Comparing cloud security directions between the academia and the Industry, A survey

L.W.L. Jansen
l.w.l.jansen@student.utwente.nl
University of Twente

ABSTRACT

The cloud represents a network that offers on demand software and hardware for users worldwide. Cloud security responsibilities are conceptualized within the shared security model. Over the last decade cloud security issues are well researched by the academia, yet many issues still occur within the industry. Mainly issues to be prevented by cloud users are still frequently reported despite being researched by the academia for more than 5 years. We believe their to be a gap between the issues worked on by the academia and the Industry. Our contribution is to shed light on this gap and show what type of problems should be addressed instead and add value for both the academia and the Industry.

KEYWORDS

Cloud Security, Survey

1 INTRODUCTION

The term 'cloud' comes from the drawing of a cloud around a computer network in order to display that the devices in that network can communicate with each other [1]. This was first done with the rise of packet switched networks [2]. Traditionally communication networks like the telephone would use circuit switching, i.e. establish a fixed connection between two nodes to communicate [3]. With packet switching the data is divided up into packets and then send to its destination to allow other devices to use the same channel. Hence there was no longer a need to know which route the data is taking and the term 'cloud' was used to describe the routes travelled by the data [4].

Within the cloud there are 3 basic service delivery models namely, Saas (Software as a Service) which offers specific applications for business that are ready to use. PaaS (Platform as a Service) that provides a company with a tool set to create and manage their own applications and IaaS (Infrastructure as a Service) provides storage, servers and network technology for the user.

Security within the cloud is not only the responsibility of the CSP (Cloud Service Provider) but partly that of the user. For this the industry build a tool called the SSM(Shared Security Model) Services [6]. This tool is used to conceptualize and show the distribution of responsibilities regarding security of the cloud. In short, the user is responsible for the security 'in' the cloud and the CSP for the security 'of' the cloud Services [6].

Over the last decade the academic world worked to improve cloud security. And the literature shows a clear direction of the academia. In a survey by Subashini and Kavitha [7] from 2010 focused on the security issues that are related to the cloud service delivery models. In 2015 Ali et al. [8] wrote a detailed survey about the state-of-the-art in cloud security and a discussion about the open issues with regard to network and virtualization technologies. While the network issues list more conventional issues like authentication and Denial of service attacks they claimed that the virtualization issues needed more attention by the academia. In 2016 Singha et al. [9], Singh and Chatterjee [10] and Khan [11] published papers that provided an update view on the cloud security issues and attacks together with more research on virtualization vulnerabilities. Despite this increase they opted for additional focus on virtualization and legal issues. The papers by Tubaishat [12], B.Hong et al. [13], Alhenaki et al. [14] and especially Kumar and Goyal [15] from 2019 give a completed overview of cloud security issues and mitigation's. They claim that future work should focus on the issues that harm the trust of the consumers the most.

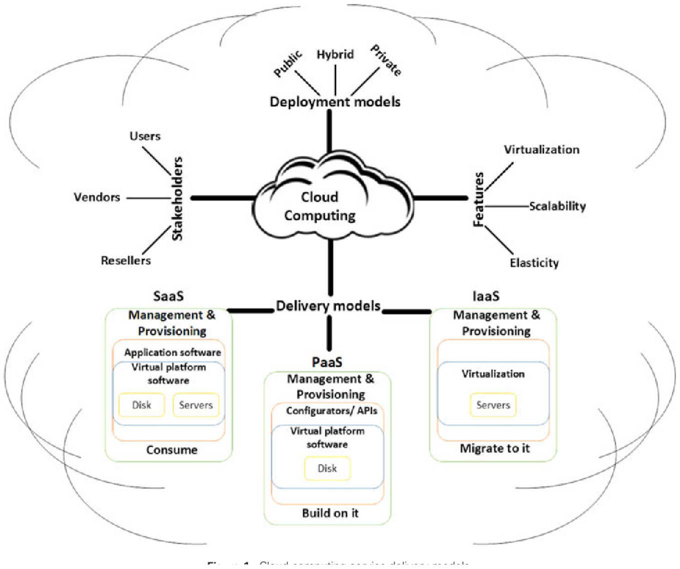

Figure 1: Example of cloud icon used to display the network and the delivery models [5]

We believe there is currently is gap between the issues worked on by the academia and the issues faced by the industry. Our goal is to get the two sides to focus on the same issues. Therefore our main contribution is to highlight the gap to shed light on what type of problems should be addressed and add value to both the academia and the industry.

