EasyChair Preprint

№ 9372

Security Framework for Hosting Systems on the Cloud: Case Study of Jordan E-Government Websites

Asma Salem and Rizik Al-Sayyed

November 26, 2022

Security Framework for Hosting Systems on the Cloud: Case Study of Jordan E-Government Websites

Asma Salem
King Abdullah II School of Information Technology
The University of Jordan, Amman – Jordan
Dr_asmasalem@yahoo.com

Rizik Al-Sayyed
King Abdullah II School of Information Technology
The University of Jordan, Amman – Jordan
r.alsayyed@ju.edu.jo

Abstract— Nowadays database systems become more and more critical in every domain of our lives. Websites are becoming more dynamics, they being more than browsing content and pages through internet. They are being more interactive and keep users comfort as they can read, browse, send and receive critical information through their interfaces. Recently websites are being hosted in larger datacenters owned by large hosting companies. Most technologies trends move towards Cloud computing technologies that leads them for global datacenters rather that local ones. Even though this technology will provide a lot of services, there are many concerns related for securing and maintaining the cloud environments safe. Many techniques are being done to handle these issues in the literature but they are provided separately; they are not dedicated for specific applications and targeted issues. Hosting websites in secure datacenter is a major concept. There are many layers should be introduced to provide access to secure websites and applications published on the internet. In this paper we introduce complete framework to host a dynamic website on cloud datacenters, to emphasis the security requirements for hosting secure websites and database services. We have analyzed the attacks targeting the hosting services and find that the application and network levels have a significant part in the security framework design. Also, best practices and recommendations were also provided.

Keywords— security; hosting; website; webserver; cloud; virtual

1. INTRODUCTION

Nowadays security is the main concern of the system's requirements when designing or publishing any website accessible through internet. While the security requirements may be affecting the accessibility, availability and performance of the website, many software engineering techniques and methodologies could be implemented successfully to improve the security of the website. Sometimes the translation of these requirements of security may fail to fulfill the desired goal. Furthermore, developers don't consider all security checklists as an important issue, however they tend to integrate concepts such as reliability and performance; but they fail to apply full security requirements when designing websites. These websites could be hosted on local datacenter or being hosted on the cloud [1-4].

Nowadays cloud computing provides the internet based services and having an option for renting of computing and storage infrastructure services; for building remote platforms; customization of business processes and applications. This new technique integrates, optimizes and supplies computing ability, giving the ability for planning and simplifying the clients computing jobs by the mean of renting resources and services [1-3].

Websites are consisting of web pages, HTML, JavaScript, and many other components such as images, video and other files to the website [1,2]. They are designed and developed with many designing and developing tools not limited with ASP.NET, PHP, etc. These websites needed to be hosted on servers which should be published through internet. These servers are commonly owned by hosting companies, who are offering the hosting services to their customers. These companies are well prepared with highly equipped datacenters, which being built on higher standard and should be well prepared and hosted in secure infrastructure [3,4].

Hosting services are provided by hosting companies; these services could be host websites, webservers, or systems hosted on cabinets belonging to clients. Online security is an important issue, when customers signed the contract to host their websites; they are relying on the hosting company to control the security of website [3-5]. On the other hand, security requirements are not implemented correctly on hosting companies; where the source code and website contents are existing. Sometimes security requirements are difficult to understand by non-security experts. From the viewpoint of the traditional security techniques, integrating security with system requirements would result in a situation that the security is considered as part of the development process, from other point of view they could be considered in the implementation process; while the complete framework is to consider the security as a continues process lasting forever in the website hosting services life cycle [6,10].

In this paper we are discussing the hosting websites life cycle. The security requirements should be implemented to improve the website security when moving hosting towards cloud. These security requirements should be taken in consideration in balanced way to keep the security from one side, and to

improve the performance from another side. The rest of paper is organized as follow: section two will cover the related work. Section 3 covers the hosting services on the cloud. Section 4 covers the cloud computing security. Section 5 covers cloud computing threats. And the final section provides our conclusions.

