SECURITY ISSUES IN CLOUD-BASED BUSINESSES

Mohamad Ibrahim AL Ladan

Department of Computer Science, Rafik Hariri University, Meshref, Lebanon

ABSTRACT

Cloud-based Business is a Business running and relying on Cloud computing IT paradigm. Cloud computing is an emerging technology paradigm that transfers current technological and computing concepts into utility-like solutions similar to electricity and communication systems. It provides the full scalability, reliability, computing resources configurability and outsourcing, resource sharing, external data warehousing, and high performance and relatively low cost feasible solutions and services as compared to dedicated infrastructures. Cloud-based Businesses store, access, use, and manage their data and software applications over the internet on a set of servers in the cloud without the need to have them stored/installed locally on their local devices. The cloud technology is used daily by many businesses/people around the world from using web based email services to executing heavy complex business transactions. Like any other emerging technology, Cloud computing comes with a baggage of some pros and cons. It is very useful in business development as it brings amazing results in a timely manner; however, it comes with increasing security and privacy concerns and issues. In this paper we will investigate, analyse, classify, and discuss the new security concerns and issues introduced by cloud computing. In addition, we present some security requirements that address and may alleviate these concerns and issues.

KEYWORDS

Cloud-based Business security issues and concerns; Cloud computing security issues and concerns. Cloud computing security requirements.

1. INTRODUCTION

Nowadays every company relies on digital data and services to operate their business. As the amount of data and software applications increase some businesses cannot afford to have them stored and installed on their local premises for various reasons starting from storing huge data and information to using expensive software applications and computing platforms. Businesses started using Cloud computing to take advantage of their many benefits like scalability, reliability, resource sharing, external data warehousing, and high performance and relatively low cost feasible solutions and services as compared to dedicated infrastructures. Cloud computing platform is a net of computing resources, including networks, servers, and applications. It is flourishing across enterprises today, serving as the IT infrastructure driving new digital businesses. It is persuasive for most businesses and an estimated 70% of all enterprises use the cloud for at least one application and its related data [1]. According to Public Cloud Market Research Report, the worldwide market for public cloud will accelerate at a compound annual growth rate of 22.78% during the projection period (2017-2023) [2]. In addition, the number of cloud service providers is growing at a rapid speed due to the increase in the rate of the businesses adopting this new platform to use their many technical and operation management benefits that it offers. As more and more businesses move towards digitization, they will adopt

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 341-352, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90929

one form or the other of the Cloud computing technology. According to a report published by Statista [3] on the current and planned usage of public cloud platform services running applications worldwide in 2018, 80% of enterprises are both running apps on or experimenting with Amazon Web Services. 67% of enterprises are running apps on (45%) and experimenting on (22%) the Microsoft Azure platform. 18% of enterprises are using Google's Cloud Platform for applications today, with 23% evaluating the platform for future use. [Figure 1]

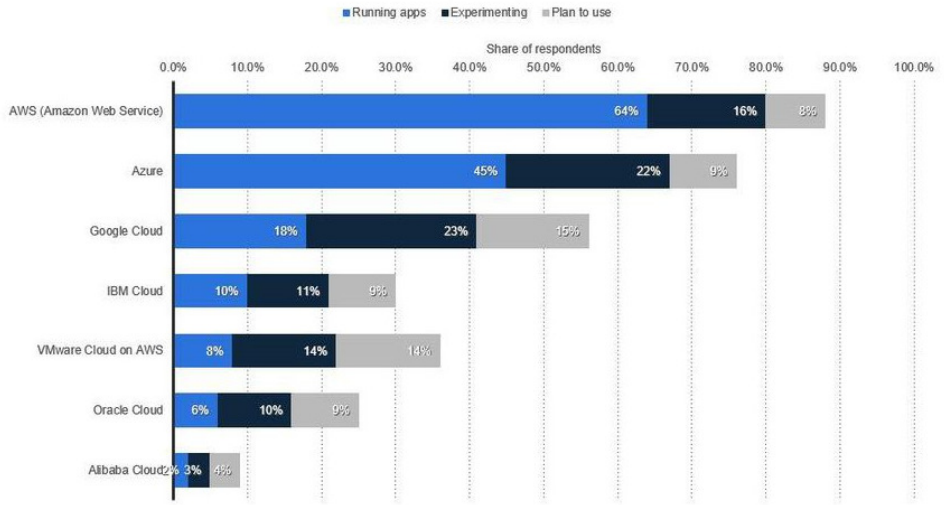

Figure 1: Current and planned usage of public cloud platform services running applications worldwide in 2018.