To pursue our goal, we have defined the following research questions (RQ) as the basis of our research:

- **RQ1:** What are the issues being addressed by the academia?
- **RQ2:** What issues addressed by the academia happened in the industry?
- **RQ3:** Which issues addressed by the academia are worked on by third-parties?

This paper is organized in the following order. The first research question is answered in section 2, with a list of the issues addressed by the academia and a description of each issues. This list is constructed by performing a literature study on cloud security and collecting papers from Scopus and Google scholar. In section 3 we answer our second research question about the occurrences of the issues in the industry. Using the list of issues from section 2 we construct queries for google.com to find occurrences of incidents within the industry. Section 4 gives an overview of the solutions to our issues list provides by third-parties involved in the cloud. Finally in section 5 the results are discussed and future work is described.

2 ISSUES ADDRESSED BY THE ACADEMIA

The goal of the first research question is to find the cloud security issues that are currently being addressed by the academia. These issues are found by performing a literature review. In order to perform this literature review we rely on a set of keywords within the cloud security domain and online paper databases. Finally the issues are categorized via the SSM. We do this in order to highlight where the potential gaps are inside the industry.

Scopus was used to first find surveys about cloud security that where published in 2019. These surveys contained security issues that formed the basis of our issue list and our keyword set. The reason for doing this in Scopus is the default overview of keywords that Scopus provides, making it easier to analyze keywords of hundreds of papers. For our search we applied the following filters in Scopus as well. Sources may only be conference proceedings or journals and articles or conference papers, as books or reviews are not useful for our goal. Finally the papers are filtered on being within the subject area of computer science. Additionally a crawler was build in python to collect papers about these issues in google scholar. With the keyword set from scopus, per issue a set of papers published between 2010 and 2019 was collected. These papers where then classified per date put together in Figure 2.

Out of our Scopus search we found the following list of issues. They are divided into two categories which are the two sides of the SSM. The set of keywords was used to find papers about the subject. This keyword set can be found in the second column of the table.

Not all Issues can be divided into two different sections. Denial of service (DoS) attacks can occur on both sides of the security model. However, the CSP has a more crucial role in providing DoS protection since they manage the Iaas layer of their own cloud. Therefore we opted to set the DoS issues as the responsibility of the CSP. GDPR compliance is again something both sides have to deal with but since the security model states that the user is responsible for the security 'in' the cloud we listed it under the users responsibility.

CSP Issues	**Keyword set**
Co-residence attack	co-residence, co-resident, attack, virtual machine
VM rollback attack	VM rollback, attack, virtual, machine, IaaS
VM Escape attack	VM Escape, virtual, machine, IaaS
Denial of Service attack	network, distributed, denial of service, attack, Iaas, Paas, Saas, mitigation
User Issues	
Phishing attack	Phishing, attack, access, control, authentication
Man in the Middle attack	Man in the Middle attack, network, authentication, PaaS
(IP) Spoofing	IP, Spoofing, attack, network, authentication, PaaS
SQL injection attack	SQL injection, attack, malware, Paas, Saas
Port Scanning	Port Scanning, attack, malware, Iaas
GDPR compliance	GDPR, regulations, cloud

2.1 Issues at the CSP side

2.1.1 Co-residence and side channel attacks. A co-residence attack [16] is when a attacker extracts sensitive information from a Virtual Machine(VM) via it's own co-located malicious VM. The first step is to place the attacker's VM next to the target VM. Second, is to perform various side channel attacks that extract data from the target VM. A side channel attack [17] is an attack that uses information gained from the implementation of a computer system. Examples are timing information, power consumption or electromagnetic leaks. Measuring this data tells the attacker information that can be used to exploit the target VM.

