ISSN: 2393-8528

IJICSE
Open Access

Contents lists available at www.ijicse.in

International Journal of Innovative Computer Science & Engineering

Volume 2 Issue 3; July-August-2015; Page No. 40-43

The Cloud Threatening Legal Storm Security Failing

Divya Hada

M.Tech CS, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India.

ARTICLE INFO

Received: 03 July 2015
Accepted 18 July 2015

Corresponding Author:

Divya Hada

Department of Computer Science and Engineering, Jayoti Vidyapeeth Women's University, Jaipur

Email: Divyahada123@gmail.com

Key words: Privacy and Security, Cloud Computing, Security Threats, Security Costs.

ABSTRACT

Cloud computing is a double-edged sword from the privacy and security standpoints. Despite its potential to provide a low cost security, organizations may increase risks by storing sensitive data in the cloud. In this thesis, we analyze how the cloud's characteristics such as newness, nature of the architecture, and attractiveness and vulnerability as a cybercrime target are tightly linked to privacy and security. We also investigate how the track Security Threats to affects privacy and security issues in the cloud. Cloud computing poses privacy concerns because the service provider can access the data that is on the cloud at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies which users have to agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access. According to the Cloud Security Alliance, the top three threats in the cloud are "Insecure Interfaces and API's", "Data Loss & Leakage", and "Hardware Failure" which accounted for 29%, 25% and 10% of all cloud security outages respectively together these form shared technology vulnerabilities.

INTRODUCTION

1.1 Overview: - Cloud computing allows application software to be operated using internet-enabled devices. Clouds can be classified as public, private, and hybrid. Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications. The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization, service-oriented architecture, and autonomic and utility computing have led to a growth in cloud computing. Companies can scale up as computing needs increase and then scale down again as demands decrease.

1.2 Security and Privacy:- In a cloud provider platform being shared by different users there may be a possibility that information belonging to different customers resides on same data server. Therefore Information leakage may arise by mistake when information for one customer is given to other. Additionally, Eugene Schultz, chief technology officer at Imagined Security, said that hackers are spending substantial time and effort looking for ways to penetrate the cloud. "There are some real Achilles' heels in the cloud infrastructure that are making big holes for the bad guys to get into". Because data from

hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack — a process he called "hyper jacking". Physical control of the computer equipment (private cloud) is more secure than having the equipment off site and under someone else's control (public cloud). This delivers great incentive to public cloud computing service providers to prioritize building and maintaining strong management of secure services. Some small businesses that don't have expertise in IT security could find that it's more secure for them to use a public cloud. There is the risk that end users don't understand the issues involved when signing on to a cloud service (persons sometimes don't read the many pages of the terms of service agreement, and just click "Accept" without reading). This is important now that cloud computing is becoming popular and required for some services to work, for example for an intelligent personal assistant (Apple's Siri or Google Now).Fundamentally private cloud is seen as more secure with higher levels of control for the owner; however public cloud is seen to be more flexible and requires less time and money investment from the user.