On the other hand, as security and privacy risks continue to increase globally, businesses cannot risk storing their critical data on remotely located servers that they do not have full control over it and could be subject to security attacks by malicious hackers [1]. Cases such as the Equifax data breach in the fall of 2017, from which the safety and privacy of more than 143 million individuals' data are compromised, have a major hit on the confidence of businesses and their customers in the new platform. Businesses can rarely afford such an enormous hit that badly affect their reputation, and hence, they should study carefully their choices and employ the best cloud security practices [4].

In addition to the general security issues like confidentiality, integrity, availability, legitimacy, and accountability that needs to be individually taken care of, new security issues and concerns are surfaced and need to be addressed properly before fully indulge in cloud computing platform/paradigm/services. Enterprises have to study and evaluate these issues to ensure the manageability and security system of the cloud provider before adopting Cloud computing technology for their businesses.

This paper provides a good presentation, discussion, and a strong overall coverage and classification of the new security issues and concerns of businesses arising from using the Cloud computing technology paradigm, and it gives a good summary of the available requirements and techniques used in handling the different types of security and concerns. The rest of the paper is organized as follows: In section II, we introduce the cloud computing architecture and the different consumption models. In section III, we present and classify the different business security issues and concerns related to cloud computing. In section IV, we discuss some of the main security requirements and measures that must be addressed or taken care of in order to

alleviate the different security issues and concerns. Finally, in section V, we present a conclusion of the paper.

2. CLOUD COMPUTING ARCHITECTURE

The general architecture of cloud computing is shown in Fig. 1 where users can access the cloud computing services using their digital devices through network providers and the internet. Cloud computing users use cloud services on the fly through the Internet and can choose between three different types of services, as explained in what follows, Platform as a Service (PaaS), Infrastructure as a Service (IaaS), or Software as a Service (SaaS).

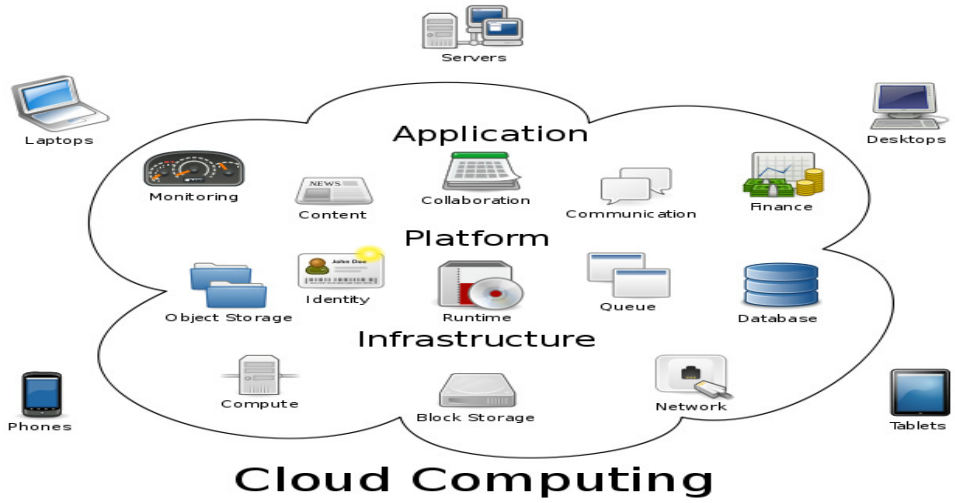

Figure 1: General Architecture of Cloud Computing

Users interact with cloud services provider using native mobile applications or embedded browser applications. Embedded browser applications are developed using standard web development languages (e.g. HTML and JavaScript). Native applications are developed using mobile platform supported programming languages and a set of APIs provided by the cloud services provider.

