A Review of Challenges and Security Risks of Cloud Computing

Hussam Alddin S. Ahmed, Mohammed Hasan Ali, Laith M. Kadhum,
Mohamad Fadli Bin Zolkipli, Yazan A. Alsariera
Faculty of Computer System and Software Engineering, University Malaysia Pahang, Kuantan, Pahang, Malaysia.
hussam.alddin@outlook.com

***Abstract*—Cloud computing has been an attention in the new era of the IT technologies as there is an increase demand in the services or utility computing all over the wide world web. Security risk resulting from resource sharing throughout the cloud computing becomes one of the most challenging concerns in providing powerful processing and storage as on-demand services. Taking the advantage of low cost derived from the increase in efficiency and performance facilitated by cloud computing, governments and organizations around the globe are motivated to build or migrate to the cloud. However, there are still many technical issues relating to the features of cloud computing and the provision of quality service, leading to a delay in adopting cloud computing. This review paper highlights the security risks and challenges of cloud computing and study the security requirements for cloud computing. The primary aim of this review is to classify the security risks and challenges related to the different forms of cloud computing (SaaS, PaaS and IaaS).**

***Index Terms*—Cloud Computing Security; Cloud Computing Risk.**

I. Introduction

Cloud computing has increased dramatically: Microsoft, Google, and a lot of enterprises have been moving to the cloud in the last few years. The notion of cloud computing is disconnecting the software from the operating system and the hardware, and it does not mean virtual computing, The software is no longer depend on the hardware and the operating system, so if they fail, the software automatically migrates to other recourses. According to [1], the term ‘cloud’ is ‘remote data center’. It also has two meanings. The first is the access of information and data resources via Internet using Web browser. The second is paying for the computing resources based on usage. Cloud computing has been defined by The National Institute of Standards and Technology (NIST) as “a model for enabling universal, suitable, on-demand network access to share pool of configurable computing resources (e.g., servers, networks, applications, storage, and services) that can be rapidly released and provisioned with minimal management effort or service provider interaction” [2]. In addition, Gartner defines cloud computing as a kind of computing style massively scalable IT that enables the capable and deliverable IT as services to external customers using internet technologies [3]. Kepes defines cloud computing in a simple term as “the infrastructural paradigm shift that enables the ascension of SaaS. It is a broad array of web based on services aimed to allow users to obtain a wide range of functional capabilities on a pay-as-you-go basis that previously required tremendous hardware/software investments and professional skills to acquire” [4]. Furthermore, Kumar et al. define cloud computing as a storage system that gives access to the files anywhere though any technology over the internet by storing the information on cloud server rather than traditional computer.

Cloud computing uses virtualization methods as well as automation decision making for hardware virtualization as well as server virtualization [5]. Cloud computing provides customers with a virtual infrastructure that they simply store and run software and share the server resources for many applications using virtualization techniques instead of running one application in the server with the traditional servers. It is possible to run many applications in one server by using hypervisor to implement virtualization. Outlook, Facebook, G-mail, Google docs and YouTube are some examples of cloud services. Services delivered throughout the internet can be generally referred as cloud computing.

Cloud computing has five essential characteristics: measured service, broad network access on-demand self-service, rapid elasticity and resource pooling. Taking into account to reduce cost, it is aimed to increase the efficiency and performance of computing systems. According to [6], 91 % of the organizations and enterprises in the Europe and US that decide to migrate to cloud environment was due to cost reduction facilitated by cloud computing.

II. Cloud Main Forms (Providers)

Cloud computing [6]-[11] systems can be classified into three main categories based on the types of services it can provide to customers. The three kinds of services are: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a service (IaaS). The descriptions of the three types of services are presented below.

A. Software as a Service (SaaS) (End customers)

It is a kind of cloud computing that provides end customers with services such as apps, computing process, and storage, and the user can use these services remotely. There are many kinds of cost plan model for such a service, such as fixed subscription and usage-based pricing plan model. The software can run on the network with the user’s interface living on a thin client. Examples of SaaS provider are mentioned in Table 1.

