The Impact of Cloud Computing on Network Security and the Risk for Organization Behaviors

Alia J. Ouda
University of Information Technology and Communications (UOITC), Baghdad, Iraq.

Ali N. Yousif
University of Information Technology and Communications (UOITC), Baghdad, Iraq.

Ayat S. Hasan
Department of Computer Science, College of Education for Pure Sciences, University of Diyala, Diyala, Iraq.

Hassan M. Ibrahim
University of Information Technology and Communications (UOITC), Baghdad, Iraq.

Methaq A. Shyaa
Department of Information and Communication Systems, Iraqi Ministry of Interior, Baghdad, Iraq.

Received August 02, 2021; Accepted November 20, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V19I1/WEB19015

Abstract

Cloud computing is currently provided consumer or business IT support via social media or by using the internet. Cloud computing on the other hand, is increasing the level of the network security risk due to the services are basically presented by a third party. This results in hard to control the privacy and data security. In addition, to maintain the service availability and support data collections. Cloud computing clouts several technologies such as virtualization, SOA, and Web 2.0, it is also claimed their security risk matters. In this paper, the most serious and important risks and threats of cloud computing are discussed. The main vulnerability is identifying through a review of the published works on the cloud computing environment with possible solutions to overcome these threats and risks.

Keywords

Cloud Computing, Security Risk, Network Security, Virtualization.

Introduction

Cloud computing is received a rapidly increasing attention in both the industrial and academic fields. Cloud computing has been considered as one of the most technologies

that has better influence on the successful of the organizations among these years. The key benefits of the cloud computing is summarized in enabling on-demand network access, ubiquitous, convenient, and able for configuration of computing resources. These resources include networks, applications, servers, services, and applications, which can be widely managed and progressively released with a minimal number of service provider interfaces.

Providing a high level of security is considered the main task of cloud computing, net computing, quick process, and convenient data storage (Zhao, G., Liu, J., Tang, Y., Sun, W., Zhang, F., Ye, X., & Tang, N., 2009). The resources of computing are imagined as services that will be delivered through the internet, which cloud computing can be seen as a distribution architecture as well as a computational model. Moreover, cloud computing improves agility, availability, scalability, collaboration, an adaption of fluctuations based on demand, cost reduction, and speed up development work (Marinos, A., & Briscoe, G., 2009).

The cloud is consisted of a number of computing models and concepts such as Web 2.0, virtualization, and service orientated architecture (SOA). These models are relied on the Internet, which provides mutual business consumers' computer requirements by providing services online using standard web browsers. In the same time, the data and software are saved on existing remotely servers (Marinos, A., & Briscoe, G., 2009). In another word, the cloud can be represented as the mature of these concepts and technologies, which presents to a marketing term the maturity of the services provided. There are many considerable obstacles to adopt it, where these roadblocks are mostly focused on security and privacy concerns, compliance, and legal matters (Rosado, D. G., Gómez, R., Mellado, D., & Fernández-Medina, E., 2012), that is mostly because cloud computing is a novel term that may be defined as computing architecture. In that matter, a great adopts of how security level can be functional on network, application, data levels, and host (Rosado, D. G., Gómez, R., Mellado, D., & Fernández-Medina, E., 2012). While the application and data security may be done in a variety of ways in the cloud computing is another issue to be investigated.

Generally, security matters Concerns about a loss of control, reliance on the internet, etc. integration with internal security, and external data storage. Cloud has several features compared to the common technologies, it can be summarized as large scale, and the resources are completely virtualized and distributed by the cloud providers (Li, W., & Ping, L., 2009). In cloud computing, the security controls are similar to any IT environment security controls. However, since cloud computing structure is

employed the operational models, the different threats and risks could be presented to an organization compared to the common IT solutions.

