Security Analysis of the Workload Distribution and Resource Pooling Architecture in Cloud Systems

Mubarak Banisakher
Mubarak.banisakher@saintleo.edu

Derek Mohammed
derek.mohammed@saintleo.edu

James Simeon
james.simeon@saintleo.edu

Department of Computer Science
Saint Leo University, FL. USA

***Abstract* - Many companies are making the move to a cloud-based environment for data storage and management. Having their data in the cloud has many benefits in that it may help the company move forward and innovate. The embracing of cloud-based services by corporates, businesses, and people, has helped to usher in a paradigm shift in the people-data-service relationship. While most steps in the evolution of technology center around "development" and "productivity", given the changing scenario of threats and cybercrime, security in the cloud needs to be thoroughly analyzed, researched, and mitigated, even if it cannot be completely eliminated or avoided. However, cloud-based environments are not completely safe from attacks. Criminals are always looking for ways to make money through malicious activity. Cyber Security is already one of the fastest growing fields in the modern world and the number of incidents that occur on a daily basis are continuing evidence of its necessity. Systems security of all types have been addressed in similar ways but cloud-base environments offer quite a few unique threats that force professionals to become creative when preparing mitigation techniques. This paper introduce a cloud computing security analysis survey where we list out some of the grave security threats that the Workload Distribution and Resource Pooling Architecture in Cloud Systems model faces, and some mitigation techniques to encounter them.**

Keywords: security, cloud, workload, pooling, resources, network, threat, systems

I. INTRODUCTION

Cloud computing technology has become increasingly popular in the past years and continues to grow in usage, especially in the business environment. This is for good reason, as cloud computing provides many benefits for cloud consumers. These benefits are characteristic of most cloud computing models.

These characteristics include on-demand usage, ubiquitous access, multitenancy/resource pooling, elasticity, measured usage, and resiliency [3] It is these characteristics that make cloud computing so popular. Cloud providers can offer a wide range of services, such as SaaS, PaaS, and IaaS, as well as different deployment methods, such as public, private, and community (Jamsa, 2013). Depending on what services and deployment methods are used, it may be difficult for cloud providers to provide all of the benefits and characteristics of cloud computing.

Many cloud computing architectures have developed due to this issue. The architectures range from fundamental to specialized, each having their specific use in the cloud computing environment. Two of the fundamental cloud computing architectures are the workload distribution and resource pooling architectures.

Cloud computing architectures "formalize functional domains within cloud environments by establishing well-defined solutions comprised of interactions, behaviors, and distinct combinations of cloud computing mechanisms and other specialized cloud technology components" [3]. In essence, this means that these architectures focus on a certain quality or characteristic of cloud computing by gearing procedures, mechanisms, and components in the cloud environment towards this quality or by allowing this quality to perform in a certain way. For example, the Dynamic Scalability architecture focuses on the scalability aspect of cloud computing. To suit some business models, cloud providers must gear their cloud services to scale well with the usage of their consumers [3]. There are many cloud computing architectures, each having an importance in the business world.

The remainder of the paper is organized as follows: Section 2 provides the brief description of the workload, section 3 provide description of the resource pooling, section 4 discuss cloud security challenges, section 5 discuss the data breaches in cloud computing, section 6 discuss some solution to the security challenges, and Section 7 concludes the survey.

II. WORKLOAD DISTRIBUTION ARCHITECTURE

This is essentially a load balancing architecture. This architecture allows for resources to be scaled, meeting the requests that are being made for services on the cloud system. Resources are scaled horizontally, meaning as more requests come in, more resources are added to the

0-7695-6405-4/18/$31.00 ©2018 IEEE
DOI 10.1109/UKSim.2018.00032

group of resources responding to the requests [12]. The process of load balancing generally functions as such:

a. One or more cloud consumers make requests for a cloud service. The requests go through a load balancer, which then determines how to evenly distribute the requests among the available resources. In the context of requests for a cloud service, the cloud provider may have multiple instances of the service across several servers. The load balancer would ensure even distribution of computing load across these servers [3]. Figure 1 represent an example of the workload distribution architecture.