B. Platform as a Service (PaaS): (Developers)

It is a kind of cloud computing service that provides a high level of integrated environment for developers to enable them to build, test, and deploy practice software. However, there are some limitations resulting in developers facing some restrictions when deploying software in this kind of service and exchanging for software scalability. Examples of PaaS providers are as mentioned in Table 2.

Table 1
Software as a service provider

Name	Service provided
Drobox and SkyDrive from Microsoft	Files and folders storage service
Salesforce	Online CRM (Customer Relationship Management)
Live Mesh from Microsoft	Files and folders to be shared and synchronized across multiple devices.
Outlook from Microsoft	Email and documents processing service
Open ID and OAuth	Identity service
Amazon Simple Queue Service	Integration service
Google Maps, Bing maps and Yahoo! Maps	Mapping service
Google Checkout, Amazon Flexible Payments Service, PayPal	Payments service
Google Search, Yahoo! BOSS, Alexa	Search service

Table 2
Platform as a service provider

Name	Service provided
Google's App Engine	Build Web applications and its Web application frameworks
Godaddy	Build Web applications and hosting
Heroku	Ruby on Rails for building Web applications
Mosso	Web hosting
Microsoft Azure	Proprietary
Force.com	Proprietary

C. Infrastructure as a service (IaaS): (system administrators)

It is a kind of cloud computing with the concerns to provide IT for sys-admins (system administrators) by supplies hardware, software and equipment to deliver software application environments with a resource usage-based pricing model. IaaS can scale up or down automatically depending on the required resources of an application. IaaS computing process and storage infrastructures are open to public access with a fix utility pricing model.

Other services that can be considered as cloud computing forms are:

- Anything(X) as a service (XaaS): It is a kind of cloud computing that has been coined for the first time in 2008. It is about sharing the capabilities of the hardware throughout the software. It is going to be possible and can be achieved through virtualization, and some examples are such as: Database as a Service (DBaaS), Desktop as a Service (DaaS), Network as a Service (NaaS), Monitoring as a Service (MaaS) and Content delivery as a Service [3], [10], [12]-[17].
- Component as a service (CaaS): It is related to services that provide an API to web services in order to make use of the web services as a component. For example, CaaS can be provided as end-to-end business services using the SaaS services within their API [1].

III. TYPES OF CLOUD

Cloud computing architecture is wide: In any of them, the client is free to choose which type depending on the hardware and the software needed and the cost. Basically, cloud architecture are as below [11].

- Public Cloud: This type of cloud computing architecture is made for the client as usage plan model payment with the method of pay as use. Examples of this type are Microsoft Azure, Google App Engine, and Amazon Web Services.
- Private Cloud: This type of cloud computing architecture is made for a critical infrastructure and for private companies and organizations purpose. This kind of cloud computing environment is not available for the public use. Data centers for private companies and government data centers is an example of private cloud.
- Community Cloud: It is a powerful infrastructure that enables the third party to provide applications and platforms on which new service can be developed, and it involves a number of different stakeholders.
- Hybrid Cloud: This type of cloud computing architecture is made of a combination of public and private clouds. It is defined by the National Institute of Standards and Technology (NIST) as "a hybrid cloud that has a combination of public and private clouds bound together by either standardized or proprietary technology that enables data and application portability" [2].

Cloud computing, also known as Utility computing has growing dramatically by several number of service providers. These service providers offer cloud computing services, such as virtual servers and storage based on on-demand model; hence, making it possible for many of the customers and organizations to move into the cloud and get Elastic and Flexible services [11].

However, the dramatically increase of on-demand application in the last few years has been facilitated by the growth of the wide world web. The prospective of cyber-attacks have been increasing at high level. Thus, security concern relating to the risk factors for the current cloud computing architecture must be taken into consideration. Therefore, this study aims to highlight the current cloud computing architecture risk factors and related issues as mentioned below.

IV. ATTACKS AND THREATS IN THE CLOUD SECURITY (RISK FACTORS)

The attacks and threats in the cloud security are listed below:

- Account and service hijacking: It is one of the most serious security threats. It happens when the attackers intend to hack a web service in a website hosted in cloud server or service providers, and then install their control software in the cloud provider infrastructure [18].
- Abuse and nefarious use of cloud computing: For this type, attacker can use the cloud computing power for the cloud infrastructure to attack targets using spam and malware, like botnet. According to the CSA it is the top security threat in the cloud computing [19].

