one tenant may negatively affect the performance of another tenant [6]. A third risk of multitenancy is resources being assigned to customers with unknown identities and intentions [1]; the virtualization layer if compromised leads directly to the compromise of any of the virtual machines on the physical host [6].This could lead to the inability to monitor the activities of the virtual machine or change its state by a malicious user [1].Moreover the virtualization layers complexity leads to vulnerabilities that could allow a virtual machine user to gain control of the virtualization layer and all other virtual machines running on the same physical host [7].

A fourth security risk is uncoordinated change controls and misconfigurations [1]; changes to the underlying infrastructure without being well coordinated and tested may lead to a security breach allowing one tenant to gain access to another tenants data or resources [1]. A fifth security risk can result from comingled tenant data [1];

providers may store data of multiple tenants in the same database table-spaces and /or backup tapes and a delete request may become a challenge as portions of data may not be properly deleted [1].

Countermeasures:-

Ref. [1] acknowledges that in IT security analytics it is rare that there is a countermeasure to mitigate and manage every risk. Therefore most security specialists advocate a holistic approach to security policy management and technology implementations that support security policies [1]. Consequently the risks can be broken down into three categories: Governance, Control and Auditing risks, Configuration, Design and Change Management risks and Logical Security, Access Control and Encryption risks [1]. Governance, Control and Auditing risks are risks related to the services provided by the CSP and the roles of the tenants in governing those risks. These risks are applicable to IaaS, PaaS or SaaS. Configuration, Design and Change Management risks are risks that are due to the multitenant architecture (i.e. virtualization and shared resources). These risks are most evident in IaaS and PaaS cloud environments. Logical Security, Access Control and Encryption risks are those dealing with security systems related to access to applications , data or business function within a multitenancy cloud service offering. These risks are more applicable to PaaS and SaaS cloud environments.

Governance, Control and Auditing:-

Separation of Duties:-

Within the IT context, Separation of Duties (SoD) refers to segregating a single task, function or component to multiple areas of responsibilities and assigning those areas to different roles or individuals [1]. The goal of SoD is to reduce or eliminate conflicts of interest, and guarantee that no individual is given the opportunities to have powers or capabilities other than his or her role [1].

The surrounding risks of SoD in a cloud computing context center around role definition and clarification [1]. Due to the rapid evolution of cloud technologies and their rapid adoption, there has been little time or opportunity for SoD to develop and stabilize into standard roles [1]. For example the CSP's role of administration access and security policy creation and enforcement the CSP needs to secure the service he offers while not exceeding the customer authorities in a resource or domain [8]. This extends to the Multitenan Architecture (MTA) environments where multiple tenants may not have the same reliance on the CSP's role in security management or the same capability to security control [9].

SoD is included in many commercial security products such as Enterprise Single Sign-On (ESSO) and Identity and Access Management (IAM) [1]. However the current security products do not support adequate SoD separation for cloud environments since they are designed generally for single security domain where the owner and user of IT facilities are one and the same [8].Li, Zhou et al [8] proposed the Multi-Tenancy Trusted Computing Environment Model (MTCEM) that implements the two basic concepts of Trusted Computing Platform (TCP) in multitenancy cloud context.

TCP is a set of standards, principles and technologies when implemented enable the data owner or steward to trust and hold accountable the infrastructure that runs the applications that create, store and manipulate their data [1]. TCP has two basic assertions: Transitive Trust and Platform Attestation [1].Transitive Trust is where a computing platform (i.e. the cloud) can only boot or initialize from a Core Root of Trust Measurement (CRTM) [1]. The initialization follows a pathway of trust through a bootstrap process where one level of initialization can implicitly trust that the previous level is passing a secure microkernel [1]. Platform attestation is a mechanism by which a computing platform (i.e. the cloud) proves to a system with which it interacts or a third party that it is trustworthy or be deemed trustworthy [1]. Attestation prototypes for the cloud have been built [8] that determine trustworthiness based on behavior history or defined properties of the cloud. The advantage of implementing MTCEM in MTA environment is that it allows a given Host or Guest to simultaneously belong to multiple security domains and serve multiple security tasks through different security policies [1]. TCP can also be a countermeasure for configuration, design and change management risks [1].