2.1. Cloud Computing Service Models

Based on the National Institute of Standards and Technology's (NIST) definition of the different cloud models [8], cloud computing services are generally classified into three delivery models, as shown in Figure 2 and Table 1: The Software as a Service (SaaS), the Platform as a Service (PaaS), and the Infrastructure as a Service (IaaS).

2.1.1. Software as a Service (SaaS)

SaaS offers comprehensive applications on demand. It consists of software running on the provider's cloud infrastructure, supplied to one or several clients on demand via a thin client over the Internet. It allows a software company to publish their software and let their users access the software via a web browser. Suite servers like Microsoft Office 365 or applications like Salesforce provide users with instant access to documents and files without the hassle of installing, managing, and storing applications and data on their personal devices.

Users and organizations utilize SaaS applications for additional computer space, added cloud security, ease of updating software, and the ability to synchronize data across many devices. SaaS applications help users avoid software ownership and costly, time-consuming updates and usually work on a monthly or annual subscription-based model. The provider controls and maintains the physical computer hardware, operating systems and software applications. Because of this, SaaS relieves the end users from the labor of software maintenance, continuing operation, and support. Most widely used examples of SaaS include Gmail, Google Docs, Microsoft Office 365, and Salesforce.com [9].

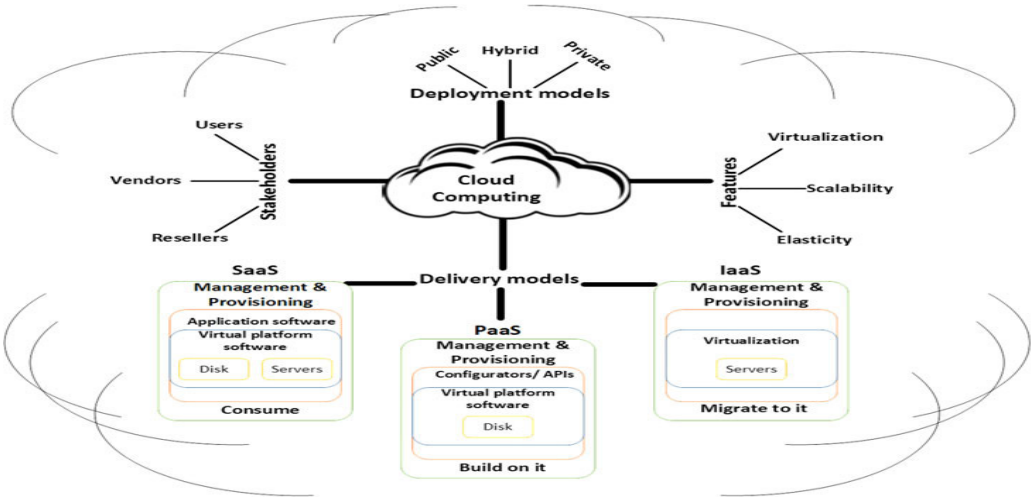

Figure 2: Service delivery models of cloud computing. [5]

2.1.2. Platform as a Service (PaaS)

PaaS provides the end users the platform that includes the operating system, the software development, the programming languages, and the testing tools needed to develop their own applications. It is the delivery of computing platform and solution stack as a service. Businesses can store their clients' data in the platform provider's cloud service, and they can use software, hardware, provided by Cloud computing services to develop, construct, test, and install their own suite of cloud-based apps/services on the Cloud without having to invest in expensive hardware, software licences/tools, operation maintenance, and connectivity. Some examples of PaaS providers include Microsoft Windows Azure, Google App Engine, and Amazon Web Services (AWS).

Table 1: Cloud Computing Service Models and Providers

Cloud Service Models	**Cloud Service Providers**
SaaS	Google Apps, Microsoft 365, IBM, Salesforce.com, and Rackspace.
PaaS	Amazon AWS, Google Apps, Microsoft Azure, SalesForce, Intuit, WorkXpress, and Joyent
IaaS	Amazon Elastic Compute Cloud, Rackspace, IBM, Savvis, VMware, Terremark, Citrix, Joyent, and BluePoint.