2. BACKGROUND

The accepted concept of Cloud Computing announced by the nation's Institute of Standards and Technology (NIST) as follow [3-6]. "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared Pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that Can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployments models" [5][6].

A web hosting service is an Internet based service that allows clients and organizations to rent or own place to host webserver/website on, and make the service published on the internet [11-13]. Website hosting began with finding suitable company having the capability to provide the required criteria of hosting website on space, providing internet connectivity in secure manner; this should meet the client or company needs [11]. Hosting services could be offered in specific offers and controlled by some contact rules signed between the hosting company and the client [10-14]. The hosting starts usually by delivering the website contents from the customer to the hosting company. Multiple security check phases should be taken to ensure that the website content is safe and secure to be published through the internet. These procedures are being done in all public and governmental institutions. We have shared the common procedure done in Jordan for governmental websites [12, 13, 24].

These steps are the user procedure used for hosting the website form user perspectives; it is usually started after delivery of the website content to the datacenter administrator. The system team and Domain Name System (DNS) are negotiating to use temporary URL used to publish the website on test domain. This step is essential to test the new hosting website environment and let the security team do their security check procedures. Usually the security team return with a report containing a full security vulnerabilities and threats. This report is directed to the customer development team to reconfigure the website according to the hosting security requirements. And the cycle will carry out again until the website is ready to be published on the real domain and being accessible through internet [3, 6, 24].

From system point of view, more and more analysis and security requirements are checked before proceeding in hosting services websites. Multiple issued should be taken in considerations to host a website in physical datacenters or cloud. These issues are classified upon multiple criteria in the following classifications [11-20]:

A) Websites types:

Website contents are consisting of pages, images, videos and many other media types. This website contents divided into two types: static or dynamic contents: -

Simple (static) Website Hosting: These types of websites are very low cost, with simple design and few pages, the website could be easily developed and published in any datacenter. Websites that do not contain any complex configuration or server-side scripting. Usually clients with minimum efforts manage infrastructure and do the administration of their static websites. [14, 15].

Enterprise (Dynamic) Web Hosting: These enterprise websites need a maximum effort for managing infrastructure and administration for the resources. They are dynamically scale resources, with highly availability and performance metrics to support the most demanding services. They are providing multiple services, split usually on multiple servers on one data center or among multiple datacenters. They are built on high levels standards of availability, scalability, security and performance. These websites are requiring sustained high resources on servers such as CPU, RAM, network, and storage space [15-18].

B) Hosting server's nature (standalone vs shared):

Hosting website environment: this type could be classified based on the website type, which could be single website hosted on a standalone infrastructure or shared web hosting service [11-13].

A standalone website: Complex infrastructure and advances pre-installed tools are required to provide complex site hosting. These websites could be hosted on multiple servers such as front end (application server) and backend servers (database, reporting or backup servers) or single server dedicated for all hosting requirements. In this type of hosting only website can benefit from all tools and roles installed on the server. This type of hosting is highly cost and customized to meet the customers with special needs which are dynamic and complex in their configurations [11-13].

Shared web hosting service: Websites here sharing the same environment resources and tools. All websites on the shared pool will use the same server resources, such as RAM, network, and the CPU. This type of hosting is less cost and more suitable for static websites [11-14].

C) Hosting service architecture:

Single Point of failure hosting: having very simple architecture for hosting services. The datacenters cabinets are consisting of single point of failure servers; no redundancy in the components are exist in this architecture [11,12].

Clustered hosting: having multiple servers hosting the same content of websites or systems. This hosting exists for improving resource utilization and performance. They are providing a high-availability hosting service. A cluster may separate web serving from database hosting servers; this will provide the website hosting capabilities [19-20].