2.1.2 Virtual machine rollback attack. In explaining this attack we assume the hypervisor is already compromised because of hypervisor hijacking. The attacker uses the hypervisor to execute a virtual machine from a older version in order to undo security updates and open up vulnerabilities to exploit [18].

2.1.3 VM Escape attack. Virtual machine(VM) escape attack is a treat where the attacker enables a guest level VM to attack its hypervisor [19]. The vulnerability is present when there is weak or no isolation between the hypervisor and its VMs. The attacker escapes or breaks out of the hypervisors control over the guest VM and takes over the hypervisor and gains access to local OS files. Through this the other co-resident VMs will be under the control of the attacker.

2.1.4 Denial of service attack. A (distributed) denial of service attack(DDoS attack) [20] is a network attack where a very large amount of data is send towards a target application or network in order to deny any user access to that target or to make use of the targets functionality.

2.2 Issues at the User side

2.2.1 Phishing. With this issues the attacker tries to get sensitive information from users by pretending to be a trusted service [21]. For example, the attacker could host a replica of a bank website to trick users into giving up their credentials. Another example would be the phishing email where the user would think the email is from a trusted service telling them to take action because of a problem or they have won a prize. After clicking on the link inside the email they are forwarded to the fake website or they download malware that threatens their computer.

2.2.2 Spoofing. Spoofing [22] is when the attacker forges header data of his malicious packets to that of a trusted computer in order to gain access to another computer system. There are different type of spoofing attacks such as Internet Protocol(IP) [23], Domain Name System(DNS) [24] and Address Resolution Protocol(ARP) [25] spoofing.

2.2.3 Man in the middle attack. A man in the middle attack can be generalised as followed. The attacker intercepts messages between two parties to read or alter the information and send it back and forth while the parties believe to be communicating to each other in secret [26] [27]. This type of attack usually involves spoofing in order falsify the identity of the attacker. Examples of this attack are WiFi eavesdropping and session or email hijacking.

2.2.4 SQL injection. With this issue database access is misused in order to read and modify sensitive data from the database in the cloud [21] [28]. First he needs to get access to the database by proving to the CSP he is a valid user. Then he can gather sensitive data from the database using SQL queries that contain executable malicious code.

2.2.5 Port scanning. One attack that is less harmful but very concerning is Port scanning [29] [30]. Here the attacker tries to get as much information out of the target as possible. By sending spoofed packets to a target operating system he finds out which ports have certain kinds of traffic. This information is stored in the return packets.

2.2.6 GDPR compliance. The General Data Protection Regulation is a law in the European Union on data protection and privacy [31] [32]. The main goal of the regulation is to give individuals control over their personal data. Businesses have to follow the regulations about storing, collecting and processing data from people. Being non complained with the law can result into a fine going up to 20 million euros or, if higher, 4% of the annual worldwide turnover. Another important feature of the GDPR is that companies are required to report a data leak within 72 hours of discovery. This results into more transparency about the companies security towards the users.

In figure 2 the demographic results for the issues can be found. In total there where 3455 papers collected using the crawler.

RESULTS ARE PRELIMINARY, more will be added towards the final submission

Before analyzing the data from figure 2 we must first state its limitations. Due to the many requests send by the crawler google blocked us after a while. This resulted in less papers for each of the issues. The way google scholar selected the papers is based of a vast number of criteria, such as location, country and personal details. This should be taking into account when looking at the relevance of the papers.

