Comparing cloud security directions between the Academia and the Industry

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

ABSTRACT

The world of cloud-based services knows a decade of impressive growth with an even more promising future to come. The rise of cloud computing comes with a high demand for security. Cloud security responsibilities are conceptualized within the shared security model, which is used to raise awareness amongst users of their responsibilities. The last decade, cloud security issues from this model were well researched by the Academia. The problem is that many of these issues still occur within the Industry. Our hypothesis is that there a gap between the issues worked on by the Academia and the Industry. In this paper, the goal is to shed light on this gap and bring the Academia and the Industry together.

KEYWORDS

Cloud Security, Survey, Comparison, Academia, Industry

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] back in 1965. Today the cloud is much more than a drawing. The basic anatomy of the cloud is shown in Figure 1. The three different delivery models provide software, infrastructure or platforms as a service. The cloud can be deployed as a public or private service and even a combination of the two as a hybrid cloud. With the cloud there are basically 2 main stakeholders, the users and the Cloud Service Providers (CSPs). Re-sellers act the same as a CSP only they buy their infrastructure from another CSP to offer it to their own customers. For this research we include re-sellers as part of the cloud users.

Between the user and the CSP there is a shared responsibility to secure the cloud. In order to conceptualize these responsibilities the CSPs created a model [3]. This so called Shared Security Model (SSM) is used to raise awareness amongst users of their security responsibilities in the cloud. In short, the user is responsible for the security 'in' the cloud and the CSP for the security 'of' the cloud. For example, you have a Dropbox account where you store data. Then Dropbox is responsible for keeping your data save from attacks against the Dropbox cloud. However, when your password is 1234 and it gets compromised you will be held responsible for not keeping your data in the cloud secure.

This model is merely a guideline and not the solution to security issues. The Academic world has worked hard to solve issues in the cloud. In the last decade alone several papers [5], [6], [7], [8], [9], [10], [11], [12] and [13] showed a wide range of issues that are well researched by the Academia. Some of these issues seem to be irrelevant to the Industry. In this paper, we address the problem

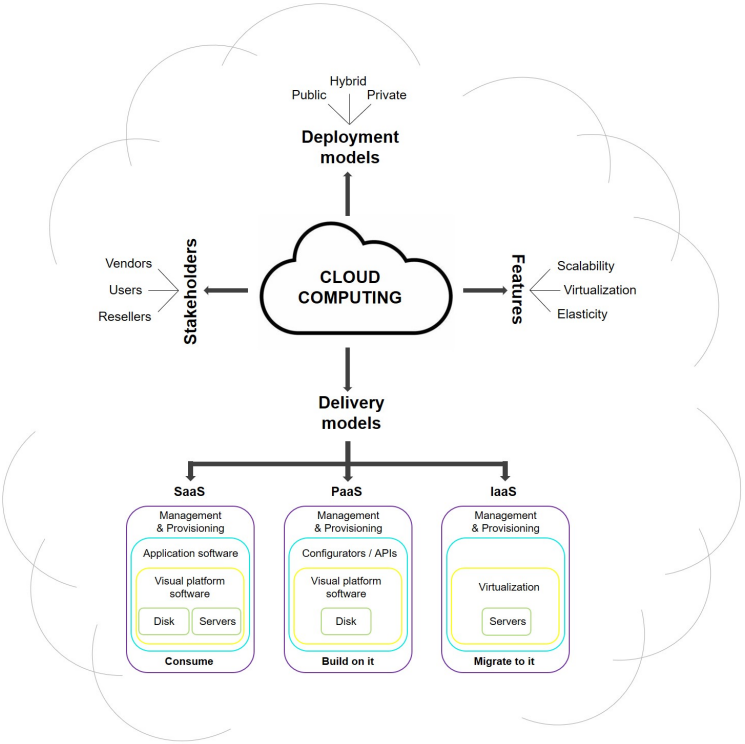

Figure 1: Overview of the aspects of cloud computing[4]

that, to the best of our knowledge, there is no academic paper that performs a broad comparison on whether the issues researched by the Academia are in-line with the needs of the cloud security Industry.