Grid hosting: This type is well-known in distributed hosting services, when a server cluster acts like a grid and is consisted of multiple nodes. This architecture is used for larger infrastructure services which are huge and complex [18-19].

D) Hosting server's nature (Physical vs virtual server):

This type depends on the server infrastructure and technology used to prepare the server; if it is physical server or virtual server [15-19].

Physical Dedicated hosting service: the clients get a full control on the web server and gains full access over it. The user has full administrative access to the server, which means the client is responsible for the updates, fixes and the security issues for management and maintenance of the dedicated server [17,19].

Virtual Dedicated Server: this type of servers divides server resources into virtual isolated slots, where resources can be allocated in a way that does not directly reflect changes on the underlying hardware. Also, clients are sometimes responsible for patching, updating and maintaining the server or the provider may provide server admin tasks for the hosting administrators [19-21].

Cloud hosting: this type of hosting provides customers scalable and reliable hosting capabilities based on clustered load-balanced servers (sometimes called pay as you go). You shouldn't own or rent a server rather than you can own or rent a service, hosting as a service raised here. As cloud servers dedicated for hosting are decentralized on diversity datacenters. From another side, the lack of centralization may give clients less control on their data, which could be an issue for users with data security and privacy [7-10].

3. CLOUD THREATS AND SECURITY

Cloud computing provides three delivery models by which different types of services are delivered to the end user. The three delivery models are the Infrastructure as A Service (IaaS), Platform as A service (PaaS), and Software as a service (SaaS), which provide infrastructure resources, application platform and software as services to the consumer. These service models also place a different level of security requirement in the cloud environment [21,22].

In cloud computing environment as capabilities are inherited, so are the information security issues and risks are also inherited and applied in layers. The dependency of each layer on the just above or below layer is so high. The roles separation and managements are the more important and most complex part in cloud computing managements [7-10].

The hosting environment either local datacenters or cloud servers are accessed with different perspectives; administrators, users, and webmasters are the actors interacting with hosted systems at any given point of time, each of them needs to have different access levels with different permissions [14,16, 23]. The cloud hosting environment could be consisted of the well-defined layers. These layers are helping us for creating forming a framework of security checklist we will introduce in this paper. Table (1) described the security levels spanned on multiple layers.

Table (1): Framework Security levels

Level	Description
Level-1 Datacenter Security (Physical)	This security aware about physical part such as surveillance cameras, biometric locks, doors locks for datacenter access, security equipment, processes and operations [1-7].
Level-2 Network Security	Any equipment provide the security on the network level, firewalls (providing protection for the network internal and external sides, they are the best first line of defense.), Intrusion Detection systems (IDS) and other equipment provides the protection on the network level from Denial of Service attacks (DOS) [17-20]
Level-3 Host Security	Hardware standardized with highly and latest updates and configurations. These standards are the vendor's responsibilities, Such as deploying Host Based Intrusion Detection (HBID) System. HBID on top of

	application layer, host firewalls also included, they are monitoring and analyzing the internals of a computing system [18-20].
Level-4 Platform Security	This level is an OS dependent level, which Operating Systems(OS) run on the servers such as Unix, Windows, and many others OS. Also, the server Software includes versions such as Apache, IIS, and Tomcat [11-15]. Application updates, bugs and fixes also included [17-20].
Level-5 Application Security	Any programming code and developed software are included here, any third party Products [11-16]. This allows hosting companies being completely control all variables involved in any particular Product [17-20] [24].

4. Design Security Framework for the Cloud Environment and Evaluation

The Ministry of Digital Economy & Entrepreneurship (MoDEE) is a governmental center that responsible for the hosting services of all government websites and services. It is hosted a private cloud computing environment and virtualization technologies. The cloud computing environment was established and implemented by Microsoft Company using Hyper Visor platform; while the virtualization environment was established and implemented by VMware-VMM platform. The government websites and database systems and government services are hosted in MoDEE datacenter. These systems and websites are hosted under three main categories of the cloud (Saas, IaaS, and Paas) [24-27].