Unluckily, implementing security controls into these solutions is usually supposed as making them more inflexible. For an organization, the transferring of their critical data and applications from their central data networks is of great concerned. To overcome these concerns, cloud computing provides a solution that should ensure the privacy and security of the customer's applications and services are highly protected (Rittinghouse, J. W., & Ransome, J. F., 2017). In this paper, a classification of network security issues of cloud computing is provided based on SPI model. The main vulnerabilities of this system are identified and the major risks and threats related to cloud computing are found and reviewed based on the recent literatures. A threat or risk is well known as a potential or unwanted an attack that may result in the misappropriation of resources or information. The vulnerability term is defined as a faults inside the system which enables an assault to be happened. a few surveys introduced cloud computing security in general without taking in consideration the vulnerabilities and threats. In this survey, a list of vulnerabilities and threats are presented in related with cloud computing security level and which cloud resources and services are affected by these vulnerabilities and threats.

The remains the following sections make up the paper II highlights the findings of our systematic research analysis. Followed in the subsection III, the depth of the security aspect for each of the cloud model's layers is defined and analysed the main vulnerabilities and threats in the cloud computing model. Finally, section IV is summarized and concluded the findings.

Systematic Analysis of the Cloud Security Issues

Related Systematic Review

To summarize the current existing vulnerabilities and threats related to the cloud computing security, a literature systematic reviews is carried out. In order to analyse the major security issues related to vulnerabilities and threats in these related existing literature for identifying the cloud computing security levels.

Question Validation

In this step, the question is focused on identifying the main issues in the cloud computing security with related to threats, risks, vulnerabilities, solutions and requirements of the network security of cloud computing. Hence, the question is addressed as follows: what is

the most serious flaws and dangers in cloud computing security network? Therefore, the keywords are stated in that order to fulfil the question handling; cloud security, SPI security, cloud systems, vulnerabilities in the cloud, dangers to the cloud, and cloud suggestions, and delivery models security.

Sources Selection

The selection of sources are defined in this research based on the following: Scholar Google, ACM digital Library, ScienceDirect, DBLP, and IEEE digital library. Once the list of sources is defined, the study selection procedure and criteria are explained. The research criteria are dependent on the research question. introduced in previous sub-section. Therefore, this research is contained topics related only to the security of dangers, vulnerabilities, and hazards associated with cloud computing.

Results and Discussion

Table 1 shows the findings of the systematic ideas and themes. As can be noticed from Table I, the threats and vulnerabilities are mostly concerned with cloud computing security issues. The approaches in the systemic review are discussed in terms of classify, identify, and analyse in respect with the vulnerabilities and threats of the cloud computing.

The studies that were examined are focused on the existing threads and risks in the cloud computing, offering a solution on how these threads can be avoided or recovered. The studies also showed a direct relationship between threats or vulnerability and possible mechanism and overcome solutions these problems. Additionally, other security issues are discussed in this study such as trust, data security, security advice, and potential solutions to these threats and hazards.

The cloud model introduces three types of service levels (Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L.L., 2009). Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) are the three types (IaaS). The capacity of employing apps offered by cloud users and operating on cloud infrastructure is referred to as SaaS. SaaS apps may be accessible over the internet. From several users using a simple or based web browser. PaaS is a platform that allows the consumer to deploy the applications onto the cloud infrastructure. This capability does not need any installing of tools or software on the client's local machines. IaaS is defined as the capability of allowing the customers to process their applications on networks, storage, and any other

cloud resources. This allowed the users to run their applications and software on the same cloud computing models.

To analyse the security problems in cloud computing, an understanding of the relationship between the cloud models should be clarified. Generally, SaaS and PaaS are stacked on the top of IaaS model. Hence, any attack or threat in IaaS will be affected both SaaS and PaaS. However, PaaS provides an applications platform for SaaS, which effects the security risk between each model. In the same time, SaaS provider can barrow a PaaS may rent infrastructure from IaaS, and PaaS can rent development environments from PaaS providers. Therefore, each layer has its own security risk and threat. Leading to have or creates confusion on which service or model was responsible on the attack.