Auditing and Client Controls:-

IT auditing frameworks rely on logging and data capture to provide positive evidence of adequate IT controls and governance [1]. In conventional IT systems, this means auditing all administrative access to systems [1]. In cloud computing, it may mean auditing all tenants of an MTA cloud service that could not be required in tenant policies but mandated by the CSP [1]. This countermeasure helps to ensure that no intruder can access an infection vector

through a lax tenant security posture and compromise another tenant's services [1]. Therefore audit and access controls should be part of the MTA usage terms and contract [1]. Moreover each client must be fully aware of the responsibilities of the CSP and themselves in security administration and governance [2].

Configuration, Design and Change Management:-

Securing Shared Services:-

One of the underlying assumptions of cloud computing is the concept of shared services [1]. Yet shared services mean differently depending on which kind of cloud in question [1]. For IaaS clouds each client environment is partitioned and controlled by a single instance of hypervisor and virtualization software [1]. Several recent exploits have been used to allow a VMWare guest to escape to the host and compromise the hypervisor through a rootkit based approach [10]. The only countermeasure to these exploits is careful watch on the part of the CSP in maintaining the hypervisor and implementing both network-based and host-based intrusion detection and prevention systems [1]. However the state of the art in cloud-based IDS and IDP systems is rudimentary [1].

For SaaS clouds, each application instance on behalf of an MTA tenant shares a single instance of object code [1]. When mistakes are made or object code is corrupted millions of clients may access private data of other clients [4]. A countermeasure to these risks is to develop SaaS solutions using Aspect-Oriented Programming (AOP) [1]. AOP abstracts the security implementation protecting the data in the service from the service functionality [2]. This allows each client to implement different security measures and use the same object code [1].

For PaaS clouds, each tenant may have the various layers of their hosted solution across multiple physical servers [1]. The risk with PaaS in an MTA environment is the lack of configuration information (i.e. which part of a tenant's platform runs where?) [1]. The risk can be countered and partially mitigated through the use of a dependency map for each tenant [1]. The CSP needs to have a dynamically managed and updated mapping of the underlying technical infrastructure to each client's virtualized servers and run-time hosted instances [1]. This helps in problem determination and communication management with the client [1].

The overall multitenancy risk for IaaS, PaaS and to a lesser extent SaaS tenants can be reduced and in some cases eliminated through the use of "Virtual Private Cloud" [1]. However this has the effect of reducing or eliminating the business case for cloud computing [1].

Network Configuration:-

Network design and implementation in a cloud environment is relatively stable and the network configuration leverages the expertise and best practices of conventional datacenter design [1]. However poor network design within a CSP network put MTA tenants at a risk of compromise from another tenant's internal network as there may not be adequate attacks controls causing the so-called "shrew" attack [1]. In addition, the countermeasures rely on very knowledgeable network administrators to implement at the core switching and routing points of the CSP's network [1].

One consequence of MTA is the network access required by administrators and users of cloud-based applications originating from outside the CSP's network address space [1]; each tenant requires a discrete set of IP addresses in order to access their applications and administration consoles. The CSP is responsible for managing a client limited pool of IPv4 addresses and subnets [1] .However, CSPs either through necessity or neglect fail to manage their addresses pools [1]. In MTA environment where tenants are provisioned and de-provisioned it may be possible for the de-provisioned tenant's services to be available under the old IP address and port number for a short period of time [10].The countermeasure to this risk is to ensure that the server, handled by one group of the CSP, and IP address, handled by another group, provisioning and de-provisioning to be harmonized [1].

Availability in an MTA Environment:-

In the MTA environment there is an availability risk to some tenants based on the activities of other tenants on the same infrastructure and platforms [1]. The risk to availability is through the lack of workload optimization particularly for batch processing and within SaaS CSPs [1]. Batch-based computing involves single-threaded applications, asynchronous processing, and serial execution of job steps and high rates of I/O to large sequentially organized datasets [6]. This poses the risk of one tenant to grab more than their allocated share of resources for an extended period of time during high batch activity [1].Momm and Theilmann [6] propose a workload planning approach based on measuring the characteristics of the batch execution environment and analyzing it to form a

performance baseline, find the minimum number of application instances to serve multiple tenants while still guaranteeing SLA performance levels, create a "master job schedule" that service all clients and minimize the penalties for time constraints and check progress against the baseline and suggest further refinement in the plan.