Our hypothesis is that there currently exists a gap between the issues worked on by the Academia and the issues faced by the Industry. The main contribution of this paper is to shed a light on this gap and bring the Academia and the Industry together in addressing this problem. To pursue our goal, we have defined the following research questions (RQ) as the basis of our research:

- **RQ1:** What are the cloud security issues being addressed by the Academia?
- **RQ2:** What cloud security issues addressed by the Academia happened in the Industry?
- **RQ3:** Which cloud security issues addressed by the Academia are worked on by the Industry?

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 digital libraries. 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 address our cloud security issues provide by Industry. In section 5 we reflect and discuss the results of our research and provide directions for future work.

1.1 Github

The results will come available in the research. Besides there is the aim is to let this work be reproducible by sharing (at least) the code that will be used for the data analysis in this research on GitHub. The results will be listed at: https://github.com/known5/Bachref.

2 ISSUES ADDRESSED BY THE ACADEMIA

The goal of the first research question is to find cloud security issues that are currently being addressed by the Academia and have been well researched in the past 10 years. The methodology to achieve this goal is to perform a literature study. This study is dependent on a set of keywords and surveys within the cloud security domain and digital libraries. Surveys provide a comprehensive overview of the state-of-the-art and thus the security issues. Keyword combinations allow for a specific description of the domain of each issue. The final list of issues will be split between the Cloud Service Provider (CSP) and the cloud user by following the Shared Security Model (SSM). These steps are necessary in order to make a comparison to the results of our second and third research question.

To find surveys and keywords we used Scopus [14]. This is a digital library for scientific readings and it offers an extensive amount of criteria to filter papers with. One of these filters is an overview of keywords of the current set of papers, with the keywords ranked by number of papers or in alphabet. This makes Scopus ideal for identifying our issues and keywords. An overview of all the Scopus filters is provided in Figure 2.

To achieve our goal, the following filters were applied to refine our search. We looked for conference papers or articles that are finalized and published in 2019, within the subject area of Computer Science. The sources of the papers are either journals or conference proceedings. These filters are necessary to remove irrelevant sources, subjects or document types. Our prior knowledge of the cloud computing domain was limited therefore, potential issues and corresponding keywords were found by a combination of two search methods.

At the basis of the first method we formulated a query to find surveys, namely "cloud security surveys". Applying the above mentioned filters resulted in a total of 146 surveys, that were subsequently analyzed for potential issues. Due to large set size, surveys were selected by reading the title, and if it was deemed relevant, the abstract was read as well. The second method used the same filters but had only "cloud security" as a basic query. When you filter on top ranking keywords in Scopus, a new overview appears of more specific keywords related to the ones already selected. Generally, when selecting more than 4 keywords, the overview showed names of potential issues as keywords. Selecting these issue keywords gave a final set of papers related to potential issues that were analyzed in a similar way as the surveys.