SaaS Security Threats and Issues

In SaaS providers, the users have application services like business applications, emails, CRM, ERP, SCM, and conferencing software (Zhang, Q., Cheng, L., & Boutaba, R., 2010). In this model, the security control is less among the three basic levels. However, some security concerns might be raised in this cloud level.

Table I The subjects that been analysed

Subjects/References
Vulnerabilities
Threats
Mechanisms/Recommendations
Security Standards
Data Security
Trust
Security Requirements
SaaS, PaaS, IaaS Security

PaaS Security Threats and Issues

In PaaS providers, the software and hardware layers is handled based on the deployment of cloud apps without incurring any costs purchase (Subashini, S., & Kavitha, V., 2011). The security level in PaaS is depending on network and web browser. The application security level is made up of two primary software layers: user-facing application security and platform security. As a result, the platform's security is within the authority of the providers, who also safeguard user applications. However, the most challenges that PaaS layer are

described as follow; life cycle development, relationships between the third party, and security of the infrastructure.

In the life cycle development, the prospective of the developers is facing a complexity from the application development. Where, the applications could be built a speed secure host in the same cloud. If the speed changes at each applications, the cloud will be affected in both security and the System Development Life Cycle (SDLC) (Onwubiko, C., 2010). Hence, in PaaS the developer should be frequently upgraded the applications to Ensure that their application development is completed quickly and securely. Developers should bear in mind, however, that any modifications to PaaS apps might have an impact on the security of the PaaS applications. Because the PaaS provides third-party web services such as mashups (Ju, J., Wang, Y., Fu, J., Wu, J., & Lin, Z., 2010), users' services apps may be exposed to a security risk. Users should rely on the security of web-hosted development as well as third-party apps and services.

In PaaS infrastructure, the users generally do not have the ability to access the infrastructure layer. Therefore, the PaaS providers are responsible on the applications services as well as the security of the infrastructure (Viega, J., 2009). As a result, there is less literature on security problems at the PaaS and SaaS levels. Software as a service (SaaS) is delivered via the internet, whereas PaaS provides development tools for building SaaS applications. However, because both PaaS and SaaS employ multi-architecture, there may be various security issues. Both SaaS and PaaS, as is widely known, allow data processing and transport. As a result, it is the provider's obligation to ensure that the data being exchanged in the cloud is safe.

IaaS Security Threats and Issues

Users can execute any program with complete administration and access to resources at the IaaS level (Ertaul, L., Singhal, S., & Saldamli, G., 2010). Storage, servers, networks, and virtualized systems are all available with IaaS. These resources are available over the internet. In comparison to PaaS and SaaS, this allows customers to have more control over security, as long as the virtual machine is secure. The program is executed on the providers' virtual machines, and they are in charge of its security settings. Despite these IaaS features, cloud providers have control over the resources. As a result, additional measures should be made to safeguard cloud systems and data.

Other Security Threats and Issues

These applications are often accessed using a web browser. Web application flaws, on the other hand, may expose any SaaS program to vulnerabilities. Opponents have utilized the

internet to hack into users' computers and do harmful actions such as stealing sensitive data. Security concerns in SaaS apps are similar to those in any online application, but traditional security tactics fail to adequately protect them from assaults, necessitating the development of new techniques. The Open Online Application Security Project (OWASP) has identified the top ten security risks to web apps (Zhang, Y., Liu, S., & Meng, X., 2009). There are a lot more security issues, but it's a good start for protecting web apps.

Scalability, configurability via metadata, and multi-tenancy are all features that may be used to classify SaaS applications into maturity models. Although this design includes flaws, the security issues aren't as severe as they are in previous versions. The provider also offers different scenarios of the apps for each client in the next design, but most cases use the same program code. Customers can customize various configuration options in this product to fit their own demands. Multi-tenancy is optional in the third maturity model, thus one example serves all clients. This method makes considerably more effective use of the resources, but it has limitations in terms of scalability. Because data from many renters is it may be stored in the exact same data source, the hazard of information seepage between the renters is significant. Customers' information must be kept distinct from that of other clients, according to security rules (Viega, J., 2009). Applications may be scaled in situ under the last architecture by transforming the application of the program to another better server if needed.