Logical Security, Access Control and Encryption:-

Encryption Protocols:-

Most CSPs suffer from lack of "security by diversity" [1]; in MTAs data of several or all MTA clients is encrypted with the same encryption algorithm. Therefore the risk exists in that if the encryption protocol is compromised or the cipher suite is "broken" for one tenant enables or eases compromise of others [2].Two countermeasures are proposed by Wood and Anderson, Predicate Encryption and Homomorphic Encryption [2].In Predicate Encryption each master key owner has fine-grained control over who gets access to encrypted data, so individuals may only have access to their particular segments [1]. Therefore a compromise of a segment does not mean other segments are in jeopardy [1]. In Homomorphic Encryption cipher text can be processed without the need to decrypt data before processing [1]. This eliminates or reduces the opportunity for a malicious party to intercept data during processing [1].

Logical Authentication and Access Controls:-

The difficulty in access management is of a) controlling different data and application resources; b) providing fine-grained access to the resources; and c) designing an access control mechanism employing a large number of authorization rules across conflicting policy domains for large number of users [5]. These are the environments of multitenant cloud offerings [1].

The most common countermeasure for this type of environment is Role-Based Access Control (RBAC) [4]. RBAC involves two phases in assigning a privilege to a user: phase one a user is assigned to one or a small number of roles, phase two privileges are assigned to roles not users [1].However multitenant cloud offering encounters this complexity at an even higher level as multiple conflicting role-based access mechanisms or hierarchies apply to the same user or the same resource [1].To reconcile multiple RBAC hierarchies, Tsai and Shao [4] propose an "ontology-based" access control mechanism where role hierarchies are "ontologies" with distilled role properties which are assigned to standard templates[1]. In a security domain the templates determine the similarities and differences between different roles at run-time [1]. A resultant set of permissions, inherited from multiple roles can be applied to an end user at time of access [1]. This countermeasure in an MTA environment can apply permissions to a role instead of a tenant or to a role in multiple sessions with multiple tenants in an MTA [1]. Consequently this is important where an agent of a CSP must execute a security function or audit process across multiple tenants in the MTA [1].

Identity and Access Management:-

MTAs have a greater need for the services of an Integrated Identity and Access Management solution (IAM) [1]. IAM enables continuous and firm authorization for customers in terms of their identity and privileges across multiple clouds [1]. However there are significant challenges to apply IAM standards and specifications to cloud computing [1]. Mather et al [9] support the approach of "federating" IAM solutions across multiple clouds and multiple tenants in an MTA. Users with their global credentials are recognized by services in the cloud [1]. CSP's delegate authentication to a third party through Identity Management-as-a-Service providers and federate access management by security policy composition across multiple CSP's [1].

Conclusion:-

Multitenancy is a double edge sword in the world of cloud computing [1]. The economies of scale by a multitenant system allow the service provider to pass savings onto the user thus reducing their overall operating costs and their total cost of ownership [1]. However multitenancy introduces its own unique set of associated security risks to the cloud computing environment. These risks and their countermeasures fall into three broad categories: Governance, Control and Auditing, Configuration, Design, and Change Management, Logical Security, Access Control and Encryption [1]. Yet the user must be aware of these risks and must take appropriate countermeasures to mitigate them and this is what the paper wants to illustrate.