To keep the services highly available, accessible, and secure; multiple practices and procedures are being done. Starting from replicating data between primary and replica sites. Replication process will have designed to keep the data in to two sites consistent and synchronized. The Replica site is good example for keep services up and running securely and highly available when any attacks on the services or network were being happened [24,27]. MoDEE also hosting services on virtualization environment, many of these services are hosted on SaaS service model. We have analyzed the security reports for the hosting services for six months based on the ticketing system used in the e-government datacenter (in the period of time between March 2018 and August 2018). We have classified **119** closed tickets with different severity and description; these tickets were in different five main levels; Applications, Networks, Host, Platforms and datacenter. The applications level consisted of many attacks targeting the application layer in the hosted websites, such as unauthorized access, SQL injection, cross-site-scripting and unauthorized upload/download. The Network level also was subjected to many dangerous attacks, such as DOS attacks, DDOS attacks and network traffic analysis. The host layer was also subjected for worms/viruses and zero day attacks, the majority of these attacks were being come from late updates for services and antiviruses software. Other level was the Platform attacks which were targeting specific operating system such as Microsoft or Linux operating systems environment [28-30]. The major security attacks were described in details table 2 for these details.

Table (2): Hosting Service Models Attacks

Security level	# Number Of Attacks	Percentage %
Applications	57	48%
Networks	38	32%
Hosts	20	17%
Platforms	4	3%
Datacenter	0	0%
Total	119	100 %

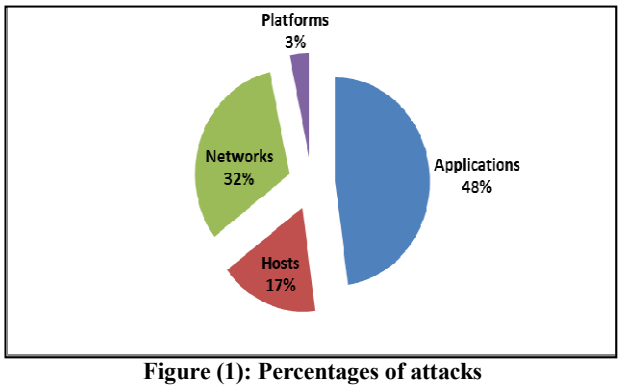

Figure (1): Percentages of attacks

Figure 1 summed up the results. We noticed that the majority of attacks are coming from the Application level side with significant fractions of total attacks with 48%. The Network attacks coming after with significant effect 32%. The Host attacks also are relatively high impact with 17%. The platform attacks were only 3% which is relatively low impact. The physical datacenter and attacks are relatively low impact with zero values. Because many security techniques and procedures are easily to be installed and applied in the physical security level, where the other parts are more important and are difficult to cope with. These results are showing us that more and more work and techniques still needed to apply

and take inconsideration's when any entity would publish their services or host them on the cloud environment. In government datacenter, following practical solutions is away to increase the Security levels in all layered models. We have summed up the majority of technical procedures that should be taken inconsideration when any entity plans to join the cloud with any type of service model. See table (3). We have already installed and operate all these security solutions in the designed framework to keep these services up and running in highly performance and with highly secure manner [30-34].

Table (3): Cloud computing security levels, attacks and countermeasures [30-35]

Security level	Cloud model	Attacks	Countermeasures
Datacenter	IaaS	1.Physical attacks 2. Stolen equipment 3.Unauthorized access	surveillance cameras, biometric door locks, authorization-based access policies, security equipment's
Network	IaaS PaaS	1.DOS and DDOS attacks 3. targeted attacks, 4. traffic anomalies, 5. unknown worms, 6. spyware/adware, 7. network viruses, 8. rogue applications 9. zero-day exploits	DDOS protection system Firewall Protection Network Intrusion Detection
Host	PaaS IaaS	1. Hardware attacks 2. Unauthorized access 3. Viruses/Worms/Bugs	Hardware standard Intrusion Detections
Platform	PaaS	1.Bugs, 2.late fixes, 3. late updates	Periodic Scans OS updates, patches, bugs fixes
Application	SaaS	1. Unauthorized access 2. SQL injection 3. Cross-Site-Scripting	Permissions and roles