Information security is a usual worry and Interest for almost all technologies, which becomes dangerous when SaaS computer workers have to depend on their suppliers for adequate protection. data is often created in unencrypted methods and placed in the cloud when using SaaS, so the SaaS providers will be held the responsibility of the information's security throughout it is being prepared, kept, and stored. Furthermore, the backup of the data is an important function so as to assist recovery in the event of a disaster, noting that it could raise security worries (Onwubiko, C., 2010).

Virtualization permit users to create, imitate, share, move, and reinstall virtual computers that allowing them to execute a variety of applications (Dawoud, W., Takouna, I., & Meinel, C., 2010). However, because of the additional level that must be anchored, it opens up entirely new options for assailants.

The security of Virtual machines will become as important as physical device security, any weakness in either of them will have an impact on the other. VMs, have two boundaries that are virtual and physical in comparison to physical servers (Almorsy, M., Grundy, J., & Müller, I., 2016). Virtual environments are susceptible to some other types of attacks as are

regular infrastructures; so the protection is more difficult because virtualization provides additional points of greater interconnection complexity and entry.

The VMM is a low-level software application that monitors and manages its virtual machines, has security vulnerabilities like any other program. Preservation of the VMM device to a minimum and essential risk of vulnerabilities makes it easier to detect and fix any flaws. Virtualization also offers an option to move virtual machines across physical servers to withstand failovers, load balancing, or possibly upkeep (Grobauer, B., Walloschek, T., & Stocker, E., 2010); this helpful feature also can increase protection difficulties. An assailant is able to compromise the migration component in the VMM and transport a victim virtual machine to some malicious server. Additionally, it's apparent that VM migration exposes the information in the VM to the system that may compromise its information integrity as well as confidentiality. A malicious virtual machine is usually migrated to the next multitude (with a different VMM) compromising it.

VMs on the same server can talk about CPU, I/O, memory, and other things. Sharing information between VMs may compromise each VM's security. For example, a malicious VM can deduce certain information about other VMs using shared memory and/or other shared resources without compromising the hypervisor. Two VMs can interact via covert channels, circumventing all of the rules specified by the VMM's security component (Ranjith, P., Priya, C., & Shalini, K., 2012). As a result, a malicious Virtual Machine can monitor shared materials without being detected by its VMM, allowing the attacker to deduce certain information about other virtual machines.

Security Threats and Risks in Cloud

We examine the present security flaws and hazards associated with cloud computing in a methodical manner. We evaluate which cloud service models, if any, are impacted by these security concerns for each threat and vulnerability. Table II shows a vulnerability assessment in Cloud Computing. This study includes a brief description of the vulnerabilities as well as a list of cloud service airers (SPI) that may be affected. We largely focus on technology-based vulnerabilities in this study; nevertheless, there are additional vulnerabilities that are common to the company, albeit they've been overlooked since they can have a negative impact. The protection of the cloud plus its fundamental platform. Several of these vulnerabilities are the following.

Poor recruiting and employee screening processes (Catteddu, D., 2009) – a number of cloud providers refused to do background checks on their vendors or workers. Privileged clients, such as cloud administrators, typically have unrestricted access to cloud data.

Lack of customer background checks - almost all cloud providers do not verify their customers' histories, and almost anybody can open an account with a valid credit card and email address. Attackers can use fictitious accounts to carry out almost any harmful operation without being detected (Catteddu, D., 2009). This is true across all types of organizations; however, it has a greater impact in the cloud since other individuals interact with the cloud: cloud suppliers, third-party suppliers, organizational customers, suppliers, and end users.