- Backdoor Channel attacks: This kind of attack happens in IaaS, when it gives an effective user's high permeation on the VM's or the Hypervisor level. This may affect the service availability and data privacy [20].
- Cross site scripting attacks: It is also called XSS. It is one of the most powerful attacks of security weakness found through the web applications. One of the widest range scripting is the Java script language commonly used in such attack [11].
- Cloud malware injection attack: This is one of the top cloud computing security list attaches, where its purpose is to inject a malware, macules application or virtual machine to the cloud infrastructure [21].
- Denial of Service attacks: In this type of attack, the service will not be available when the users intend to request it from the server. They will get the error 404 that provides the service is not found [11].
- Insecure application programming interface: This type is when the service providers deliver the service to the customers using APIs, and the APIs have an encryption with secure authentication, provided with secure access control and activity monitoring mechanisms [22].
- Man in the middle attacks: In this type of attack, the hacker makes an autonomous connection between the customer and the service provider to observe the data and information for the service without their knowledge [11].
- Metadata spoofing attack: In this type, the web services providers send the service metadata document to the client system that has all the information about the service invocation, such as security requirements, message format and network location. In this case, the attacker's objective is to reengineer the web service metadata descriptions, demanding to modify the network references and endpoints to the security policies [23].
- Malicious insiders: This kind of security threat happens when there is a lack in the security concern for how to access the service provider by employees to the virtual properties of the cloud. This threat may be more complex due to employee's privilege in lack of implementing in the cloud system and updated the responsibilities when their behavior or job is changed [18].
- Phishing attack: It is about affecting the user privacy and the exposure of its data and information by allowing users to access fake web link installed in their PCs: Malicious codes expose that data [18].
- SQL Injection attacks: This kind of issue happens when hackers try to attack website database through the code injected in SQL statements using the website inquiry methods that can deactivate a security in a website [11].
- Shared technology's vulnerabilities: This issue related to cloud computing that uses the same infrastructures used in the internet shared among the cloud customers. Thus, all the problems currently in the internet infrastructures will be migrated to the cloud. In other way, the traditional components have not been developed to share the resources in the cloud computing systems [18].
- Sniffer attacks: For this type attack, attacker intends to read the content of the network packet, although there are no encrypted methods have been applied during the sending of the data. Sniffer could be a script, an application or a device [11].
- Security concern with the virtual machine Manager: The concern of type of security is that the service providers have to be very careful on the services provided by the VM technology to the users because this type of technology suffers from some security levels in some cases [11].
- Unknown risk profile: This kind of security threat happens as a result of making attention on the functionalities and the features gained from implementing cloud services without making any consideration for the security technologies and producers that are going to be developed. The concern is on which the features may have access to the data from third-party and this data may be disclosed for any reasons [18].
- Zombie attack (DoS/DDoS): It happens at the indirect/ direct flooding to host in the Hypervisor, Network, or VM level. It may affect the service availability and create a user account for false service usage [18].

V. CLOUD COMPUTING CHALLENGES

- **Access controls:** It is a concern for all service providers, in which it may cause a security issue by revealing user's data and giving hackers the ability to gain access to the organization's infrastructure [24].
- **Accounting:** It is one of the key aspects that have to be measured in deploying services in the cloud computing solutions in order to maintain network management [25].
- **Compliance:** Cloud computing has a weak point for supporting the methods of compliance management. This may cause serious issues in data security and privacy [25].
- **Cross-Organizational Security Management:** It is a big challenge in cloud computing to achieve and maintain security requirements and compliance with SLAs. It needs to have a corporation among organizations to ensure an appropriate security requirement in cloud computing is achieved [26].
- **Extensibility and Shared Responsibilities:** The service providers and users have to give attention to the security concern in cloud computing. Until now, there is no clear view of how the security responsibilities are going to be achieved in cloud computing [27].
- **Private Cloud:** Since the term of a private cloud is on-premises, so it is expected that the location that will be working is just like traditional computing. By using virtualization technologies for computing resources, the computing resources are virtually extendable or de-extendable depending on the user's needs. This will give accessibility to shared resources for the entire departments in the organization. However, this has not been fully implemented in a wide range in the organizations. In other words, it is a halfway step to be implemented by the public cloud services [1].