5. CONCLUSIONS

Cloud Computing will be the next generation architecture of IT Enterprise. Although it has revolutionized the computing world, it is mainly suffering from many security threats varying from physical level threats to software level threats. In order to keep the Cloud secure, these security threats need to be managed to be always under the control. The most critical part of sensitive information residing in the cloud is also subjected to a number of threats and various issues; this information should be safe and secure [10,15].

In addition, cloud services providers nowadays are searching for multiple patterns that could be provided to their customers to overcome these threats. Finally, Security as a service (SecAAS) very soon is appeared on the surface as the forth service model which is now a hot topic in this era [29,35]. We have provided a simple weighted framework for security pattern selections; one case study was provided to illustrate the proposed framework we have suggested for the hosting on cloud computing solution. Websites are becoming more dynamics, they being more than browsing content and pages through internet. They are more interactive and keep users comfort as they can read, browse, send and receive critical information through their interfaces. In this paper we introduce complete framework to host a dynamic website on cloud datacenters, to emphasis the security requirements for hosting secure websites and database services.

From the e-gov experience, we have analyzed the attacks targeting the e-gov datacenters. We noticed that the majority of attacks are coming from the Application level side with significant fractions of total attacks with 48%. The Network attacks coming after with significant effect 32%. The Host attacks also are relatively high impact with 17%. The platform attacks were only 3% which is relatively low impact, and then come the physical level which was zero fractions from total attacks. These results are showing us that more and more work and techniques still needed to apply and take inconsideration's when any entity would publish their services or host websites, database systems on the cloud environment.

6. REFERENCES

[1] 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), pp. 1-11.

[2] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information sciences, 305, pp. 357-383.

[3] Ouda, A. J., Yousif, A. N., Hasan, A. S., Ibrahim, H. M., & Shyaa, M. A. (2022). The impact of cloud computing on network security and the risk for organization behaviors. Webology, 19(1), pp.195-206.

[4] Jansen, Wayne, and Timothy Grance. (2011. "Guidelines on security and privacy in public cloud computing." NIST special publication, pp. 144.

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

[6] Jin, H., Ibrahim, S., Bell, T., Gao, W., Huang, D., & Wu, S. (2010). Cloud types and services. In Handbook of Cloud Computing, pp. 335-355. Springer.

[7] Shaikh, A. H., & Meshram, B. B. (2021). Security issues in cloud computing. In Intelligent Computing and Networking, pp. 63-77. Springer, Singapore.