Cloud computing makes use of a variety of current technologies such as virtualization, online browsers, and web services, accelerating the growth of cloud locations. As a result, any vulnerability connected to these solutions also affects the cloud, and it might have a significant impact.

Table II Vulnerabilities in cloud computing

Vulnerabilities	Description	level
V01(resources)	Inaccurate modeling usage	SPI
V02 (data related)	Unrestricted allocation	SPI
V03 (Insecure Appl.) interfaces	Weak credential	SPI
V04 (virtual machine)	Possible covert channel	SPI
V05 (virtual image)	Uncontrolled virtual machine	SPI
V06 (hypervisors)	Complex code	SPI
V07 (virtual network)	Sharing of virtual networks	SPI

Table III Threats in cloud computing

Threats	Description	Level
T01 (account risk)	Attacker access user profiles	SPI
T02 (data leakage)	Attacker recover data	SPI
T03 (denial of service)	the system cannot satisfy any request	SPI
T04 (VM scape)	to take control of the infrastructure	SPI
T05 (VM hopping)	VM is able to gain access to another VM	SPI
T06 (VM creation)	Malicious VM creation	SPI
T07 (VM migration)	Insecure VM migration	SPI

Table IV threats and vulnerabilities relationship

Vulne.	Threats	Description	Possible solutions
V01	T01	Use user profile account	Identity and Access Management Guidance
V02	T02	Data cannot be removed	Dynamic credential
V03	T03	Side channel	Digital Signatures
V04	T04	An attacker can request more computational resources	limited computational resources scanners
V05	T05	command injection	Web application scanners
V06	T06	most virtual machines monitors	Mirage
V07	T07	Sniffing and spoofing virtual networks	network modes: “bridged” and “routed

Table II shows the virtualization and data storage are the most important, and any attack on these will cause harmful. Attacks on lower levels have a far greater impact on the higher levels. Table III provides an overview of the hazards associated with Cloud Computing. Table III, like Table II, discusses the dangers connected with the science used in cloud settings, as well as which cloud service providers are vulnerable to these threats. Table IV describes the connection between risks in addition to vulnerabilities and how the threat is able to make use of vulnerability to compromise the product.

The goal of this investigation is also to identify any current defenses that might be used to eliminate these risks. Misuse patterns (define how a wrong use is carried out from the enemy's point of view) are commonly used to present this information in a thorough manner (Catteddu, D., 2009). For example, during live migration, an adversary can inspect or even tamper with the contents in the VM declare papers. Because VM migration transfers data through network stations that are typically unsecured, such as the Internet, this may be possible. The following approaches have been proposed to reduce insecure VM migration: TCCP (Catteddu, D., 2009) offers confidential execution of secure migration operations and VM also. PALM (Reuben, J. S., 2007) proposes a protected migration process that provides VM live migration features under the condition. That a VMM protected system is active and present. Another threat is yet a cloud threat in which an attacker captures a malicious VM image that contains some type of malware or virus.

This risk is doable because every genuine user is able to make a VM picture and also post it over the provider's repository where various other people are able to access them.

If the malicious VM impression features malware, it is going to infect other VMs instantiated with this particular malicious VM image. Mirage, an image management

system, was presented as a solution to the danger (Wei, J., Zhang, X., Ammons, G., Bala, V., & Ning, P., 2009). Entry management framework, repository maintenance services, provenance tracking system, and picture filters are among the security management capabilities available.

