Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing

Yasir Ahmed Hamza[1,] Marwan Dahar Omar[1]
[1]Department of Computer Science, Computer and IT Faculty, Nawroz University, Duhok, Iraq

ABSTRACT:
Cloud computing is an emerging and promising computing model that provides on-demand computing services which eliminates the need of bearing operational costs associated with deploying servers and software applications. As with any technology, cloud computing presents its adopters with security and privacy concerns that arise from exposing sensitive business information to unauthorized access. This paper will explore and investigate the scope and magnitude of one of the top cloud computing security threats "abuse and nefarious use of cloud computing" and present some of the attacks specific to this top threat as it represents a major barrier for decision makers to adopting cloud computing model. Also, this paper aims to serve as an introductory research effort to warrant more extensive research into this top threat and help researchers to make recommendations to business organizations as to whether or not their data are vulnerable to such threat when deciding to join the cloud.

KEYWORDS: Abuse and nefarious use of cloud computing, Cloud computing security threats, Private cloud, Public cloud, Virtualization.

I. INTRODUCTION

Cloud computing is one of the revolutionary technologies that is expected to dominate and reshape the information technology industry in the near future. This emerging computing technology provides highly scalable computing resources (e.g. information, applications, and transactions) in a way that is accessible, flexible, on-demand, and at a low cost [1]; it provides unique opportunities for organizations to run business with efficacy and efficiency by allowing businesses to run their applications on a shared data center thus eliminating the need for servers, storage, processing power, upgrades, and technical teams. Furthermore; in cloud computing model, business organizations do not need to purchase any software products or services to run business because they can simply subscribe to the applications in the cloud; those applications normally are scalable and reliable and ultimately allow business leaders to focus on their core business functions to enhance performance and increase profitability. Many organizations have become interested in the cloud computing concept due to many compelling benefits presented by this emerging computing paradigm [2].

Cloud computing vendors are offering scalable services and applications via centralized data centers utilizing thousands of server computers which provide easy access to computing resources anytime and anywhere [2]; the capability of cloud computing to quickly scale and provide access to computing services and resources anytime and anywhere, allowing organizations to quickly respond to changing business needs without the expenditures of time, space, money, personnel, and other resources needed for traditional infrastructures for example, New York newspaper organization were able to convert 11 million scanned and archived hard copies into portable document format (PDF) files in 24 hours by renting 100 servers from Amazon's cloud services at a cost to the organization was approximately $250. Alternative methods for the conversion would have required cost and taken weeks or even months to complete [3].while cloud computing offers enormous potential for reducing costs and increasing an organization's ability to quickly scale computing resources to respond to changing needs, there are risks associated with cloud computing.

Specifically, cloud computing may mean that an organization relinquishes control, resulting in exposure to breaches in confidentiality, losses in data integrity and availability. However; as with any technology, cloud computing has its own disadvantage such as releasing control of maintaining confidentiality, integrity, and availability of sensitive business data; In general, most cloud computing consumers want to be assured that cloud providers have effective security policies and controls in place to comply with data protection standards and meet regulatory compliance requirements prior to making a decision to migrate their data or applications to the cloud.

II. CLOUD DEPLOYMENT MODELS

According to [4] there are four cloud deployment models regardless of the service model adopted (Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS)):

2.1. Public Cloud. This is also called external cloud sometimes and it basically involves an organization that sells readily available cloud services to the general public. Business organizations with sensitive corporate data are reluctant to adopt this model because it increases the threat of exposing confidential data to unauthorized access by third parties and potential cyber criminals. The advantage of using the public cloud is that an organization itself does not have to manage the cloud computing infrastructure nor maintain operational activities. The disadvantage of utilizing the services from a public cloud provider is that it is entirely dependent upon another business entity that is offering resources through public cloud [5].

2.2. Private Cloud. Also referred to as internal cloud which means that cloud infrastructure and services are explicitly made available for a single organization. This deployment model can be located on premise or off site as it can also be managed by the organization itself or can be outsourced to a third party. Privately-hosted cloud services tend to be more costly but safer than other deployment models because organizations can retain control of their sensitive data and applications and implement their own security measures. The advantage for maintaining the private cloud is that an organization can retain full control of all the computing resources (e.g. applications, data, and systems) related to a cloud infrastructure. The disadvantage of such a deployment model is that an organization has to invest significantly in computing and storage resources and bear the cost of maintaining all software and computing platforms.