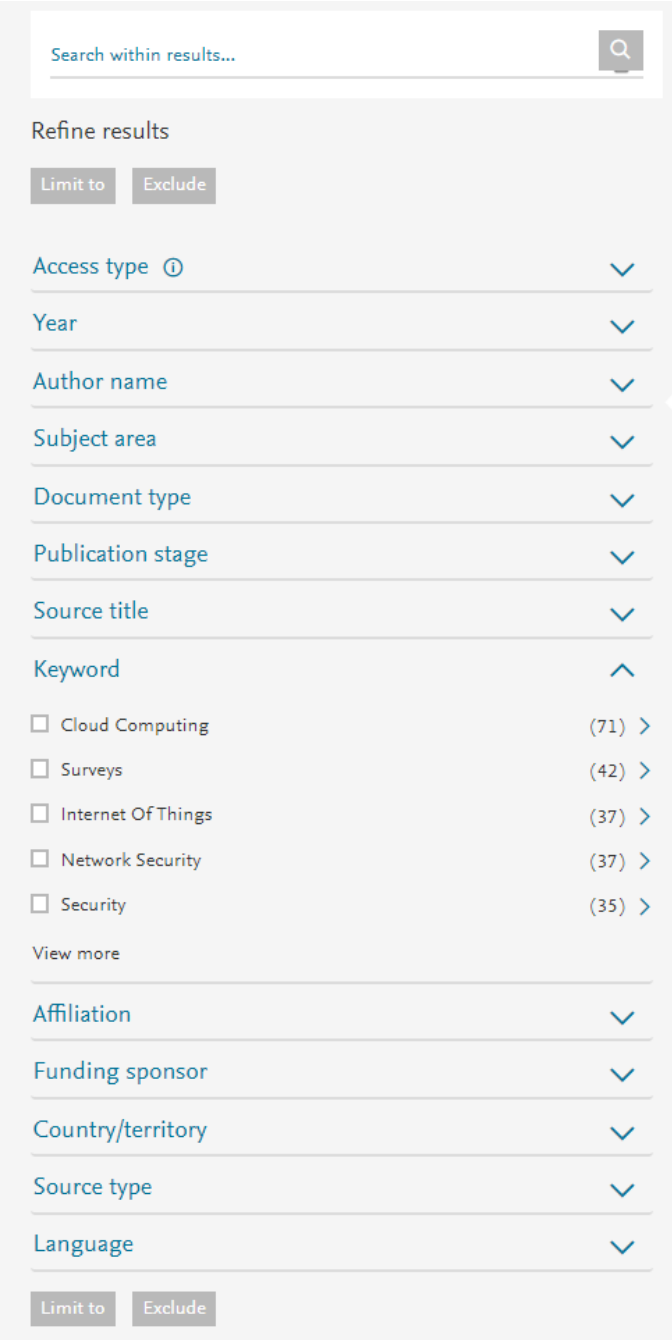

Figure 2: Overview of all the Scopus search filters

Having found issues that were currently addressed by the Academia, we wanted to see how well each issues was research over the last 10 years. For this we chose to use a different article source, namely

Google Scholar. This source is ideal for answering this question because of the way Google matches papers to your search queries. It tries to show results that are the most relevant to you depending on factors such as, search location, article language, number of citations and the keywords of the query.

To collect a significant amount of data we made use of Jupyter Notebook [15]. This is a web-based development environment with data collection, cleaning and transformation in different programming languages amongst its uses. In python we wrote a type of program called "crawler" [16]. Taking a set of keywords to construct a query, our crawler collected at each iteration the meta-data of 10 papers. This is because Google Scholar, like Google, presents its results 10 web-links at a time. Additionally, these iterations needed to occur in a random order otherwise Google would think we were a robot and thus block us. Therefore between each iteration of 10 papers the crawler would "sleep" for 60 to 100 seconds.

This literature study identified a total of 10 cloud security issues. By following the SSM the issues are placed in the category of the stakeholder that is responsible for addressing the issue. Each issue is described in sections 2.1 and 2.2. In the end a nearly 5000 papers where collected from Google Scholar. After section 2.2 a graph shows the distribution of papers per year per issue in Figure 3.

2.1 Issues of the CSP

The following 4 issue fall within the responsibility of the CSP. Denial of Service (DoS) attacks can happen to both stakeholders. However, the CSP has a more crucial role in providing DoS protection since they manage the Infrastructure of the cloud. Therefore we opted to set the DoS issue as the responsibility of the CSP.

2.1.1 Side channel attack. 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. This attack is performed in two steps, virtual machine (VM) placement and information extraction. For example, the attacker can create an account on Amazon Web Services [18] and with that gets a VM that runs on a physical server in the cloud. He can keep creating accounts and new VM until the so-called "co-residency" is achieved [19]. This is when the malicious VM gets placed next to the target VM. Once placed correctly, the attacker moves on to the last step and extracts information from the target VM via the previously mentioned side channel attacks.

2.1.2 VM Escape attack. First we explain the role of Virtual Machine Monitoring (VMM). VMM is performed by a program called the Hypervisor. All VMs in the cloud have a Hypervisor that manages VM creation, deletion, isolation and memory access. Now, assume the attacker created a guest account in the cloud with a VM co-resident to a Hypervisor and other VMs on a physical server. Through weak isolation provided by the Hypervisor the attacker can "escape" his guest VM into another VM or the Hypervisor. Once the Hypervisor is compromised he can take control over other VMs that are co-resident to his Hypervisor, this is called a VM Escape attack [20].