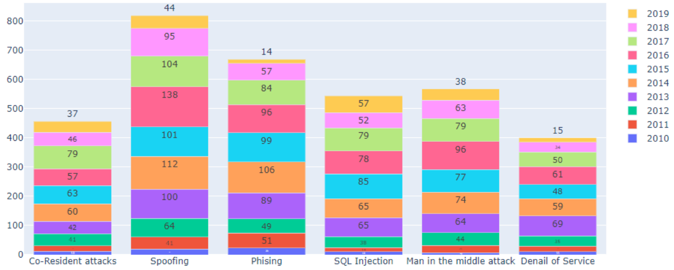

Figure 2: The amount of papers published per year per issue.

3 ISSUES THAT HAPPENED IN THE INDUSTRY

We have identified 10 issues that are being addressed by the academia. In this section our goal is to find out which issues actually happened in the industry and how often.

Our methodology for this research question makes use of the keyword set constructed in the previous section. To find reports of incidents the issues are combined with keywords to make queries for the google news search engine. The difference between google news and the standard search engine is that only news sources will appear to us. This help in filtering commercial websites at the cost of missing out on some reports of incidents because google news didn't not show it to us. However, due to the time-constraint of this project we decided to use the google news engine.

Before starting this search we need to take into account what we might expect to find. We expect to find reports of incidents related to the issues that are the responsibility of the user. Not only because these are the easiest to perform, but we don't expect CSPs to bring out stories or report that their infrastructure is vulnerable. They may release statements saying they fixed a vulnerability but that leaves only speculating about whether or not anything went wrong.

The results can be found in figure 3 below. In total there where 2.632 web pages manually analyzed. For each issues different queries where constructed. Through out the search process new keywords or synonyms for issues where noted and reused for the queries.

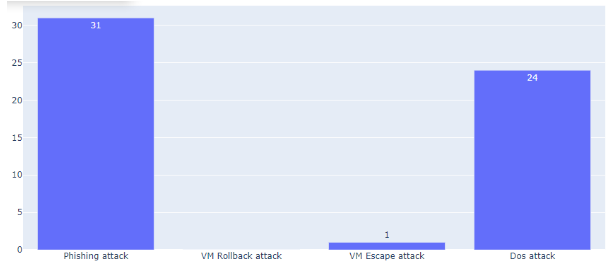

Figure 3: Total amount of incident reports found per issue

RESULTS ARE PRELIMINARY, more will be added towards the final submission

With these results we can draw some conclusions. CSPs are either having no issues at all or they are doing their best in keeping reports down. Or the worst case scenario is that a they themselves don't even know when they are happening. A DoS attack is easily recognized but VM escape or co-resident attacks can happen without the knowledge of the host.

The incidents that where found reside mostly on the user side of the shared security model. This can be explained by companies still not realizing their responsibility for their own security. Sometimes the lack of responsibility is accompanied by the lack of knowledge about the security of their systems. These results show that cloud users need to improve on their security and live up to their part of securing the cloud.

4 ISSUES ADDRESSED BY THIRD-PARTIES

With the incidents collected from the Industry our next goal is to look at the solutions the industry provides to these issues. The goal here is to find out which solutions the Industry provides towards the issues addressed by the academia. These solutions can be offered by the CSP themselves or by third-parties. Many third-parties offer their solutions on the CSP marketplace, from which we collected our data.

For this research question both manual searching and crawler scraping is used in order to fulfill our goal. The crawler is used to collect advertisements on the marketplaces from Microsoft Azure and Amazon Web Services. Additionally a manual search for advertisements is performed similarly to the methodology in the previous section.