2.1.3. Infrastructure as a Service (IaaS)

IaaS offers end users direct access to processing, storage and other computing resources over the network. It is the delivery of computer infrastructure as a service which is sometimes referred to as utility computing. It provides virtual servers with unique IP addresses and chunks of storage on demand using pay-as-you-go method to allow users to pay a single monthly subscription fee based on how many gigabytes or megabytes of data they need to store. Businesses can install and run different software, and have control over operating systems, storage, and installed applications. IaaS is the most flexible cloud computing service that allow organizational users to customize their product combination and enable them to have the most control over their cloud infrastructure although the Cloud service provider owns the equipment and is responsible for housing, running and maintaining it. Some examples of IaaS include Amazon Elastic Compute Cloud (EC2), Joyent, Rackspace, and IBM Computing on Demand.

2.2. Cloud Computing Consumption Models

There are three basic cloud application deployment and consumption models or configurations: public, private, or hybrid clouds. Each offers complementary benefits, and has its own trade-offs [10, 11, 12]. It is very important for businesses to choose the appropriate cloud model based on their needs. This is very important and critical to the safety and security of the Business' operations. Some companies having enormous data so they prefer private clouds while small organizations usually use public clouds. A few companies like to go for a balanced approach with hybrid clouds. Before choosing a cloud model, businesses should be fully aware of the terms of use, service level agreement, and the security and privacy measures implemented in the Cloud model. In what follows, we will give a brief description of each cloud model.

2.2.1. Public Clouds

Public clouds are owned and managed by providers, and applications from different customers are likely to be mixed together on the cloud's servers, storage systems, and networks. However, this model has a variety of inherent security risks that need to be considered. A well architected private cloud properly managed by a provider provides many of the benefits of a public cloud, but with increased control over security. Public clouds are most often hosted away from customer premises, and they provide a way to reduce customer risk and cost by providing a flexible, even temporary extension to enterprise infrastructure.

2.2.2. Private Clouds

Private clouds are client dedicated and are built for the exclusive use of one client, providing the utmost control over data, security, and quality of service. The enterprise owns the infrastructure and has control over how applications are deployed on it. If the private cloud is properly implemented and operated, it has reduced potential security concerns. A managed private cloud may enable enterprise customers to more easily negotiate suitable contracts with the provider, instead of being forced to accept the generic contracts designed for the consumer mass market that are offered by some public cloud providers. Private clouds may be deployed in an enterprise datacenter, and they may be deployed at a co-location facility.

2.2.3. Hybrid Clouds

A Hybrid cloud involves a combination of both public and private cloud models. They can help to provide on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to maintain service levels in the face of rapid workload

fluctuations. Enterprise Computing and private cloud extend outward to consume public compute resource for peak need or deliver on Industry cloud. An example is using commodity resources from a public cloud such as web servers to display non-sensitive data, which interacts with sensitive data stored or processed in a private cloud. Focus primarily on proprietary data centers, but rely on public cloud resources to provide the computing and storage needed to protect against unexpected or infrequent increases in demand for computing resources.

3. CLOUD COMPUTING SECURITY CONCERNS

The Cloud computing platforms, like any other IT platforms, are vulnerable and subject to a variety of malicious attacks that may affect sensitive business data and applications. In addition, a cloud provider usually hosts numerous clients; each can be affected by actions taken against any one of them. When any threat came into the main server, it affects all the other clients also. Businesses should choose a cloud provider who can meet their security standards set by their company's internal policies and government agencies. They must carefully read the service level agreement and understand the provider's policies, terms, and security measures.
Security experts in the field of Cloud computing have identified several critical security issues and concerns. These include the following:

- Data breaches and loss.
- Incomplete data control.
- Inability to monitor data in motion.
- Denial of Service.
- Insecure Application Programming Interfaces.
- Vulnerable systems and applications.
- Host Access Management.
- Lack of consistent security controls over multi-cloud and on-premises environments.

In general, we can classify the Cloud computing security issues and concerns into four main classes as shown below in figure 3. In what follows, we will discuss each class in more details.

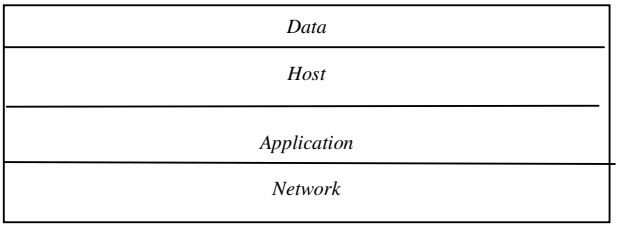

Figure 3: Different Classes of Cloud Computing Security issues and concerns.