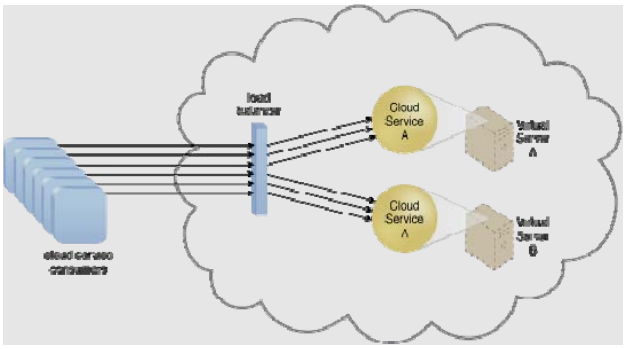

Figure 1. Workload distribution in a cloud system

Here, Cloud Service A and Cloud Service B are identical IT resources parallel and horizontally placed and accessed through a load balancer, that internally uses efficient algorithms to decide to which service (A or B) to send a request. Cloud Service B, which internally maps to the resource pool through Virtual Server B, is actually a redundant copy of Cloud Service A and is implemented on Physical Server B [3]. The load balancer is the first point of entry for a cloud service consumer request and, upon receiving the request, it directs them to either Physical Servers A or B. The load balancer takes care to ensure an even workload distribution through the computation of a load-balancing algorithm.

The workload distribution architecture thus allows for service provider to horizontally expand services as needed and cater efficiently to client needs. It also ensures that the IT resources and infrastructure are not over-taxed (or under-utilized), adds redundancy, and provides the feature of high availability.

A real world use case of using the load-balancing architecture would be a cloud service that caters to multiple e-commerce websites on a multitenant model. Each request to each e-commerce website must be responded to with availability, efficiency, and secure processing. The absolutely essential feature for an e-commerce web service is high availability. A load-balancing architecture ensures that each service is processed without any latency, outages, and denial of service.

b. The component that makes the workload distribution architecture different from other fundamental architectures is the load balancer. The load balancer is essentially made up of an algorithm that attempts to distribute computation load as evenly as possible [6]. Despite the fact that cloud-based load balancing is a well-defined concept in the cloud environment, effective load balancing continues to elude professionals. Researchers are constantly trying to develop new or improved algorithms to distribute load. Commonly used load balancing algorithms include Ant colony optimization, Genetic algorithm, Bin-packing, Adaptive, etc. [7]. Below is the pseudo-code of one example of such runtime algorithm [18].

c.

```
BalanceLoad()
{
        generate a completionTime matrix;
        for each task in taskList
        {
        find minimum completionTime from matrix;
        assign task to respective virtualMachine;
        update the completionTime;
    }
}
```

d. Besides the main load balancing mechanism, the architecture can also include the audit monitor, cloud usage monitor, hypervisor, logical network perimeter, resource cluster, and resource replication mechanisms [3]. A great example of the workload distribution architecture would be a public cloud service, such as Google Drive. Google Drive is a cloud storage service that is offered to all users with a Google account. Users can upload, download, and use files in Google Drive. With hundreds of thousands of users using Google's services, Google has to distribute the workload among its many servers, so that no server is more under- or over- utilized than another. This ensures smooth functioning of Google's services.

III. RESOURCE POOLING ARCHITECTURE

As the name implies, the resource pooling architecture utilizes resource pools. Resource pools can be thought of as a group of identical and either physical or virtual resources that form a single logical unit. In the cloud environment, nearly every IT resource can be pooled together. Common IT resource pools include physical server pools, virtual server pools, storage pools, network pools, CPU pools, and memory pools. Resource pools are versatile components because they are extremely useful in most cloud environments and can be as simple or as complex as needed [3]. Resource pools can also be created for specific uses, such as an application that needs a resource pool implemented in a specific way. In cloud environments, resource pooling is useful because it allows the pooling of IT resources that are not in close physical proximity to other resources [3]. Despite resource