RESULTS ARE PRELIMINARY, more will be added towards the final submission

5 DISCUSSION

Cloud was first used as a term to describe a communication network within a drawing. Now the cloud represents a large network with on demand software tools for companies all around the world. It is divided into 3 different service models, each representing another layer of the cloud. There is Software as a Service, Platform as a Service and Infrastructure as a service. These layers have a joint security responsibility between the Cloud Service Provider and the user. This task division is described and explained using the shared security model. From this model we see that the CSP is takes care of security 'of' the cloud and the user takes care of the security 'in' the cloud. Cloud Security has been well researched by the academia over the last decade. The security landscape expanded with new issues arising in virtualization of the cloud. Currently the state-of-the-art is well documented, yet many issues still seem to occur inside the Industry. CSPs seem to provide solutions via either themselves or offering a marketplace where companies can offer their solutions to the cloud users. Despite this attacks that are well researched for more than 5 years still occur with the cloud. Therefore we believe there is a gap between the issues the academia is addressing and what is actually happening in the Industry. We set up 3 research questions in order to shed light on what type of problems should be addressed and add value to both the academia and the industry.

The goal of our first research question was to find out the cloud security issues currently being addressed by the academia. We identified 10 issues and categorized them by which responsibility it is to solve them, that is the user or the CSP. Additionally we show how well the issues are researched over the last 10 years by stating the amount of papers published per year.

In the second section we took the 10 issues and looked for related incidents within the Industry. By manually constructing queries and analyzing web pages via google and google news we gather a set of incidents. The data indicated that issues on the user side of the security model have a lot of known occurrences while the CSP issues are not well reported. Therefore we cannot claim anything about how well CSPs are addressing the issues, but on the user side there are still issues from more than 8 year ago occurring in 2019. Meaning that security and awareness of responsibility of security in the cloud needs to be improved.

Finally in the third section we searched for solutions to our 10 security issues provided by the industry. By analyzing the CSP marketplaces and google search queries we identify the number of different solutions to the 10 issues.

To conclude, in this literature study we found that within cloud security the academia has researched the issues well and while uncertain the CSPs seem to provide good security towards their side of the security model. The biggest improvement lies with the cloud user, a lot of issues still occur at their side and have been occurring for the last 5 years. CSPs and companies should focus on increasing the awareness for security responsibility so every aspect of the cloud gets improved security.

REFERENCES

[1] Wikipedia. Cloud Computing. In *https://en.wikipedia.org/wiki/Cloud*$_{c}omputingcite_{r}ef-MITCorbato_{1}9-0, visitedon02.01.2020.$

[2] Wikipedia. Packet Switching. In *https://en.wikipedia.org/wiki/Packet*$_{s}witching, visitedon02/01/$

[3] Wikipedia. Circuit Switching. In *https://en.wikipedia.org/wiki/Circuit*$_{s}witching, visitedon02/01,$

[4] Mark Laubach and Hewlett-Packard. Minutes of the IP Over Asynchronous Transfer Mode Working Group (ATM). In *https://archive.is/20120710170149/http://mirror.switch.ch/ftp/doc/ietf/ipatm/atm-minutes-93jul.txt*, visited on 02/01/2020.

[5] Salman Iqbal, Miss Laiha Mat Kiah, Nor Badrul Anuar, Babak Daghighi, Ainuddin Wahid Abdul Wahab, and Suleman Khan. Service delivery models of cloud computing: security issues and open challenges. In *Security and Communication networks, volume 9 issues 17*, 2016.

[6] Amazon Web Services. https://aws.amazon.com/compliance/shared-responsibility-model/.

[7] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. In *Journal of network and computer applications*, 2011.

[8] Mazhar Ali, Samee U.Khan, and Athanasios V.Vasilakos. Security in cloud computing: Opportunities and challenges. In *Information Sciences*, 2015.

[9] Saurabh Singha, Young-Sik Jeong, and Jong Hyuk Park. A survey on cloud computing security: Issues, threats, and solutions. In *Journal of network and computer applications*, 2016.

[10] Ashish Singh and Kakali Chatterjee. Cloud security issues and challenges: A survey. In *Journal of network and computer applications*, 2016.

[11] Minhaj Ahmad Khan. A survey of security issues for cloud computing. In *Journal of network and computer applications*, 2016.