3.1. Data Security

Most Cloud computing security issues and concerns are directly or indirectly related to data security. Whether a lack of visibility to data, inability to control data, or theft of data in the cloud, most issues come back to the data customers put in the cloud. Individuals and enterprises take advantage of the benefits for storing large amount of data on a cloud. However, by using Cloud computing businesses have concerns and fear of so many security issues related to data access control, integrity, protection, and data location [22]. Businesses count on cloud content management platforms from vendors such as Dropbox, Google, and Microsoft to access, store and share data and files within an enterprise repository. However, there are security concerns about this information falling into the wrong hands and be subject to phishing attacks and

malware. In what follows in this section, we will discuss the main security issues and concerns related to data in cloud computing.

3.1.1. Data Access Control and Authentication

Different authentication mechanisms have been presented and proposed using cloud computing to secure the data access suitable for cloud environments. Some uses the open standards and even supports the integration of various authentication methods. For example, the use of access or login IDs, passwords or PINS, authentication requests, etc. Sometimes confidential data can be illegally accessed due to lack of secured data access control. Sensitive data in a cloud computing environment emerge as major concern with regard to data security in cloud computing.

3.1.2. Data Integrity

Data integrity is essential in cloud computing. Every cloud user must ensure the integrity of their data stored on the cloud. Errors may occur when data is entered or transmitted from one computer to another. It could also occur because of some hardware malfunctions, such as disk crashes, software bugs or viruses. Every access a cloud user make must be authenticated and verified. Different approaches in preserving integrity for one's information that is stored on the cloud is being proposed. For example, every access a user make must be authenticated assuring that it is his/her own information and thus verifying its integrity.

3.1.3. Data Confidentiality and Protection

Cloud computing allows users to store their own information on remote servers, which means content such as user data, financial data, business data, videos etc., can be stored with a single cloud provider or multiple cloud providers. When users store their data in such servers, data confidentiality is a necessity. Storing of data in remote servers also arises some privacy and confidentiality issues among individual, business, government agency, etc., each customer data in the public cloud environment are exposed to internet. Cloud computing services should require reliable processes for protecting data before, during, and after any operation.

3.1.4. Data Theft

Cloud computing uses external data server for cost effective and operation flexibility. Therefore, there is a risk of data being stolen from the external server.

3.1.5. Data Loss

Data loss is a very serious concern in cloud computing since they are stored on premises that they have no control over. Customers may lose data as a result of a major server crashes, a hacker's attack on main and backup servers, or due to financial or legal problems with the service provider.

3.1.6. Data Location

Cloud computing customers do not always know the location of their data. The provider does not reveal where all the data are stored. In addition, cloud computing offers a high degree of data mobility, so data could be very far away from the location of the customer and could be on different servers in different countries [23]. In addition, location of data may have considerable effects on the privacy and confidentiality, on information protection, and on privacy obligations for those who process or store the data.

3.2. Host Security

Host security concerns are those which affect the host infrastructure when it is connecting itself to the cloud computing. They are directly related to virtualization vulnerabilities and weak access control in public cloud environment.

In the IaaS model, customers are primarily responsible for securing the host provisioned in cloud. They are accountable for security management of the guest VM. Cloud service provider recommends the customer to use SSH to manage the VM instances. The attacker may steals the SSH private keys that are used to access and manage virtual instances. This can be eliminated by storing the private keys on system in an encrypted form [13]. Other host security threats related to virtual machine security is attacking the vulnerable services like FTP and NetBIOS. It is recommended to run only the necessary services and turn off the unused services that are not required. Some more security threats like capture user accounts that are not properly protected with strong password, attack the systems that are not properly protected by host firewalls and deploy Trojans embedded in the VM software component or within the VM image itself. Cloud service provider must ensure that the strong operational security procedures are followed to secure the virtual machine from these threats.

In PaaS and SaaS models, cloud service providers do not share their host platform and the host operating system with their customers, therefore, host security responsibility is transferred to the cloud service provider. As a result of that, PaaS and SaaS customers should get the appropriate level of guarantee from the cloud service provider about their host security [13].