[8] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of internet services and applications, 1(1), pp. 7-18.
[9] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation computer systems, 25(6), pp. 599-616.
[10] Berger, S., Cáceres, R., Pendarakis, D., Sailer, R., Valdez, E., Perez, R., ... & Srinivasan, D. (2008). TVDc: managing security in the trusted virtual datacenter. ACM SIGOPS Operating Systems Review, 42(1), pp. 40-47.
[11] Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. Decision support systems, 51(1), pp. 176-189.
[12] Buyya, R., Yeo, C. S., & Venugopal, S. (2008, September). Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In High Performance Computing and Communications, 2008. 10th IEEE International Conference, pp. 5-13. IEEE.
[13] Al Nafea, R., & Almaiah, M. A. (2021, July). Cyber security threats in cloud: Literature review. In 2021 International Conference on Information Technology (ICIT), pp. 779-786. IEEE.
[14] Sharma, A., Singh, U. K., Upreti, K., & Yadav, D. S. (2021, October). An investigation of security risk & taxonomy of Cloud Computing environment. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), pp. 1056-1063. IEEE.
[15] So, K. (2011). Cloud computing security issues and challenges. International Journal of Computer Networks, 3(5), pp. 247-55.
[16] Molnar, D., & Schechter, S. E. (2010, June). Self-Hosting vs. Cloud Hosting: Accounting for the Security Impact of Hosting in the Cloud. In WEIS.
[17] 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), pp.1-11.
[18] Sengupta, S., Kaulgud, V., & Sharma, V. S. (2011, July). Cloud computing security--trends and research directions. In Services (SERVICES), 2011 IEEE World Congress, pp. 524-531. IEEE.
[19] Greenberg, A., Hamilton, J., Maltz, D. A., & Patel, P. (2008). The cost of a cloud: research problems in data center networks. ACM SIGCOMM computer communication review, 39(1), pp. 68-73.
[20] Strauch, S., Kopp, O., Leymann, F., & Unger, T. (2011, December). A taxonomy for cloud data hosting solutions. In Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference, pp. 577-584. IEEE.
[21] Nazir, M., Bhardwaj, N., Chawda, R. K., & Mishra, R. G. (2015). Cloud computing: Current research challenges. Book chapter of cloud computing: Reviews, surveys, tools, techniques and applications-an open-access eBook published by HCTL.
[22] Reznor, T. (2022, October 17), A Guide to Web Hosting Security Issues and Prevention, Retrieved from http://www.instantshift.com/2011/02/11/a-guide-to-web-hosting-security-issues-and-prevention/
[23] Razaque, A., Frej, M. B. H., Alotaibi, B., & Alotaibi, M. (2021). Privacy Preservation Models for Third-Party Auditor over Cloud Computing: A Survey. Electronics, 10(21), 2721.
[24] The Ministry of Digital Economy & Entrepreneurship (MoDEE),(2018,October),Retrieved_from_https://modee.gov.jo/En/Pages/eGovernment_Program.
[25] Schouten, E. (2022, October 15), Design patterns for the cloud, Retrieved_from https://www.ibm.com/blogs/cloud-computing/2012/11/26/design-patterns-for-the-cloud/
[26] El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering, 29(1), pp. 223-246.
[27] Müller, S. (2017). Security trade-offs in Cloud storage systems. Technische Universitaet Berlin (Germany) ProQuest Dissertations Publishing, 2017. DOI:10.14279/depositonce-6179.
[28] VMware. (2022, October 14), Virtual Appliances: A New Paradigm for Software Delivery, Retrieved from https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vam/vmware-virtual-appliance-solutions-white-paper.pdf
[29] Achar, S. (2022). Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. International Journal of Computer and Systems Engineering, 16(9), pp. 379-384.
[30] VMware. (2022, October 15), VMware Virtual Appliance Solutions,Retrieved_from https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vam/vmware-virtual-appliance-solutions-datasheet.pdf
[31] Furht, B. (2010). Cloud computing fundamentals. In Handbook of cloud computing, pp. 3-19. Springer, Boston, MA.
[32] VMware. (2018, October 27), VMware® AlwaysOn Desktop™ VALIDATED DESIGN GUIDE, Retrieved from_ http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.269.2530&rep=rep1&type=pdf
[33] Sasubilli, M. K., & Venkateswarlu, R. (2021). Cloud computing security challenges, threats and vulnerabilities. In 2021 6th International Conference on Inventive Computation Technologies (ICICT), pp. 476-480. IEEE.
[34] Dastjerdi, A. V., Tabatabaei, S. G. H., & Buyya, R. (2010, May). An effective architecture for automated appliance management system applying ontology-based cloud discovery. In Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, pp. 104-112. IEEE Computer Society.
[35] AlMendah, O. M., & Alzahrani, S. M. (2021). Cloud and edge computing security challenges, demands, known threats, and vulnerabilities. Academic Journal of Research and Scientific Publishing, 2(21), pp.156-175.