pooling having a dedicated architecture, resource pooling is also used in other architectures. Besides the main resource pooling mechanisms, other mechanisms that may also be used in this architecture include audit monitor, cloud usage monitor, hypervisor, logical network perimeter, pay-per-use monitor, remote administration system, resource management system, and resource replication mechanisms [3]. An example of a resource pooling architecture in the business world would be a SaaS cloud service. A cloud provider offers an accounting SaaS program. They have many clients that use this service to calculate their payroll. Some consumers may need a large amount of CPU resources to run the mass calculation. It would be wise for the provider to pool CPU resources, so that consumers have enough resources to use the application.

These two architectures are fundamental and lay the foundation for other, more specialized architectures. The key components in these architectures can be found in other architectures and models. It is important for businesses to consider the fundamental architectures before investing in a cloud system. It can help them understand their business needs more clearly, as well as improve the effectiveness of the cloud system in their work environment. Consider the illustration below [3].

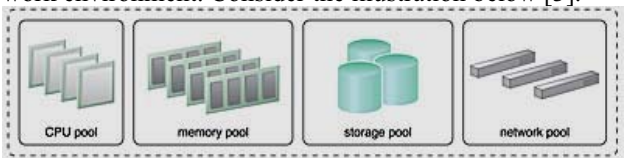

Fig 2. Resource pooling (Erl, Puttini, and Mahmood, 2016)

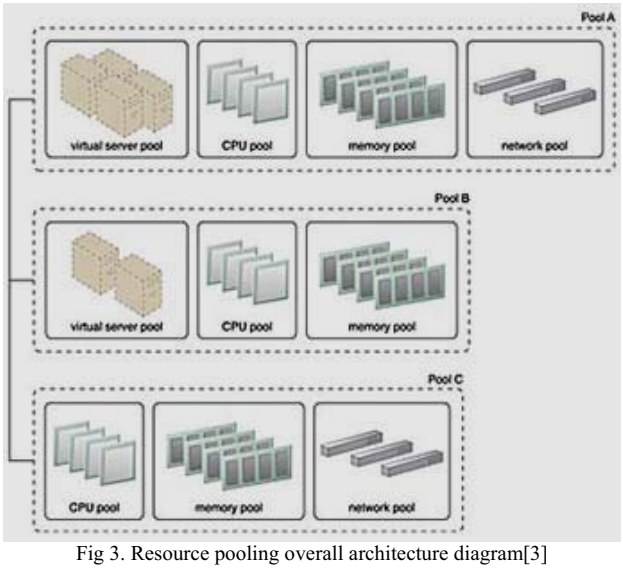

Fig 3. Resource pooling overall architecture diagram[3]

Each pool consists of identical resources. The CPU pool (or any of the other resource pools) can be made to grow, on the fly, to provide rapid elasticity. Each pool is considered a single resource, and viewed as an abstraction of the internal group of resources. These pools of resources can be designed together to build the overall architecture, as illustrated in the diagram below [3].

In fig3 above, resource pooling allows for cloud service providers to dynamically provide resources on-demand and ensure flexibility, scalability, and high availability of their services, without falling prey to efficiency reduction caused by over utilization of any one type resource. However, it is also evident in the above illustrations that resource pooling can quickly become complex, tangled, and hard to maintain if strict architectural guidelines and designs are not followed [12]. It is possible for resources to be under-utilized or escape unaudited. It is also possible for resource allocation and routing algorithms to get convoluted and inefficient. This can add over-head and latency, as well as slow down processing time and prove counter-effective. It is thus best to stick to a simple hierarchical parent-child model when designing the overall architecture that internally uses resource pooling [12]. It helps demark the group that each set of diverse resource pools belongs to, makes auditing (and maintenance and patching) easy, and helps in the application of tree-based allocation and synchronization algorithms.

The threats that affect cloud systems are similar to threats on other computer systems. The uniqueness of these threats pertains to the unique characteristics of cloud systems. One threat that is relevant to cloud systems is insecure interfaces and APIs [10].