3.3. Application Security

In cloud computing platform, any application or software that is used does not reside on the machine of the actual user, and if this software/application has vulnerabilities then it can have a negative impact on the security of all the customers using the cloud. These vulnerabilities can lead to compromising security, and can affect the availability of cloud computing. Traditional security mechanisms such as network firewalls, network intrusion detection and prevention mechanisms do not adequately satisfy being used as a solution for application vulnerabilities [20, 21]. The typical security issues arising with applications technology are: Session riding, hijacking and injecting vulnerabilities. Other web application specific vulnerabilities are browser's front-end components in which, data sent from the user component to server component is manipulated. XML signature attacks, browser based attacks for cloud authentication are other examples of application vulnerabilities that can affect the cloud computing security. Application security is the main threat to SaaS platform.

3.4. Network Security

Network related security issues are considered to be the biggest security challenges in clouds since cloud computing is more prone to network related attacks compared to the traditional computing paradigms [14]. In addition, cloud computing are tightly coupled and highly depend on networking. The ratio of network attacks and fraud radically increases as people and organizations migrate their data into clouds. Security experts anticipate that clouds will be the focus of hackers in future due to the concentration of valuable data, application, and information within the clouds. Some of these security issues and concerns are the results of the following gaps: The possible lack of proper installations of network firewalls and the overlooked security configurations within clouds and on networks make it easier for hackers to access the cloud on behalf of legitimate users. Hackers can run malicious code to control hardware and software

resources. Internet access problems due to some kind of attacks make Cloud computing services unavailable. Therefore all the network reliability issues will have direct implication on the cloud computing. Other more specific security issues that are network-related and may affect directly the access control restrictions of cloud resources include the following:

3.4.1. Denial of Service Attacks

Most of the serious attacks in cloud computing come from denial of service (DoS), particularly HTTP, XML and Representational State Transfer (REST)-based DoS attacks. The cloud users initiate requests in XML, then send requests over HTTP protocol and usually build their system-interface through REST protocols such as those used in Microsoft Azure and Amazon EC2. Due to weaknesses in the system interface, DoS attacks are easier to implement and very difficult for security experts to countermeasure [15]. XML-based distributed denial of service (DDoS) and HTTP-based DDoS attacks are more destructive than traditional DDoS because these protocols are widely used in cloud computing with no strong deterrence mechanisms available to avoid them. HTTP and XML are critical and important elements of cloud computing, so security over these protocols becomes critical to providing safe and secure cloud computing model.

3.4.2. Issue with Reused IP Addresses

With respect to cloud provider the IP address is the billable entity. It will be reassigned and reused by new user when the existing users no more using that IP address. From the customer perspective it can pose the security risk to their resource access by some other user due to the time delay between the change of an IP address in DNS and clearing that address in DNS cache. The similar time delay may occur for changing physical address in ARP tables and clearing that address from an ARP cache. With the impact of this issue, the Amazon web services a leading cloud provider has announced the elastic IP address, by which the customers are assigned with a set of routable IP address and they have control over that IP address until they release it. [16] However, the issue can persist in non-routable IP addresses where the customers can reach the provider's network via the private address. [17]

3.4.3. Limited Auditing Capability

A business using a public cloud irrespective of any type of service models face the significant risk in their data. They have limited ability to access the network-level logs and audit the cloud provider operations [18].

3.4.4. Attack Against SSL\TLS

Secure Socket Layer and Transport Layer security is the protocol used to create an encrypted channel to provide communication over the public cloud. Many cloud providers support this protocol to provide secure communication. Authors in [19] presented a new attack by which the hackers are able to break the SSL encryption in millions of websites. This attack named as BEAST (Browser Exploit Against SSL\TLS). This suggests that even HTTPS cookies are no longer secure of this template.