2.3. Community Cloud. Organizations who share the same concerns and goals (e.g. security controls, privacy concerns, organizational mission, and regulatory compliance requirements) can join this deployment model to share the cloud infrastructure which could exist on-premise or off-premise as it could be managed by a third party as well.

2.4. Hybrid Cloud. This deployment model can span two or more other deployment models such as private, public, or community. In this model, data and applications are still standardized and enabled by a proprietary technology. The benefit of this model is that it offers a blend of cost effectiveness and scalability without exposing sensitive business data to external threats. This is possible because the hybrid model allows organizations to maintain their mission-critical applications in a private cloud (which provides security and control of in-house computing resource) and migrates their non-critical applications and platforms to the public cloud. Data availability, control, and performance are some of the disadvantages that can arise from adopting the hybrid cloud model. Figure (1) below is a visual model defined by the National Institute of Standards and Technology (NIST) illustrating the three cloud service models and the four deployment models:

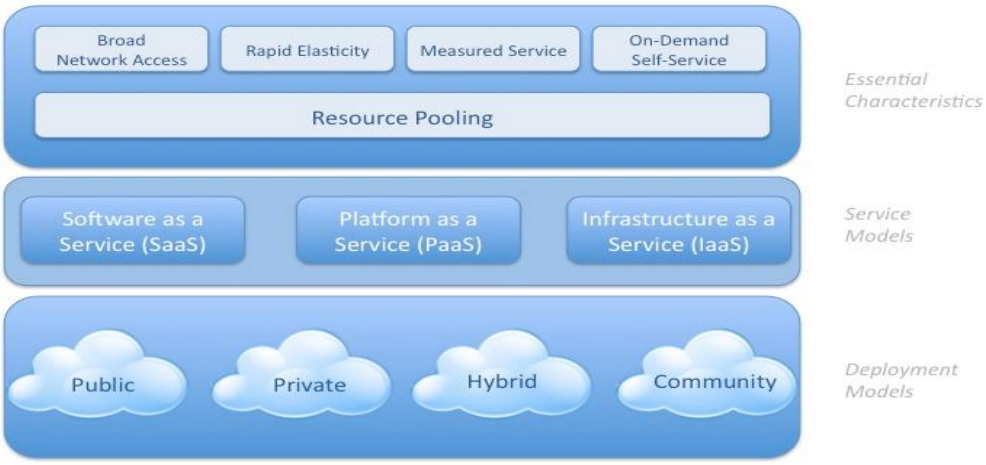

Figure 1. NIST visual model of cloud computing definition

III. CLOUD COMPUTING SERVICE MODELS

[4] States that the cloud computing technology comprises three fundamental classifications which are commonly referred to as "SPI Model" where "SPI" refers to "Software", "Platform", "Infrastructure" respectively. Below is a definition of each service model:

3.1. SaaS. In this model, the cloud provider has control of the underlying cloud infrastructure such as servers, operating system, processing, storage, and even the applications capabilities. Cloud provider has the responsibility of managing application capabilities while allowing cloud customers to use and access the

application capabilities from their own devices via a thin client interface such as a web browser. Cloud subscribers who adopt this service model will generally have the least control over cloud applications while they have very limited freedom in changing user specific configuration settings [4]; a good example for this type of service model is the Gmail application which is a web-based e-mail provided by Google as a SaaS.

3.2. PaaS. This computing model is similar to the previous one in that cloud consumers do not have any control over the underlying cloud infrastructure such as network, servers, storage, processing, and applications. This model allows cloud customers to deploy their own application (created by customer) onto the cloud infrastructure that enables them to control and mange those applications. Furthermore; cloud clients do not need to purchase or manage the cloud computing infrastructure while they are provided with capabilities to develop and use software applications. For example, Google has a PaaS that allows clients to run their web applications on the Google App Engine using an internet browser such as Internet Explorer [6].

3.3. IaaS. This is the foundation of cloud services because it provides capabilities for cloud consumers to deploy fundamental computing resources such as operating systems, applications, servers, bandwidth, storage, and processing. As with the other two models, this model does not demand cloud consumers to manage or control the underlying cloud infrastructure. For example, Amazon EC2 allows individuals and businesses to run their own applications on machines that can be rented with preconfigured and selected operating system [6].