The embracing of cloud-based services by corporates, businesses, and people, has helped to usher in a paradigm shift in the people-data-service relationship. While most steps in the evolution of technology center around “development” and “productivity”, given the changing scenario of threats and cybercrime, security in the cloud needs to be thoroughly analyzed, researched, and mitigated, even if they cannot be completely eliminated or avoided. Cybercrime, as it is known, is one of the fastest-growing crimes in the U.S., causing damages to businesses totaling in $3 trillion in 2016 [11].

IV. CLOUD SECURITY CHALLENGES

One of the many things that change between regular systems and cloud-based systems is the nature of data breaches. Cloud-based platforms often carry the data of a minimum of one client and potentially many more. This means not only is the parent cloud platform compromised, all of the clients that reside on the breached system are also exposed. This can become incredibly damaging if the platform holds sensitive medical information, trade secrets, intellectual property, and other data types. This would incur not only the standard data breach law but laws like HIPAA and other relevant laws. As mentioned, this will then damage the reputation of the client and the parent cloud platform. While cloud providers often take

every possible step to ensure the security of their systems (and often advertise as such), many cloud providers transfer ultimate responsibility for clients to protect their own data in the cloud. Figure 4 represent NIST definition of cloud computing, the characteristics that are implemented using various technologies and figure 5 represent the challenges in cloud computing.

The technologies along with the cloud service and deployment models introduce cloud specific security risks and vulnerabilities in addition to shared risks with the conventional IT infrastructure [13].

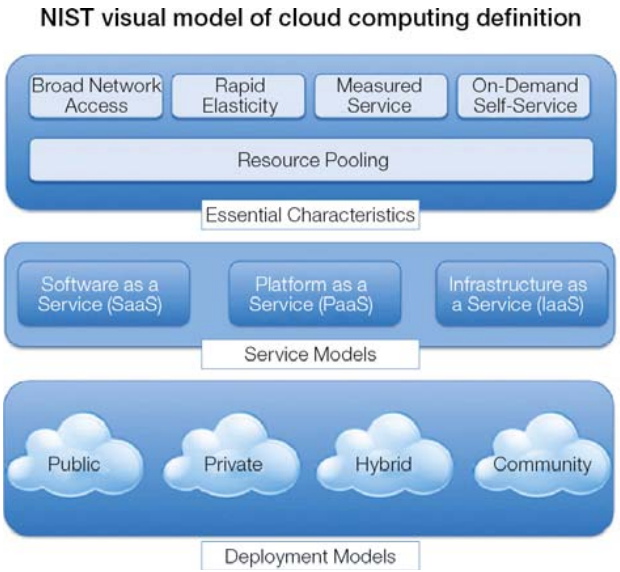

Fig. 4. NIST definition of cloud computing.

Fig. 5. The challenges in cloud computing.

V. DATA BREACHES IN CLOUD COMPUTING

In terms of specific threats towards cloud systems, the CSA (Cloud Security Alliance) listed the top cloud computing threats that organizations face. Among these threats includes data breaches, compromised credentials and broken authentication, hacked inter-faces and APIs, exploited system vulnerabilities, account hijacking, malicious insiders, APTs (Advanced Persistent Threats), permanent data loss, inadequate diligence, cloud service abuses, DoS attacks, and shared technologies.

A. Weak/Compromised Credentials or Broken Authentication

Weak credentials refer to the threat that users pose when they create passwords to access their accounts. Compromised credentials are often a result of weak credentials. Attackers can use credentials to gain access to sensitive information assets [5]. Broken authentication is in a similar vein to weak credentials, except that the fault of weak authentication is attributed to the mechanism developer rather than the user. Mistakes or negligent actions that develop include using weak passwords encryption/hashing, embedding credentials or cryptographic keys into source code that is made public, etc. [15]. These threats affect all systems with authentication mechanisms, but pose a unique issue in cloud systems. Cloud systems often use Single-Sign-On systems for management and convenience purposes. This means that the authentication mechanism becomes a single point of failure, allowing attackers to access a host of sensitive assets with one set of credentials [8].