4. DISCUSSION

For a wider adaptation of cloud computing services by businesses, the security issues and concerns need to be addressed more seriously at various levels. When you do not own the network, it is open to the rest of the world, and you do not control the security layers of the cloud infrastructure, the cloud computing will not be as secure as storing data and applications on your

own premises. Hence providing the suitable security measures that overcome the security risks in cloud computing are necessary when a business is transferring to cloud. Moreover, not every business has sufficient knowledge about the implementation of the cloud solutions, and not every business has the expert staff and the right tools to use the cloud computing in a proper and safe way. Businesses should be aware of the threats, and risks involved in using public cloud environments when considering outsourcing data, applications and infrastructure to a Cloud computing platform in general and to a public cloud in particular. For businesses to protect their data on the cloud, they should inspect and study their cloud provider's security measures, and their terms of use and conditions in case hacking and breaching incidents occur. In addition, they should train their employees on the different processes and tools of cloud computing, and they should be able to verify the integrity and safety of their data and information before and after being stored on cloud resources. In addition, they should be able to determine who can enter data into the cloud, track transactions and operations to identify abnormal behaviors, secure and strengthen network traffic analysis tools. All of the above are rapidly becoming standard measures in protecting utilizations of cloud computing infrastructure. [6]

In general, businesses should follow some guidelines in order address and alleviate the main security issues and concerns in cloud computing. These guidelines include the following: Understanding the different Cloud computing platforms and the type of services offered by the cloud provider, making sure that the selected Cloud computing solution fulfill their security requirements, and maintaining responsibility and accountability over the security of data and applications implemented and deployed on the Cloud.

5. CONCLUSIONS

Cloud computing is a new concept for most businesses and it is very difficult for them to verify that Cloud providers meet the security requirements standards to address security threats and concerns. Hence, every business should treat security issues and concerns very seriously. A lot of research works have been done related to cloud computing security issues that have resulted in several security methods and measures that can be used to alleviate the security risks in cloud computing. Many researchers and practitioners worked and are working on identifying cloud threats, vulnerabilities, attacks, and other security issues, in addition to proposing countermeasures in the form of frameworks, strategies, service oriented architectures, and recommendations [28, 30, 31]. However, providing a comprehensive security framework intended to support all types and levels of security issues and concerns is not available yet.

In this paper, we have introduced and presented the cloud computing architecture and the different consumption models, in general, and we have presented, discussed, and classified the different security issues and concerns that businesses should be aware of when using Cloud computing. Furthermore, we have presented and discussed the different measures and requirements that can be put in place to address the major security risks. The paper can be considered as a very good starting reference for those researcher that are planning to work on security issues in cloud computing and for businesses planning to enter to the world of Cloud computing.

REFERENCES

[1] The 2018 Cloud Security Guide: Platforms, Threats, and Solutions. Cloud security is a pivotal concern for any modern business. Learn how the cloud works and the biggest threats to your cloud software and network, July 31, 2018. https://www.secureworks.com/blog/cloud-security-guide-to-platforms-threats-solutions.

[2] Public Cloud Market 2018: Global Size, Share, Growth Opportunities, Emerging Trends, Sales Revenue, Key Players Analysis, Future Prospects and Regional Forecast to 2023. Oct 24, 2018. https://www.marketwatch.com/press-release/public-cloud-market-2018-global-size-share-growth-opportunities-emerging-trends-sales-revenue-key-players-analysis-future-prospects-and-regional-forecast-to-2023-2018-10-24

[3] Statista, Current and planned usage of public cloud platform services running applications worldwide in 2018. https://www.statista.com/statistics/511467/worldwide-survey-public-coud-services-running-application/

[4] Sara Ashley O'Brien, Giant Equifax data breach: 143 million people could be affected. September 8, 2017. https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html

[5] Iqbal, S et al. Service delivery models of cloud computing: security issues and open challenges. Security and Communication Networks 2016; 9:4726–4750. 30 August 2016.

[6] Cloud Computing Security Issues and Solutions. https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/security-issues-in-cloud-computing.html.

[7] ReportsnReports, http://www.kuam.com/story/26655451/pricing-the-cloud-2014-market-research-report-with-2019-cloud-computing-pricing-and-revenue-forecastsDALLAS, September 29, 2014.

[8] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", NIST Special Publication 800-144, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494, Dec. 2011.

[9] R. D. Caytiles and S. Lee, Security Considerations for Public Mobile Cloud Computing, International Journal of Advanced Science and Technology, Vol. 44, July 2012.