[12] Abdallah Tubaishat. Security in Cloud Computing: State-of-the-Art, Key Features, Challenges, and Opportunities. In *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, 2019.

[13] Jin B.Hong, Armstrong Nhlabatsi, Dong Seong Kim, Alaa Hussein, Noor Fetais, and Khaled M.Khan. Systematic identification of threats in the cloud: A survey. In *Computer Networks, volume 150*, 2019.

[14] Lubna Alhenaki, Alaa Alwatban, Bashaer Alamri, and Noof Alarifi. A Survey on the Security of Cloud Computing. In *2019 2nd International Conference on*

Computer Applications Information Security (ICCAIS), 2019.

[15] Rakesh Kumar and Rinkaj Goyal. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. In *Computer Science Review*, 2019.

[16] Bhrugu Sevak. Security against Side Channel Attack in Cloud Computing. In *International Journal of Engineering and Advanced Technology (IJEAT)*, 2012.

[17] Wikipedia. Side Channel Attack. In *https://en.wikipedia.org/wiki/Side-channel*$_{a}ttack, visitedon06/01/2020.$

[18] S. Rama Krishna and B. Padmaja Rani. Virtualization Security Issues and Mitigations in Cloud Computing. In *Proceedings of the First International Conference on Computational Intelligence and Informatics*, 2017.

[19] Abdulrahman K. Alnaim, Ahmed M. Alwakeel, and Eduardo B. Fernandez. Threats Against the Virtual Machine Environment of NFV. In *2019 2nd International Conference on Computer Applications Information Security (ICCAIS))*, 2019.

[20] Wikipedia. Denial of service attack. In *https://en.wikipedia.org/wiki/Denial-of-service*$_{a}ttack, visitedon06/01/2020.$

[21] Lubna Alhenaki, Alaa Alwatban, Bashaer Alamri, and Noof Alarifi. A Survey on the Security of Cloud Computing. In *2019 2nd International Conference on Computer Applications Information Security (ICCAIS)*, 2019.

[22] Wikipedia. IP spoofing. In *https://en.wikipedia.org/wiki/IP*$_{a}ddress_{s}poofing, visitedon06/01/2020.$

[23] Opeyemi.A. Osanaiye. Short Paper: IP Spoofing Detection for Preventing DDoS Attack in Cloud Computing . In *18th International Conference on Intelligence in Next Generation Networks*, 2015.

[24] Wikipedia. DNS spoofing. In *https://en.wikipedia.org/wiki/DNS*$_{s}poofing, visitedon07/01/2020.$

[25] Wikipedia. ARP spoofing. In *https://en.wikipedia.org/wiki/ARP*$_{s}poofing, visitedon07/01/2020.$

[26] Esther Daniel, S. Durga, and S. Seetha. Panoramic View of Cloud Storage Security Attacks: an Insight and Security Approaches. In *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)*, 2019.

[27] Wikipedia. Man in the middle attack. In *https://en.wikipedia.org/wiki/Man-in-the-middle*$_{a}ttack, visitedon07/01/2020.$

[28] Iva Ranjan and Ram Bhushan Agnihotri. Ambiguity in Cloud Security with Malware-Injection Attack. In *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2019.

[29] Prachi Deshpande, Aditi Aggarwal, S.C.Sharma, P.Sateesh Kumar, and Ajith Abraham. Distributed Port-Scan Attack in Cloud Environment . In *2013 Fifth international Conference on Computational Aspects of Social Networks (CASoN)*, 2013.

[30] Prachi Deshpande, S. C. Sharma, Sateesh K. Peddoju, and Ajith Abraham. Security and service assurance issues in Cloud environment. In *International Journal of System Assurance Engineering and Management, Volume 9, Issue 1*, 2016.

[31] Ciarán Bryce. Security governance as a service on the cloud. In *Journal of Cloud Computing*, 2019.

[32] General Data Protection Regulation (GDPR). In *https://gdpr-info.eu/*, visited on, 16/01/2019.