References:-

1. W.J. Brown,V. Anderson,Q. Tan. "Multitenancy – Security Risks and Countermeasures".2012 15th International Conference on Network-Based Information Systems. Melbourne, VIC, Australia, 26-28 Sept. 2012.
2. K. Wood, M. Anderson, "Understanding the complexity surrounding multitenancy in cloud computing", 2011 Eighth IEEE International Conference on e-Business Engineering, Vol. 1, no. , 119-124, 2011.
3. Z. Feng, B. Bai, et al, "Shrew Attack in Cloud Data Center Networks", 2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks, Vol. 11, no. , 441-445, 2011.
4. W. Tsai, Q. Shao, "Role-Based Access-Control Using Reference Ontology in Clouds", 2011 Tenth International Symposium on Autonomous Decentralized Systems, Vol. 11, no. ,121-128, 2011.
5. A. Abdulrahman, M. Sarfraz, et al, "A Distributed Access Control Architecture for Cloud Computing," IEEE SOF T Ware, Vol. 12, no., 36-44, 2012.
6. C. Momm, W. Theilmann, "A Combined Workload Planning Approach for Multi-Tenant Business Applications", 2011 35th IEEE Annual Computer Software and Applications Conference Workshops, Vol. 11, no. 255-260, 2011.
7. B. Hay, K. Nance, et al, "Are Your Papers in Order? Developing and Enforcing Multi-Tenancy and Migration Policies in the Cloud", 2012 45th Hawaii International Conference on System Sciences, Vol. 12, no. , 5473-5479, 2012.
8. X. Li, L. Zhou, et al, "A TRUSTED COMPUTING ENVIROMENT MODEL IN CLOUD ARCHITECTURE", Proceedings of the Ninth International Conference on Machine Learning and Cybernetics, Qingdao, Vol. 9, no. , 2843-2848, 2010.
9. Tim Mather, SubraKumaraswamy, ShahedLatif, Cloud Security and Privacy, O'Reilly Press, 2009.
10. John Rhoton, Cloud Computing Explained Second Edition, Recursive Publishing, 2011.
11. S. Subashini, and V. Kavitha, " A Survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications (2011).
12. DimitriosZissis, and DimitriosLekkas, "Addressing cloud computing security issues," Future Generation Computer Systems (2011).
13. Md. TanzimKhorshed, A.B.M. Shawkat Ali, and Saleh A. Wasimi, "A Survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing," Future Generation Computer Systems (2012).
14. Wayne A. Jansen, " Cloud hooks: security and privacy issues in cloud computing," Proceedings of the 44th Hawaii International Conference on System Sciences (2011).
15. David Teneyuca, "Internet cloud security: the illusion of inclusion," SciVerseScienceDirect (2011).
16. AfkhamAzeez, SrinathPerera, DimuthuGamage, Ruwan Linton, PrabathSiriwardana, DimuthuLeelaratne, SanjivaWeerawarana and Paul Fremantle, "Multi-Tenant SOA middleware for cloud computing," IEEE 2rd International Conference on Cloud Computing (2010).
17. Verizon RISK Team, "Data breach investigations report (DBIR)," (2012).
18. Prasad Saripalli, and Ben Walters, "QUIRC: a quantitave impact and risk assessment framework for cloud security," IEEE 2nd International Conference on Cloud Computing (2010).
19. F. Gens, "IT cloud services user survey, pt.2: top benefits & challenges," Oct. 2008. (http://blogs.idc.com/ie/?p=210).
20. Hagai Bar-El, "Introduction to side channel attacks,".
21. S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," 2010 IEEE Second International Conference on Cloud Computing Technology and Science, vol. 8, no. 6, pp. 692-702, Nov. 2010.
22. Ruoyu Wu, Gail-JoonAhn, Hongxin Hu, and MukeshSinghal, "Information flow control in cloud computing," (9-12 Oct. 2010).
23. G. I. Davida, D. L. Wells, and J. B. Kam, "Security and Privacy," IEEE Concurrency, vol. 8, no. 2, pp. 24-21, 2000.
24. Augusto Ciuffoletti, "Monitoring a virtual network infrastructure," (October 2010).
25. Z. Chen and J. Yoon, "IT Auditing to Assure a Secure Cloud Computing," 2010 6th World Congress on Services, pp. 252-259, Jul. 2010.
26. S. Bleikertz, M. Schunter, C. W. Probst, and K. Eriksson, "Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds Categories and Subject Descriptors," pp. 92-102.
27. R. Chakraborty, S. Ramireddy, T. S. Raghu, and H.R. Rao, "Assurance Practices of Cloud Computing," pp. 29-27, 2010.
28. H. Aljahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, J. Xu."Multi-Tenancy in Cloud Computing,".In proceedings of the 8th IEEE International Symposium on Service-Oriented System Engineering, Oxford, UK. 7-11 April 2014.