B. Malicious Insiders

As with most systems, cloud systems suffer from the age-old threat of malicious insiders. Malicious insiders are typically employees (current and former), third party contractors, or temporary workers that have, at least, partial authorized access to resources within an organization [14]. They also know the inner physical and logical layout of the organization's assets and infrastructure. They use their access and knowledge to exfiltrate or destroy assets [14]. Insiders are a serious threat to many organizations because of the sheer damage and havoc they can cause for an organization. Malicious insiders can have a variety of motives: greed, revenge, fame, etc. This makes insiders hard to predict. The malicious insider threat is amplified in the presence of cloud systems because of the greatly increased attack surface. Insiders threaten the security of both the cloud provider and consumer [1]. On the provider's side, insiders enjoy administrative access to consumers' sensitive data and resources, allowing significant damage of multiple organizations to occur [3]. On the consumer's

side, insiders can easily access a wide variety of resources in one logical place in the organization. Threats are perpetrated through certain methods, or attacks.

C. Threats to Identification, Authentication, Authorization

Access is the next big concern when services are on the cloud. Most security compromises in the recent times have occurred due to weak or non-existent Identity and Access Management systems. To mitigate this grave risk, both the organization and the provider can start by cleaning out the file structures (like ADFS), streaming their federated services, having a single point of entry and exit, policies and control for identity creation, deletion, and provisioning and revoking access, and finally the stringent use of multi-factor authentication (smartcards, mobile phones, biometrics etc.) The recent security breakdown at Equifax could have well been averted with deployment of mandatory multi-factor authentication.

D. Man-in-the-Middle (MitM) Attack

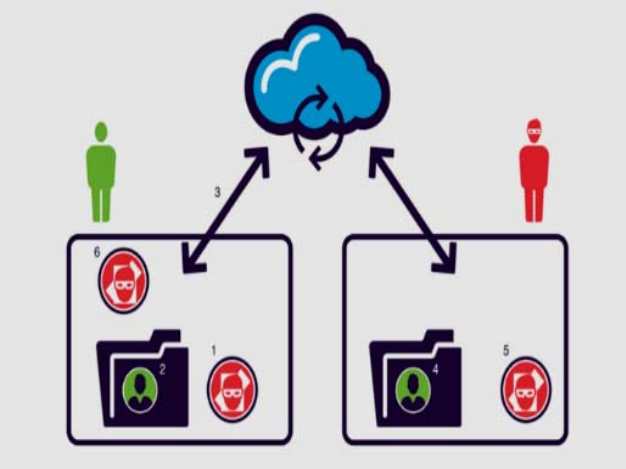

Fig 6 : Quick double switch attack method

Another attack is called Man-in-the-Middle (MitM) attack, or more specifically to cloud systems, Man-in-the-Cloud (MitC) [17]. MitM attacks refer to when an attacker surreptitiously intercepts network messages between two entities. The attacker can then read and/or modify the message and send through to the receiver [9]. In a MitC attack, the attacker steals a user's cloud synchronization token. First, the user must be infected with remote access malware. Once the attacker has control of a user's local files, they replace the user's sync token with one that points to their computer. The original token is placed with the cloud-synced files that are uploaded to the cloud and downloaded to the attacker's computer. The attacker can then use the user's cloud resources [17]. There are several attack methods used to execute MitC attacks: quick double switch, persistent double switch, and single switch [6]. Figure 6 shows a basic quick double switch attack. First, the victim is infected with malware where the cloud application is installed. The malware then switches the victim's token with the attacker's and inserts the victim's token into their sync folder. The cloud application recognizes an account switch and syncs the victim's files with the new account. Now the attacker has a copy of the victim's token. The malware runs again to switch the victim's token back to its original state, so that the attacker can avoid detection [8].