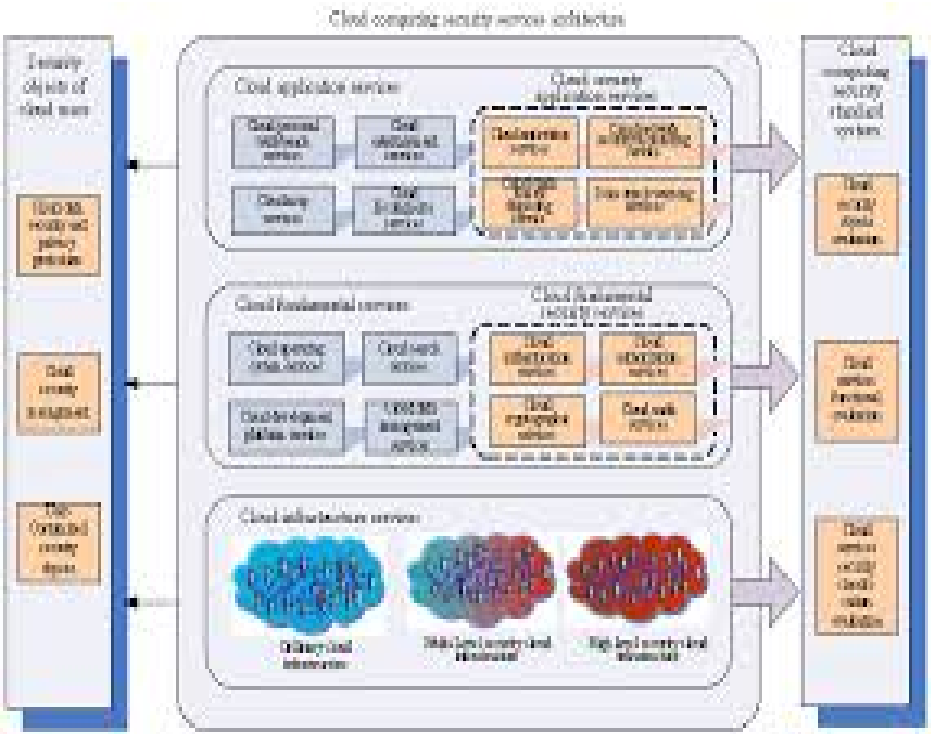

Diagram 1.1 Cloud Computing Security Issues

1.3 Nature of the Architecture

Virtual and dynamic

The virtual and dynamic nature of the cloud computing architecture deserves mention. For one thing, the shared and dynamic resources of the cloud such as CPU and networking reduce control for the user and tend to pose new security issues not faced by on-premise computing (Brynjolfsson et al. 2010). A related point is that these characteristics of the cloud allow data and information to distribute widely across many jurisdictions. The locations where data are stored may vary in laws regarding security, privacy, data theft, and protection of intellectual property (McCafferty 2010).

Virtualization is the primary security mechanism in the cloud. Nonetheless, some resources are not virtualized. Virtual systems, despite their insulation from the customer, run on physical systems (Sturdevant 2010). Moreover, virtualization environments are not necessarily bug-free (Armbrust et al. 2010).

Sophistication and complexity

The cloud's security related problems can also be linked to its sophisticated and complex architecture. In April 2010, U.S. and Canada-based researchers published a report on a sophisticated cyber-espionage network, which they referred as Shadow network. The targets included the Indian Ministry of Defense, the United Nations, and the Office of the Dalai Lama. The report noted: "Clouds provide criminals and espionage networks with convenient cover, tiered defences, redundancy, cheap hosting and conveniently distributed command and control architectures" (IWMSF 2010).Another problem concerns the cloud's complexity. An important trend facilitated by the cloud is social media, which are arguably "corporate security nightmare" (BBW 2010). In the Shadow case noted above, the cyber-espionage network combined social networking and cloud platforms, including those of Google, Baidu, Yahoo!, Twitter, Blogspot and blog.com with traditional command and control servers (IWMSF 2010).