Conclusion

Cloud Computing is a relatively new concept that offers a number of benefits to its users; yet, it also raises certain security concerns that may hinder its adoption. Understanding the vulnerabilities that exist in Cloud Computing can assist organizations in making the transition to the Cloud. Because Cloud Computing makes use of a variety of technologies, it also inherits their security problems. Traditional web applications, information hosting, and virtualization were investigated, however some of the solutions offered were either unavailable or undeveloped. We've listed security issues for three cloud models: IaaS, PaaS, and IaaS, with versions varying. Virtualization, storage, and networks, as mentioned in this publication, are the most serious security concerns in Cloud Computing. One of the key challenges for cloud users is virtualization, which allows multiple individuals to communicate about a physical server. Furthermore, there is a difficulty in that there are numerous types of virtualization solutions, each of which may deal with security systems in a different way. When communicating with remote virtual devices, virtual networks might be the target of a few assaults. Some studies have noted cloud security issues without distinguishing between threats and vulnerabilities. We've focused on this distinction whenever we believe it's critical to notice these issues. Enumerating these security concerns was insufficient; as a result, we established a link between vulnerabilities and threats, allowing us to determine which flaws aid in the delivery of these risks while also allowing the device to become more powerful. In addition, some existing treatments for mitigating these risks have been highlighted. New security approaches, as well as modified traditional solutions that leverage cloud architectures, are required. Traditional security measures may not perform well in cloud environments since it is a complex structure made up of a variety of solutions. Three of the items in Table IV have been labeled as misuse patterns.

References

Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. *arXiv preprint arXiv:1609.01107*.

Catteddu, D. (2009). Cloud Computing: benefits, risks and recommendations for information security. *In Iberic Web Application Security Conference*, Springer, Berlin, Heidelberg, 17-17.

Dawoud, W., Takouna, I., & Meinel, C. (2010). Infrastructure as a service security: Challenges and solutions. *In the 7th International Conference on Informatics and Systems (INFOS)*, 1-8.

Ertaul, L., Singhal, S., & Saldamli, G. (2010). Security Challenges in Cloud Computing. *In Security and Management*, 36-42.

Grobauer, B., Walloschek, T., & Stocker, E. (2010). Understanding cloud computing vulnerabilities. *IEEE Security & privacy*, *9*(2), 50-57.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L.L. (2009). On technical security issues in cloud computing. *In IEEE international conference on cloud computing*, 109-116.

Ju, J., Wang, Y., Fu, J., Wu, J., & Lin, Z. (2010). Research on key technology in SaaS. *In International Conference on Intelligent Computing and Cognitive Informatics*, 384-387.

Li, W., & Ping, L. (2009). Trust model to enhance security and interoperability of cloud environment. *In IEEE international conference on cloud computing*, *Springer, Berlin, Heidelberg*, 69-79.

Marinos, A., & Briscoe, G. (2009). Community cloud computing. *In IEEE international conference on cloud computing*, Springer, Berlin, Heidelberg, 472-484.

Onwubiko, C. (2010). Security issues to cloud computing. *In Cloud Computing*, Springer, London, 271-288.

Ranjith, P., Priya, C., & Shalini, K. (2012). On covert channels between virtual machines. *Journal in Computer Virology*, *8*(3), 85-97.

Reuben, J.S. (2007). A survey on virtual machine security. *Helsinki University of Technology*, *2*(36).

Rittinghouse, J.W., & Ransome, J.F. (2017). *Cloud computing: implementation, management, and security*. CRC press.

Rosado, D.G., Gómez, R., Mellado, D., & Fernández-Medina, E. (2012). Security analysis in the migration to cloud environments. *Future Internet*, *4*(2), 469-487.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.

Viega, J. (2009). Cloud computing and the common man. *Computer*, *42*(8), 106-108.

Wei, J., Zhang, X., Ammons, G., Bala, V., & Ning, P. (2009). Managing security of virtual machine images in a cloud environment. *In Proceedings of the ACM workshop on Cloud computing security*, 91-96.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, *1*(1), 7-18.

Zhang, Y., Liu, S., & Meng, X. (2009). Towards high level SaaS maturity model: methods and case study. *In IEEE Asia-Pacific services computing conference (APSCC)*, 273-278.

Zhao, G., Liu, J., Tang, Y., Sun, W., Zhang, F., Ye, X., & Tang, N. (2009). Cloud computing: A statistics aspect of users. *In IEEE International Conference on Cloud Computing*, Springer, Berlin, Heidelberg, 347-358.