[10] NEC Company, Ltd. and Information and Privacy Commissioner, Ontario, Canada. "Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach, http://www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf, 2010.

[11] https://wiki.cloudsecurityalliance.org/guidance/index.php/Cloud_Computing_Architectural_Framework.

[12] H. T. Dinh, C. Lee, D. Niyato and P. Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches", Wireless Communications and Mobile Computing – Wiley, Available at http://www.eecis.udel.edu/~cshen/859/papers/survey_MCC.pdf.

[13] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)," O'Reilly Media, Sep. 2009; ISBN: 9780596802769.http://oreilly.com/catalog/9780596802776.

[14] I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud Computing Security: A Survey", computers journal, www.mdpi.com/journal/computers, ISSN 2073-431X, Feb 3, 2014.

[15] Karnwal, T.; Sivakumar, T.; Aghila, G. A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In Proceedings of the 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 1–2; pp. 1–5, March 2012.

[16] Announcing Elastic IP addresses and Availability Zones for Amazon EC2," http://aws.amazon.com/about-aws/whatsnew/2008/03/26/announcing-elastic-ipaddresses-and-availability-zones-for-amazonec2/

[17] RFC1918, "Address Allocation for private Internets," http://tools.ietf.org/html/rfc1918

[18] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Edition on Risks and Compliance (Theory in Practice)," O'Reilly Media; ISBN: 9780596802769, Sep. 2009.

[19] "Hackers break SSL encryption used by millions of sites," http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/

[20] Danny Harnik, Elliot K. Kolodner, Shahar Ronen, Julian Satran, Alexandra Shulman-Peleg, and Sivan Tal. Secure access mechanism for cloud storage. Scalable Computing: Practice and Experience, 12(3), 2011.

[21] B. Hay, K. Nance, and M. Bishop. Storm clouds rising: Security challenges for IaaS cloud computing. In 2011 44th Hawaii International Conference on System Sciences (HICSS), pages 1-7. IEEE, January 2011.

[22] Serrao, G.J., "Network access control (NAC): An open source analysis of architectures and requirements", IEEE International Carnahan Conference on Security Technology (ICCST), pp 94 - 102 , San Jose, CA, USA, Oct. 5-8, 2010.

[23] Anitha Y, "Security Issues in Cloud Computing - A Review", International Journal of Thesis Projects and Dissertations (IJTPD), Vol. 1, Issue 1, PP: (1-6), Month: October-December 2013.

[24] Tim Mather, Subra Kumaraswamy, and Shahed Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, October 2009

[25] Zhang Yandong and Zhang Yongsheng. Cloud computing and cloud security challenges. In Information Technology in Medicine and Education (ITME), 2012 International Symposium on, volume 2, pages 1084-1088.

[26] Syed Mujib Rahaman and Mohammad Farhatullah. PccP: a model for preserving cloud computing privacy. In Data Science & Engineering (ICDSE), 2012 International Conference on, pages 16-170, 2012.

[27] G. Kulkarni, J. Gambhir, T. Patil, and A. Dongare. A security aspects in cloud computing. In 2012 IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS), pages 547-550, June 2012.

[28] Wang, C.; Wang, Q.; Ren, K.; Lou, W. Towards secure and dependable storage services in cloud computing. *IEEE Trans. Serv. Comput.* 2012, *5*, 220–232.

[29] J R Jiang, J P Sheu, C Tu, J W Wu, " A secure anonymous routing protocol for wireless sensor networks", IEEE Journal of Information Science and Engineering, Vol. 680, Issue 2, 2010, Pages: 657-680.

[30] Sabahi, F. Virtualization-level security in cloud computing. In Proceedings of the 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), Xi'an, China, 27–29 May 2011; pp. 250–254.

AUTHOR

Prof. Mohamad Al Ladan has over 19 years of teaching and training experience in the area of computer hardware & software and Information Technology. He received the M.Sc. and the Ph.D. degrees in Computer Engineering from Syracuse University, Syracuse, N.Y., USA, in 1990 and 1995 respectively. He is a reviewer for different international conferences and journals. He is currently a full professor of computer science and the Dean of the College of Sciences and Information Systems at Rafik Hariri University in Lebanon.