E. Insecure Application Programming Interfaces (APIs)

API security can be on the trickier side of things. API security is largely dependent on code reviews, bug reports, and patching. The CSA states on the record that penetration testing is one of the best tools here. Both of these solutions are solutions to exploitable system vulnerabilities as well. Both account hijacking and malicious insiders are closely related threats. Strict zero-tolerance on sharing credentials, strong password policies, and user logging can widely mitigate these issues.

Cloud systems rely heavily on interfaces and Application Programming Interfaces (API), which are the structures in which users interact to use the cloud services. For this reason, they are a major building block that cloud systems are built upon. This also make them a common attack vector for attackers. Interfaces and APIs are public-facing, acting as a door for attackers. APIs in particular, are not only public-facing, but also lie outside of the business's trusted boundary and is very visible to external entities [8]. Interfaces must be built with security in mind and as one of the main focuses. The issues that lead to insecure interfaces are weak authentication mechanisms, insufficient authorization mechanisms, and weak or poorly implemented encryption [10].

F. Denial of Service (DoS), and its Distributed Version (DDoS),

Threats are perpetrated through certain methods, or attacks. One attack on cloud systems is Denial of Service (DoS). DoS disables access to a service or system by consuming most or all of the available resources on the host system through the use of network requests. A Distributed DoS (DDoS) is a specific DoS where multiple nodes send requests to overload a system [9]. Because of cloud systems' heavy reliance on network infrastructure and centralized nature, cloud systems may suffer from this attack. DoS are often hard to mitigate and are resource consuming, making them a deadly attack against cloud systems [12]. The advantage that cloud systems have compared to other systems is that they typically have a large pool of resources to draw from, requiring attackers to have more resources to overload the system [9].

VI. SOLUTIONS FOR THREATS AND ATTACKS ASSOCIATED WITH CLOUD SYSTEMS

Once a business has considered the threats and attacks associated with cloud systems, they should also consider what solutions could be implemented to mitigate, prevent, or avoid them. A solution that will fix some issues would be proper protection of data, network connections, and authentication mechanisms [1]. Proper protection may include:

1- Encryption, to protect the confidentiality of authentication and messages,

2- Hashing, to ensure the integrity of the data.

3- Businesses should also regularly check applications, interfaces, etc. for vulnerabilities or misconfigurations and implement security provisions when necessary [1]. This is crucial for preventing unauthorized access to cloud resources.

4- Lastly, cloud providers should follow standards such as ISO/IEC 27001, ISO/IEC 27017, and ISO/IEC 27018. ISO/IEC 27001 sets standards for general information security that most organizations should follow. ISO/IEC 27017 and 27018 focus specifically on security in cloud systems [1]. Cloud consumers can look for providers that have certifications related to these standards; table1 lists the steps that enhance protections for customers.

TABLE 1: FIVE MAIN STEPS USED TO PROTECT THE INFORMATION AND DATA OF THE USERS.

Steps to enhance protections for consumers	
1	Protect private information before sending it to the Cloud
2	Don't replicate your organization in the Cloud
3	Keep an Audit Trail
4	Governance:
5	Protect your API Keys

VII. CONCLUSION

Workload and resource pooling architectures are fundamental and they lay the foundation for other, more specialized cloud architectures. The key components in these architectures can be found in other architectures and models. It is important for businesses to consider the securing the fundamental architectures before investing in a cloud system. It can help them understand their business needs more clearly, as well as improve the security effectiveness of the cloud system in their work environment. Since cloud-based systems are still a new technology, it is important for the Security professionals to adjust and provide a tremendous security to them. Because of the nature of the cloud and the loss of control over many of its security aspects, many businesses will choose to completely disregard such a platform until conditions become more favorable for their security and bottom line. There are many aspects that professionals must acknowledge when considering implementing a cloud-based system into an organization. The threats, attacks, and solutions discussed are just some of the security-related aspects that a business must consider. A firm grasp of the concept of these aspects can go a long way when making the correct choice for an organization. Professionals are encouraged to explore all of the aspects and security challenges to ensure the precision of whatever decision is made.