IV. CLOUD COMPUTING THREATS

Security researchers as well as industry experts strongly predict that cloud computing will be the "next big thing" due to its compelling cost saving advantage and on-demand web based nature which allows business organizations to focus on their core business competencies; however, these computing possibilities do not come risk free because they expose organization's sensitive data to cyber threats and open the door for new attack vectors. In fact; migrating to the cloud magnifies risks to confidential data because business information resources are exposed to third parties (cloud providers) who themselves may pose a risk from their internal employees and thereby increasing the possibility of insider threat.

Moreover; the real threat arises from the fact that service provider has the privilege of accessing sensitive business data and may be allured to misuse or abuse this privilege or even access data in an unauthorized manner. Therefore cloud consumers have to take the risk of entrusting service providers with their sensitive information assets and hope that the cloud service providers have security measures in place to restrict employee access to information thereby reduce risk of insider threat to a minimum. One of the unique security risks associated with the use of cloud services is that of virtualization; cloud computing utilizes virtual machines to run different multiple instances on the same physical machine [7]. Those instances have to be isolated to prevent malicious hackers from eaves dropping or taking control of host machine. Although cloud providers such as Amazon have VM monitors in place to detect such malicious or illegal activity; however, this security measure cannot fully address the security requirements necessary to block or prevent compromised VMs from extracting and leaking information to cyber criminals.

- Top Cloud Computing Security Threat: Abuse and Nefarious Use of Cloud Computing: According to[8], abuse and nefarious use of cloud computing is considered as the top security threat to cloud computing because cloud providers do not enforce any strong registration process where any person with a valid credit card can register to receive cloud services; this huge flaw in the registration system coupled with weak fraud detection capabilities lends cloud computing models such as IaaS and PaaS to malicious attacks by criminals who can leverage those technologies and target cloud providers.

  To make matters worse, and according to [8], some cloud service providers offer readily available free limited trial period of cloud services which presents a perfect opportune time for cyber criminals to join the cloud and possibly misuse and abuse their access privilege to cloud services. Cloud computing model by its very nature involves multiple data centers across possibly multiple locations and each data center is dedicated to many customers and their data needs; this in turn makes investigating and detecting unauthorized or inappropriate activity significantly difficult in a cloud environment. Attackers can exploit this threat and launch an attack called "cloud computing malware injection attack" by creating their own implementation module (e.g. PaaS or SaaS) within the cloud environment and trick the cloud system to treat that malicious instance as a valid instance for the particular service module; once adversary is capable of doing this trick, the cloud system will automatically redirect valid user requests to the service module run by attackers [9]. As a case in point, hackers can host malicious data and possibly convince users of Amazon Elastic Cloud Compute (EC2) to run images on a virtual machine by giving the image a name that sounds official such as "Fedora-core" [10].

  In fact; [11] were able to use the Amazon EC2 service as a case study and demonstrated information leak by first mapping internal cloud infrastructure, identify the possible location of a target virtual machine, and then continue to create instances of Virtual Machines (VM) until one is created adjacent to the target VM; once the target VM has been located and identified, hackers can compromise that VM and use it to leak

information. They showed that investing a few dollars to buy an instance of a VM with Amazon EC2 service can have a % 40 chance of successfully placing a malicious VM on the same physical machine as the target customer. Moreover; cyber hackers can masquerade themselves as legitimate cloud users and abuse this feature to launch spam campaigns, run botnets, and brute force attacks. Figure (2) below shows different components of security requirements within a cloud platform which makes security a more challenging task for cloud providers given that there are four deployment methods and three cloud computing models.

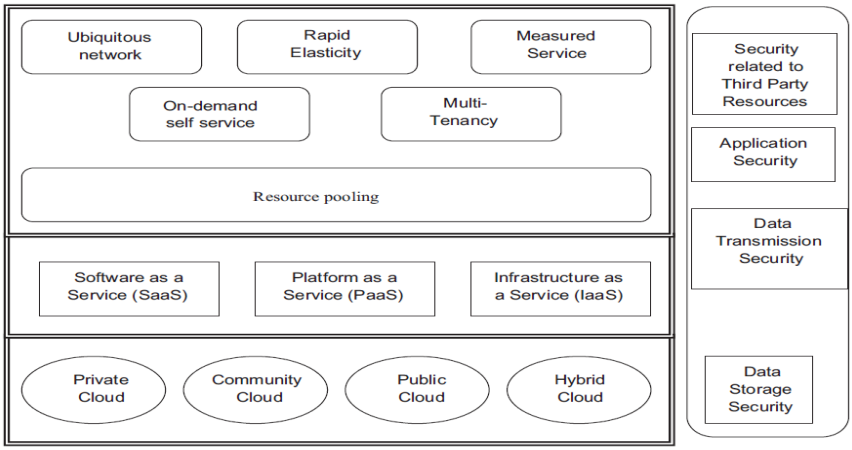

Figure 2. Complexity of security in a cloud environment [7]