- **Heterogeneity:** Heterogenous issue exists when various service providers deliver a massive number of services using different technologies. Heterogeneity could be happen as a result of differences in software or hardware level [28].
- **Identity management (IdM):** It is a key aspect in cloud computing security that has the goals to perform verification and validation process among heterogeneous clouds services. However, it still has some issues associated with interoperability among the latest security technologies [29].
- **Integration:** When customers or organization need to implement multiple service providers for several reasons, they have to implement and integrate software and data in several clouds. In some cases, this issue can be solved by using hybrid clouds [1].
- **Performance:** Cloud computing may reduce the cost, but the performance issues such as communication time between the user and the cloud services has become a problem because as the number of users increases, the amount of the information and the data to be transferred to the users increases as well. This will cause a high load on the hardware and software. Another factor is that there are differences in the distance between the user and the service providers. Furthermore, the customers may scale up their cloud infrastructure beyond the original expectation, leading to a serious problem to the service providers [1].
- **Bandwidth requirements:** Before implementing a cloud service, organizations have to evaluate the communication bandwidth requirements and assess the services with respect to the large amount of data transmission [1].
- **Monitoring:** When cloud computing is based on service monitoring, there will be an enormous demand on using monitoring throughout cloud services and activities either in the public or private infrastructure [25].
- **Risk analysis and management:** It is an important key aspect in the cloud security. It is about decreasing the loud capacity in cloud computing by scanning and identifying any risk before providing the service to the customers [25].
- **Service Level Agreement:** It is an important component of the contractual relationship between a cloud service customer and a cloud service provider. Given the global nature of the cloud, SLAs usually span many jurisdictions, with varying applicable legal requirements, especially with respect to the protection of the personal data hosted in the cloud service [30].
- **Virtualization:** It is a way to deliver cloud services to the customers, especially when applying IaaS services, but it is still suffering from security issues [28].
- **Policies:** Cloud computing needs a well-written policy for the security procedures and guidelines that will be implemented in the solutions [31].
- **Security in the web browser:** The security requirements in the web browser is not enough to handle the user’s needs in terms of complex and sophisticated banking and critical environments for a shared solution, such as cloud solutions [32].

VI. Conclusion and Future Work

Cloud computing has been getting major interests in the industry fields and academic fields lately, as it is reflected a backbone of future modern societies. Cloud computing helps economic efficiencies and reduces costs. Governments, organizations, and enterprisers are looking for enabling features of cloud computing. However, without suitable solutions for a substantial number of security risks and privacy challenges, the adoption of the cloud computing is still a far away in the near years to come. In this work, the latest risks and challenges of cloud computing have been identified. Making a security model concern about the risks and challenges identified is going to be our future research.

References

[1] Kim, W., et al. Adoption issues for cloud computing. in Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia. (2009). ACM.

[2] Mell, P. and T. Grance, Draft nist working definition of cloud computing. (2009).

[3] Plummer, D.C., et al., Cloud computing: Defining and describing an emerging phenomenon. Gartner, (2008) June 17.

[4] Sajid, M. and Z. Raza. Cloud computing: Issues & challenges. in International Conference on Cloud, Big Data and Trust. (2013).

[5] Kumar, S., et al., An Approach of Creating a Private Cloud for Universities and Security Issues in Private Cloud, in Recent Science. (2013).

[6] Modi, C., et al., A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing. 63(2) (2013) 561-592.

[7] Kaufman, L.M., Data security in the world of cloud computing. Security & Privacy, IEEE, **7**(4) (2009) 61-64.

[8] Loganayagi, B. and S. Sujatha. Cloud Computing in Stax Platform. in Computer, Communication and Electrical Technology (ICCCET), 2011 International Conference on. (2011). IEEE.