A. Suggestions for Future Research

We are going to study the importance of secure cloud computing system for data at rest and data on transit using Encryption and biometric system because the future of cloud services especially those offering Data as a Service, depends on the guarantee of data security in the cloud. As a result we need to simulate different scenarios for the attacks that might happened to these cloud systems and how sever the system will insure recovery after the attacks.

REFERENCES

[1] Cloud Standards Customer Council (2015, March). Security for Cloud Computing Ten Steps to Ensure Success (Version 2.0). CSCC. Retrieved from http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

[2] CSA (Cloud Security Alliance) https://cloudsecurityalliance.org/

[3] Erl, T., Mahmood, Z., & Puttini, R. (2013/2015). Cloud Computing: Concepts, Technology, & Architecture. Westford, MA: Arcitura Education.

[4] Evans, S. (2016, August 22). Cloud Use Increases Attack Surface, But Security Not Keeping Up. Infosecurity Magazine. Retrieved from https://www.infosecurity-magazine.com/news/cloud-use-increases-attack-surface/

[5] Granneman, J. (2012, August). Password-based authentication: A weak link in cloud authentication. TechTarget. Retrieved from http://searchcloudsecurity.techtarget.com/tip/Password-based-authentication-A-weak-link-in-cloud-authentication.

[6] Ghomi, E. J., Rahmani, A. M., & Qader, N. N. (2017). Load-balancing algorithms in cloud computing: A survey. Journal of Network and Computer Applications, 88, 50-71. https://doi.org/10.1016/j.jnca.2017.04.007

[7] Goraya, M. S. & Thakur, A. (2017). A taxonomic survey on load balancing in cloud. Journal of Network and Computer Applications, 98, 43-57. https://doi.org/10.1016/j.jnca.2017.08.020

[8] Imperva (2015). Man in the Cloud (MITC) Attacks. Hacker Intelligence Initiative. Retrieved from https://www.imperva.com/docs/ HII_Man_In_The_Cloud _Attacks. pdf

[9] Jamsa, K. A. (2013). Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security, and More. Burlington, MA: Jones & Bartlett Learning.

[10] Leach, S. (2016). Cloud Security Threats - Insecure APIs. Hewlett Packard Enterprise. Retrieved from https://community.hpe.com/t5/Grounded-in-the-Cloud/Cloud-Security-Threats-Insecure-APIs/ba-p/6871684

[9-11] Morgan, S. (2017). Top 5 cybersecurity facts, figures and statistics for 2017. CSO from IDG. Retrieved from

https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

[12] Palmer, G. (2016, November 30). Workload Distribution and Resource Pooling Architecture. Zymitry. Retrieved from https://zymitry.com/workload-distribution-resource-pooling-architecture/

[13-10] Posey, B. & Rouse, M. (2017). Insider Threat. TechTarget. Retrieved from http://searchsecurity.techtarget.com/definition/insider-threat

[14-11] Ryan M.D. Cloud computing security: the scientific challenge, and a survey of solutions J. Syst. Softw., 86 (09) (2013), pp. 2263-2268

[15-12] Rains, T. (2014). Threats in the Cloud – *Part 2: Distributed Denial of Service Attacks*. Microsoft Secure. Retrieved from https://cloudblogs.microsoft.com/microsoftsecure/2014/02/06/threats-in-the-cloud-part-2-distributed-denial-of-service-attacks/

[16-13] Rashid, F. Y. (2016). The dirty dozen: 12 cloud security threats. Retrieved October 20, 2017, from https://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html

[17-14] Siemons, F. (2017). Four common cloud attacks and how to prepare for them. TechTarget. Retrieved from http://searchcloudsecurity.techtarget.com/tip/Four-common-cloud-attacks-and-how-to-prepare-for-them

[18] Wang.S, Yan, K., Wen-Pin Liao. W (2010). Towards a Load Balancing in a three-level cloud computing network. 2010 3rd International Conference on Computer Science and Information Technology. doi:10.1109/iccsit.2010.556388.