- Applicability of "abuse and nefarious use of cloud computing" to "PaaS":

The threat of abusing cloud services is somewhat unique in that it involves the risk of insider threat as well as the risk posed by cyber criminals to join the cloud and misuse its services; cloud providers can be a big risk on organizational information assets if they do not enforce stringent security procedures to regulate employee access to sensitive business data. With the increased adoption of cloud services, cloud provider employees are prone to be targeted by malicious hackers given the fact that "PaaS" model involves storing and processing sensitive organizational resources such as intellectual property, trade secrets, and customer confidential information on the provider's servers; therefore cloud providers have to practice due diligence to minimize the risk of insider threat and detect unauthorized access from internal employees [12].

The other security risks stems from the fact that " PaaS" is readily available for the public which provides an opportunity for hackers to try the service with the intent of circumventing provider's security controls and ultimately compromise sensitive business data illegally; arguably, "PaaS" can be used as a "Hacking as a Service" because cloud computing is increasingly becoming an ecosystem that involves numerous services, interactions, interdependencies, and its many deployment models with different structures (SaaS, PaaS, and IaaS).

PaaS is particularly susceptible to nefarious cyber threats because it allows "legitimate" cloud customers to deploy their own- created applications on a platform that is supported by the cloud provider. For example, many cloud vendors (e.g. Google App Engine& Sun Microsystems) facilitate the deployment of applications and APIs that are written in Java, Python, or .Net on their computing platform [13].Furthermore; Cloud providers allow their customers to deploy and control their applications and configure the hosting environment, this feature, in turn, could be exploited by attackers to inject malicious code into the hosting environment and eventually infect the underlying cloud infrastructure. A representative example of this threat is the Amazon EC2 cloud based service that was used by cyber criminals whom ran a botnet called "Zeus crimeware" for command and control purposes [14]

V. ATTACKS RELATING TO "ABUSE AND NEFARIOUS USE OF CLOUD COMPUTING" THREAT

5.1. Host Hopping Attacks. This attack exploits one of the most defining characteristics of cloud computing: resource sharing; this attack can be launched by hackers if cloud provider does not enforce strict mechanism to isolate shared resources such as memory, storage, and reputation of different customers or hosts [15]. Failing to separate tenants (customers) can certainly facilitate this type of attack and thereby allow malicious hackers to hop on other hosts to compromise other customers' data and gain illegal access to it. This attack can be particularly dangerous for public clouds and the PaaS model where multiple clients share the same physical machine. Attackers can cause severe damage that could range from compromising sensitive customer data to interrupting service for cloud providers and distorting their image and reputation.

5.2. Malicious Insider and Abuse of Privileges. The shared and multi-tenancy nature of cloud computing creates a fertile ground for insider threat and promotes risk of "privilege abuse" to confidential customer

information. Hosting sensitive information from multiple clients on the same physical machine certainly entices users with high privilege roles such as system administrators and information security managers to abuse their privileged access to clients' sensitive data and the possibility of leaking or selling that information to competitors or other parties of interest. The possibility, and hence impact, of this risk can be further amplified if cloud provider does not enforce strict definition of roles and responsibilities or does not apply the "need to know" principle [15]. Also, it's worth noting that with the increased adoption of cloud computing services; cloud computing employees are becoming a target of cyber criminals as an effort to gain unauthorized access to sensitive business data in the cloud. Unfortunately, most organizations that experience this type of insider attacks choose not to publicize the issue and "sweep it under the rug" due to reputation and customer trust concerns; not to mention that they may face legal and regulatory compliance issues.

5.3. Identity Theft Attacks. Malicious hackers can easily set up accounts with cloud providers to use cloud resources by simply paying for the usage without any restrictions or limits from cloud vendors on resource consumption or workloads. Attackers can exploit this advantage to use and compromise customer's critical information and sell it for a price. Furthermore; cyber criminals could also set up rogue clouds and entice individuals to host their sensitive data and provide cloud computing services such as e-mail applications. Once individuals entrust their confidential data with rogue cloud providers, their identity is at risk and can be compromised and thereby can lead to identity theft and financial fraud.