2.1.3 Virtual machine rollback attack. With this exploit we assume the Hypervisor is already compromised via a VM Escape attack for example. With the Hypervisor under his control the attacker can launch VMs of an outdated software version that still contained vulnerabilities that were previously patched. Via these vulnerabilities the attacker can take control of the target VM. This is called a VM rollback attack [21].

2.1.4 Denial of service attack. A denial of service attack(DoS attack) [22] 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. These targets can be anything that is connected to the internet and thus the cloud.

2.2 Issues of the User

The last 6 issues are the responsibility of the cloud user. General Data Protection Regulation is something both stakeholders to uphold to but since the security model states that the user is responsible for the security 'in' the cloud we listed it under the users responsibility.

2.2.1 Phishing. With this issue the attacker tries to get sensitive information from users by pretending to be a trusted service [23]. 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 [24] 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) [25], Domain Name System(DNS) [26] and Address Resolution Protocol(ARP) [27] 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 [28] [29]. 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 [23] [30]. First the attacker needs to get access to the cloud 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. Here the attacker tries to get as much information out of the target as possible [31] [32]. By sending spoofed packets to a target operating system he finds out which ports have certain kinds of traffic. This traffic contains information that the attacker can use for launching a bigger attack such as a DoS attack.

2.2.6 General Data Protection Regulation. The General Data Protection Regulation (GDPR) is a law in the European Union on data protection and privacy [33] [34]. 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, Article 83.6 [35] of the GDPR. 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.

To summarize, the list below shows our 10 issues within their respected category.

- CSP
  - Side Channel attacks
  - Virtual machine escape attack
  - Virtual machine rollback attack
  - Denial of service attack
- User
  - Phishing attack
  - Man in the middle attack
  - Spoofing attack
  - SQL Injection
  - Port scanning
  - GDPR Compliance

In Figure 3, the results of the Google Scholar search are presented. In total we collected 4949 papers on the 10 issues. In Figure 3 you can see that each issue is represented by a Bar chart, with on the y-axis the percentage for the number of papers in relation to the total paper count of the issue. On the x-axis you see all the issues listed with their total paper count. Each year has its own color and in each color block the number of papers from that year is posted.

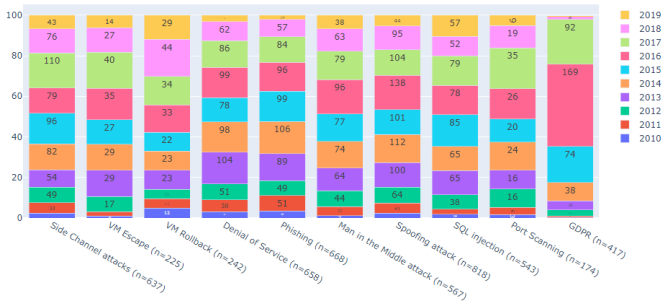

Figure 3: The number of papers published per year per issue.

Surprisingly, we saw that the number of papers in 2019 is relatively low, despite the relevancy of the issues in this year. This can be explained with the way Google Scholar selects papers. It selects papers that are most relevant to you. However, papers from 6 years ago have increased relevancy because they have more time to get cited and viewed than papers from 2019.

The last column of the GDPR is very different from the other issues. This can be due to the fact that GDPR was made in 2016 and came into effect in 2018 [36]. The other columns have a relatively even distribution, which indicates that these issues have been well researched throughout the last 10 years.

The goal here was to find 10 cloud security issues that are and have been relevant for the past 10 years. Each issue is placed together with the stakeholders responsible for solving it. In the next section we take these issues to answer our second research question.

3 ISSUES THAT HAPPENED IN THE INDUSTRY

In this section our goal is to find out which of our 10 issues actually happened in the Industry and how frequently.

Our methodology for this research question makes use of the keyword set constructed in the previous section. Issues and keywords were combined to create queries to be used in the search. For finding our incidents we used Google. For each incident found, we stored the title and data into an Microsoft Excel file. This is done to prevent duplicate data and statistical analysis later on.

For a query we would manually analyze the search results for incidents. Would we have automated this process, a classifier would be required to identify the news articles in the search results. Due to time constraints this was not possible, therefore a manual method was the best solution. Looking at Figure 4, we see an example of the first 3 results of a query.