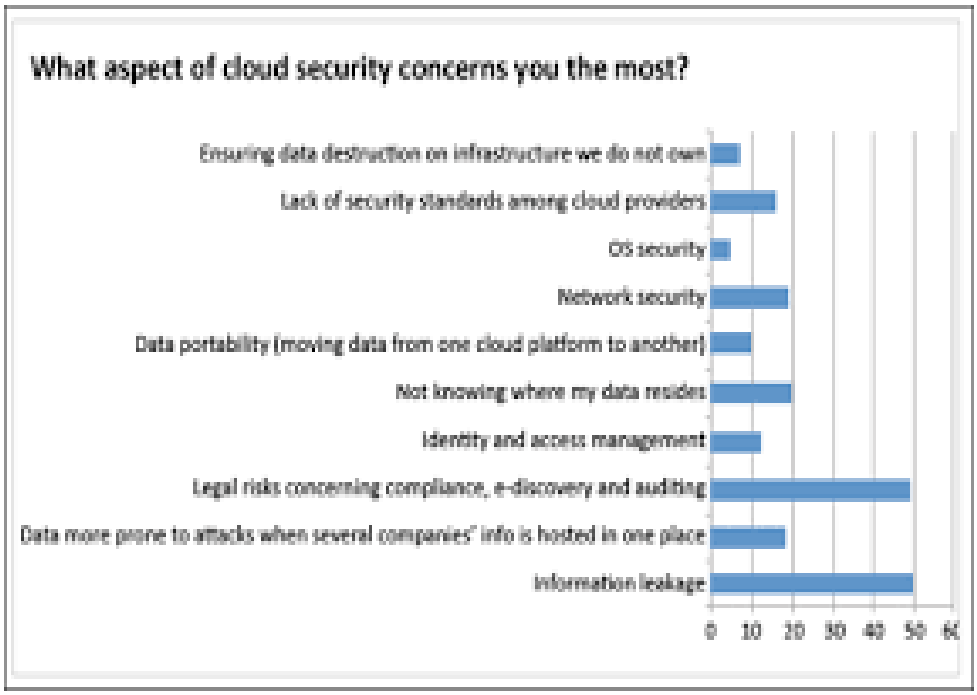

Diagram 1.2 Cloud Computing Security Concerns

1.4 Importance & Relevance of Study:

The Notorious 9 Cloud Threats as the cloud is not as safe as many people think, as a report from the Cloud Security Alliance explains. The CSA has outlined nine major categories of threats that face cloud technologies that organizations "must weigh ... as part of a rigorous risk assessment, to determine which security controls are necessary."The CSA's nine threats to cloud security, ranked in order of severity:

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure APIs
5. Denial of Service
6. Malicious Insiders
7. Abuse of Cloud Services
8. Insufficient Due Diligence
9. Shared Technology Issues

1.6 Future Research

Before concluding, we suggest several potentially fruitful avenues for future research. Cloud-related institutions are currently thin and dysfunctional. For instance, as noted above, privacy and security issues of data stored on the cloud currently fall into a legally gray area. Future research might examine how political, ethical, social and cultural factors are associated with security issues in cloud computing. Prior research conducted in other sectors (e.g., chemical industry) indicates that institutional evolution entails transitions among the three institutional pillars—regulative, normative, and cognitive. Building a regulative/law pillar system is the first stage of field formation. It is followed by a formation of normative institutions and then cognitive institutions (Hoffman 1999). A comparison of institutional evolution in the cloud industry with that in other economic sectors might be worthwhile target of study. Second, an empirical examination of core premises and propositions of the model presented and would be useful to advance the model's utility as a viable framework for studying the technological and institutional drivers of the cloud industry. Such a study would shed light on the relative importance of various components of the model in organizations' cloud adoption decision. Finally, future research might also explore antecedents of organizations' cloud computing decisions in terms of various technological dimensions identified in the prior literature. One avenue would be to test how the cloud performs in terms of major dimensions proposed by Rogers (1995) such as relative advantage, compatibility, complexity, observability and trialability.

1.7 Conclusion

Cloud security skeptics were given yet another reason to doubt the fortitude of online storage when the strange tale of Mat Honan emerged earlier this month. Through the clever use of social engineering, a hacker was able to life. Apparently, the hacker talked Amazon tech support into providing the last four digits of Honan's credit card number. This information was then used to fool Apple into thinking the hacker was Honan and issuing a temporary password for Honan's email account. The hacker used this information to ultimately delete Honan's Gmail account, permanently reset his AppleID and Twitter passwords, and remotely wipes his iPhone, iPad and MacBook.Apple and Amazon closed the specific security holes that enabled this attack after news of Honan's problem hit the headlines.

References

1. BBW (Bloomberg Business week). (2010). Salesforce.com Channels Facebook. August 30-September 5, 34-35.
2. Bottoms, A. E., &Wiles, P. (2002). Environmental criminology. Oxford Handbook of Criminology, 620–656.
3. Bradley, T. (2010). Build Your Own Private Azure Cloud with New Microsoft Appliance.
4. Bradner, S. (2010). Internet privacy conflicts. Network World, September 27, 2010, 27(18), 15-15.
5. Brenner, S. W. (2004). Toward a criminal law for cyberspace: A new model of law enforcement? Rutgers Computer and Technology Law Journal, 30 (2004), 1-9.
6. Brodkin, J. (2010). 5 problems with SaaS security. Network World, 27(18), 1-27. Brynjolfsson, E., Hofmann, P., & Jordan, J. (2010). Cloud Computing and Electricity:
7. Clarke, R. V. (1995). Situational crime prevention. In M. Tonry & D. P. Farrington (Eds.), Building a safer society. Strategic approaches to crime (pp. 91–150). University of Chicago Press.
8. Crosman, P. (2009). Securing The Clouds, Wall Street & Technology, December 1, pp.23.
9. Dean, T. J., & Meyer, G. D. (1996). Industry Environments and New Venture Formations in U.S. Manufacturing: a Conceptual and Empirical Analysis of Demand Determinations. Journal of Business Venturing, 11, 107-132.
10. Del Nibletto, P. (2010). The seven deadly sins of cloud computing, March 19, 2010.
11. Gilson, R .J. (2001). Globalizing corporate governance: convergence of form or function. The American Journal of Comparative Law, 49(2001), 329–58.