5.4. Service Engine Attacks. The service engine is a highly customized platform that sits above the physical layer and characterizes the underlying cloud architecture; this service engine is normally controlled by cloud provider to mange customer resources but it can be rented by potential customers who wish to use and adopt the IaaS model. hackers can abuse this feature by subscribing to the IaaS model and renting a virtual machine that would be hosted and controlled by the service engine; then they can use the VM to hack the service engine from the inside and use the service engine to their advantage where it may contain sensitive business information through other VMs from other cloud subscribers. In other words, hackers can escape the isolation feature that separates data belonging to different cloud customers and possibly breach and compromise their confidential data [15].

VI. CONCLUSION

The foregone discussion explored the security aspects of cloud computing; specifically shed light on one of the top cloud computing security threats "abuse and nefarious use of cloud computing". The research indicated that cyber criminals have already exploited and misused cloud computing due to weak registration procedures of obtaining cloud computing services and lack of effective security controls; also, hackers are able to abuse cloud services by obtaining unauthorized and illegal access to other customer's confidential data residing on the same cloud platform. As a result, scholars are encouraged to conduct more extensive research to reveal more information about the risks and impact of this threat on sensitive business data; additionally, cloud security providers need to implement and deploy more proactive security techniques to prevent unauthorized and illegal access to sensitive organizational information residing on the cloud.

REFERENCES

[1] Eludiora, S., Abiona, O., Oluwatope, A., Oluwaranti, A., Onime, C., & Kehinde, L. (2011). "A user identity management protocol for cloud computing paradigm". International Journal of Communications, Network and System Sciences, 4(3), 152-152-163

[2] Aslam, U., Ullah, I., & Ansari, S. (2010). "Open source private cloud computing". Interdisciplinary Journal of Contemporary Research in Business, 2(7), 399-399-407

[3] Mongan, K. (2011). "Cloud computing the storm is coming". Accountancy Ireland, 43(3), 58-58-60

[4] Cloud Security Alliance 2009. Security guidance for critical areas of focus in cloud computing. V2.1 retrieved on August, 24th, 2011 from http://www.cloudsecurityalliance.org.

[5] Baber, M. & Chauhan, M. (2011) "A Tale of Migration to Cloud Computing for Sharing Experiences and Observations". *Proceedings of the 2nd International Workshop on Software Engineering for Cloud Computing 2011,* Retrieved May, 20, 2012 from http://delivery.acm.org.ezproxy.apollolibrary.com

[6] Choo, K. (2010). "Cloud computing: Challenges and future directions" (cover story). Trends & Issues in Crime & Criminal Justice, (400), pp. 1-6.

[7] Subashini, S. and Kavitha, V. (2011), "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications. 34 (1), pp. 1-11.

[8] Cloud Security Alliance (2010). "Top Threats to Cloud Computing". Cloud Security Alliance. Retrieved on August, 25th 2011 from http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[9] Jensen.M, Schwenk.J, Gruschka.N, Iacono.L, "On Technical Security Issues in Cloud Computing," pp.109-116, 2009 IEEE International Conference on Cloud Computing, 2009.

[10] Checn, Paxson, and Katz, 2010, "What's new about cloud computing security". Technical Report No. UCB/EECS-2010-5 retrieved from http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.html.

[11] Ristenpart.T, Tromer. E, Shacham. H, and Savage.S "Hey, you, get off of my cloud": Exploring information leakage in third-party compute clouds. In CCS'09: *Proceedings of the 16th ACM conference on Computer and communications security*.

[12] Blumenthal, M. S. (2011). "Is security lost in the clouds?" (*). Communications & Strategies, 81(1), 69-86.
[13] Chakraborty, R., Ramireddy, S., Raghu, T. S., & Rao, H. R. (2010). "The information assurance practices of cloud computing vendors". IT Professional Magazine, 12(4), 29-29-37.
[14] Danchev D, (2009), "Zeus crimeware using Amazon's EC2 as command and control server", Retrieved on August 25th 2011 from **http://blogs.zdnet.com/security/?p=5110.**
[15] European Network and Information Security Agency (ENISA, 2009); Cloud Computing: Benefits, Risks, and Recommendations; retrieved on August 14, 2011 from http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.