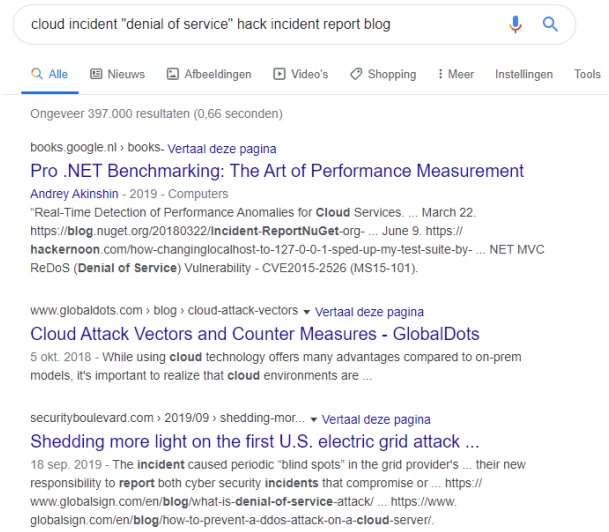

Figure 4: Example of the first 3 results of a Google search.

First we read the title and inspect the abstract for signs that this web page reports an incident. Result number three in Figure 4 shows clear signs of an incident report. If deemed interesting enough, the web page was bookmarked in our browser and the title and date are copied into our Excel file. By approximation we spend around 1 to 1.5 hours of searching per issue, again due to time constraints.

Before we present our results we must discuss a model, the so-called Cyber Kill Chain (CKC) [37]. This model is used to defend data security organizations by recognizing and defining phases of a cyber attack. Once they know which phase the attack is at, they can predict and intercept his next move in the kill chain. Our issues

are distributed in different phases. For example, port scanning and spoofing can be used to gather information about the target. A DoS occurs in the last phases of the kill chain, where the attack can be focused directly on the now identified target. An overview of this CKC including the different phases is presented in Figure 5.

Figure 5: Example of the Cyber Kill Chain [37].

In the end we managed to analyze a total of 9946 search results and found 142 incidents reports. An overview of these results can be found in Figure 6 on the next page. On the vertical axis the number of incidents found for each issue is shown and on the horizontal axis we see a total number of analyzed search results per issue. The blue bars belong to Cloud Service Provider (CSP) issues and the green bars belong to user issues. In addition Pie charts are provided of the distribution of the number of papers per year per issue in Figure 7. The charts were generated per two issues, therefore there is a different legend for every two issues. Incidents for port scanning and VM escape came from 2019, 2018 and 2019 respectively. Pie charts for issues with no incident reports were not created.

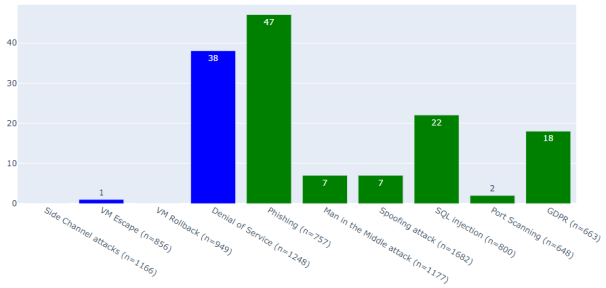

Figure 6: Total number of incident reports found per issue.

When looking at Figure 6, we found far less incidents related to the CSP than to the user. This can be explained by the characteristic of these four issues. Side Channel, Virtual Machine (VM) Escape and VM Rollback attacks require a higher amount of skill to perform than generating a phishing email for example. They require specific knowledge about the target cloud infrastructure. Making them a time consuming option for the standard malicious intruder.

Another possible explanation is that CSP's such as Amazon Web Services [18] have either excellent security or they manage to detect and solve the issue before it gets reported. The last option seems unlikely due to the amount of harm these attack can cause, any CSP would be affected by it. Also considering the GDPR, a CSP would have to report a data breach within 72 hours[34]. But not every CSP is located in Europe and thus adhere to these regulations. Denial of Service attack does have a large number of reports. This is probably due to the fact that a denial of service affects the users in the cloud. Therefore, the possibility of the incidents being reported is far larger with DoS then the other three attacks in this category.