[9] Sun, D., et al. A Dependability Model to Enhance Security of Cloud Environment Using System-Level Virtualization Techniques. in Pervasive Computing Signal Processing and Applications (PCSPA), 2010 First International Conference on. (2010). IEEE.

[10] Schaffer, H.E., X as a service, cloud computing, and the need for good judgment. IT professional. 11(5) (2009) 4-5.

[11] SUBBIAH, M., D.S.S. MUTHUKUMARAN, and D. RAMKUMAR, Enhanced Survey and Proposal to secure the data in Cloud Computing Environment. International Journal of Engineering Science, (2013) 5.

[12] Kim, K.H., A. Beloglazov, and R. Buyya. Power-aware provisioning of cloud resources for real-time services. in Proceedings of the 7th International Workshop on Middleware for Grids, Clouds and e-Science. (2009). ACM.

[13] Loganayagi, B. and S. Sujatha. Creating virtual platform for cloud computing. in Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on. (2010). IEEE.

[14] Kim, K.H., A. Beloglazov, and R. Buyya, Power- aware provisioning of virtual machines for real- time Cloud services. Concurrency and Computation: Practice and Experience, 23(13) (2011) 1491-1505.

[15] Loganayagi, B. and S. Sujatha, Enhanced cloud security by combining virtualization and policy monitoring techniques. Procedia Engineering, 30 (2012) 654-661.

[16] Mladenow, A., et al. Value Creation Using Clouds: Analysis of Value Drivers for Start-Ups and Small and Medium Sized Enterprises in the Textile Industry. in Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on. (2012). IEEE.

[17] Geelan, J., Twenty-one experts define cloud computing. Cloud Computing Journal, **2** (2009) 1-5.

[18] Younis, M. and K. Kifayat, Secure cloud computing for critical infrastructure: A survey. Liverpool John Moores University, United Kingdom, Tech. Rep, (2013).

[19] Khorshed, M.T., A.S. Ali, and S.A. Wasimi, A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation computer systems, 28(6) (2012) 833-851.

[20] Modi, C., et al., A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1) (2013). 42-57.

[21] Chou, T.-S., Security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information Technology, 5(3) (2013) 79.

[22] Akande, A.O., N.A. April, and J.-P. Van Belle. Management Issues with Cloud Computing. in Proceedings of the Second International Conference on Innovative Computing and Cloud Computing. (2013). ACM.

[23] Jensen, M., N. Gruschka, and R. Herkenhöner, A survey of attacks on web services. Computer Science-Research and Development, 24(4) (2009) 185-197.

[24] Zissis, D. and D. Lekkas, Addressing cloud computing security issues. Future Generation computer systems, 28(3) (2012) 583-592.

[25] Moreno-Vozmediano, R., R.S. Montero, and I.M. Llorente, Key challenges in cloud computing: Enabling the future internet of services. Internet Computing, IEEE, 17(4) (2013) 18-25.

[26] Khalil, I.M., A. Khreishah, and M. Azeem, Cloud computing security: a survey. Computers, 3(1) (2014) 1-35.

27. Zhang, L., et al., Cloud manufacturing: a new manufacturing paradigm. Enterprise Information Systems, 8(2) (2014) 167-187.

[28] Crago, S., et al. Heterogeneous cloud computing. in Cluster Computing (CLUSTER), 2011 IEEE International Conference on. (2011) IEEE.

[29] Lar, S.-U., X. Liao, and S.A. Abbas. Cloud computing privacy & security global issues, challenges, & mechanisms. in Communications and Networking in China (CHINACOM), 2011 6th International ICST Conference on. (2011). IEEE.

[30] Oliveira, A.C., et al. Efficient network service level agreement monitoring for cloud computing systems. in Computers and Communication (ISCC), 2014 IEEE Symposium on. (2014). IEEE.

[31] Zhang, Q., L. Cheng, and R. Boutaba, Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1) (2010) 7-18.

[32] Wei, L., et al., Security and privacy for storage and computation in cloud computing. Information Sciences, 258 (2014) 371-386.