The green bars in Figure 6 represent the incidents found our the issues on the user side of the SSM. Phishing is ranked the highest overall in reported incidents, which seems logical because like DoS it directly affects the users. Looking at the phishing pie chart from Figure 7 one might think the GDPR is a cause do to the high amount of reports in 2018 and 2019. Note that under the GDPR companies are required to report a data breach within 72 hours of discovery [34]. However, Almost all our phishing reports were related to incidents that occurred within the United States. Therefor GDPR had no impact on this results as it only effects European located companies.

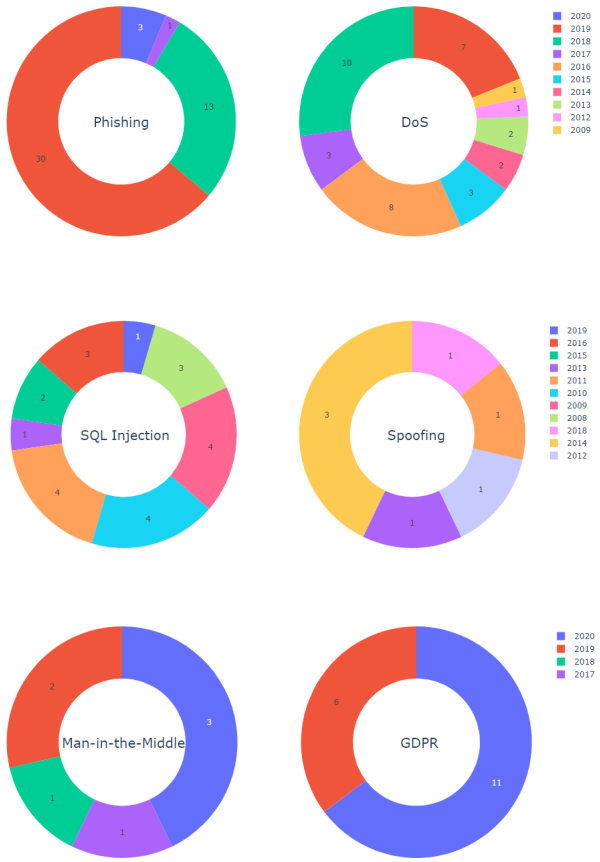

Figure 7: Distribution of the number of papers per year per issue.

In Figure 7 we can see that DoS and SQL injections have a relatively even distribution. This can be due to the fact that these issues

have been around for 10 years. They are also very easy to perform by the attacker, for example, you can buy a DoS attack online for only 5 dollars [38], Spoofing, Man in the Middle and port scanning attacks have a relatively low number of reported incidents. This can be explained by looking at the CKC. These attack appear in the early phases of an attack and are mostly used for reconnaissance and therefor would go relatively unnoticed as they would not directly affect cloud users. The pie chart for GDPR is very straight forward. All results are from European countries and all the reports came after the implementation of the GDPR in the European Union.

From our 10 issues of the previous section we collected a total of 142 reported incidents. The highest number of incidents, 103 out of the 142, where of issues that fall under the responsibility of the users (Figure 6). A reason for this can be that the CSPs have more knowledge and resources to protect the cloud, than a cloud user. Perhaps the CSPs are facing the same issues but are not reporting them for the fear of a bad reputation. An report of a phishing incident at AWS would wear of potential customers and halt cloud adoption across the world. Another reason can be that the issues on for the cloud user are more likely to get reported because they directly affect the users. This would explain the high number of reports for the DoS attacks.

Taking all this into account we think these results show that most security issues still occur at the users. The lack of knowledge, resources or awareness for security are all factors that seem to play a role in the frequency of the attacks. While the Academia and CSPs are going their own direction the users of the cloud seem to lagging behind in securing the cloud. This is a clear point of focus for both the Academia and the Industry.

The goal of this section was to find out how frequently the each of the 10 issues from section two occurred in the Industry. By performing a literature research we discovered 142 reported incidents. The results seem to suggest that the cloud user is struggling the most with addressing the security issues. However, the Academia is not the only one that offers solutions. In the next section we want to find out the solutions to address the security issues provided by the Industry.

4 ISSUES ADDRESSED BY THE INDUSTRY

In the previous two sections we identified 10 cloud security issues within the Academia. With these issues we search for incidents reports about these issues inside the Industry. The goal of this section is to identify the solutions to address these issues provided by the Industry.

Our methodology for this third research question is to perform a literature study. For each of our 10 issues we constructed a single query in order to find examples of companies that offered software to prevent the issue. For this search we again used the Google search engine. For a query we would manually analyze the search results for solutions. Again due to time constraint we could not automate this study with the use of a crawler and a classifier. Therefore, the results of each query are manually analyzed. First we read the title and inspect the abstract for signs that this web page provides software to address the issue. If deemed interesting enough, the web page was bookmarked in our browser.

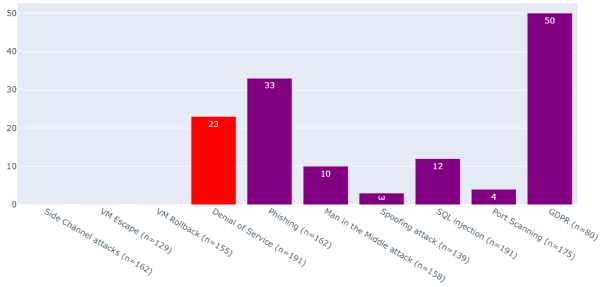

Figure 8: Total number of solutions found per issue.

In the end we analyzed a total of 1575 search results and found 112 solutions. The results are displayed in Figure 8 in the form of a bar chart, presented in Figure 8. On the vertical axis the number of solutions found is displayed. On the horizontal axis we show the 10 issues. The red bars represent the issues under the responsibility of the Cloud Service Provider and the purple bars represent the issues under the responsibility of the cloud user. Again following the Shared Security Model (SSM).

The most noticeable result it that of the General Data Protection Regulation (GDPR) [34]. In our first 80 search results we found 50 web links offering solutions to address GDPR compliance. This is very logical since the Google search results depended on the location of the enquirer. Since the implementation of the GDPR in 2018 every company needs to be compliant with this new law. Since this requires specific knowledge about IT and law a lot of companies offer this knowledge as a service to other companies.

Next to that, our results seem to be similar to the results of our previous research question. With the issues that directly affect the cloud users showing the highest number of results. This confirms our hypotheses of the previous section that the cloud users struggle the most with securing the cloud.

5 DISCUSSION

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 following the Shared Security Model. Additionally we showed how well the issues are researched over the last 10 years with a total of 9949 papers collected. At the second research question we took these 10 issues and searched for reports of incidents that happened inside the Industry. The search resulted in 9946 web-links analyzed and 142 reports found. With the third research question we looked for solutions to address our 10 issues that the Industry provided. A total of 1575 web-links were analyzed and 112 solutions found.

This paper addresses the problem that, to the best of our knowledge, there are currently no papers on performing a comparison on whether the issues researched by the Academia are in-line with the needs of the cloud security Industry. We have identified the cloud security issues of phishing, denial of service need to be addressed by the Academia. That doesn't mean that the Academia didn't research these topics well enough, but new research should focus on what the Industry needs to resolve these cloud security

issues. This requires a better cooperating between the Academia and the Industry.

In the future this work can be improved and expanded. In this research the time constraint didn't allow for constructing an automated process for gathering information from the Industry. Additionally the literature study performed in section 2 could be expanded to include more issues. It would be interesting to see if the results would change depending on a bigger population. More work can be done on shedding more light on the gap between the Academia and the Industry and identify key aspects of the gap that need to be addressed by both.

REFERENCES

[1] Wikipedia. Cloud Computing. In *https://en.wikipedia.org/wiki/Cloud_computing#cite_ref-MITCorbato_19-0*, visited on 02.01.2020.

[2] Wikipedia. Packet Switching. In *https://en.wikipedia.org/wiki/Packet_switching*, visited on 02/01/2020.

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

[4] 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.

[5] 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.

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

[7] 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.

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

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

[10] 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.

[11] 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.

[12] 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.

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

[14] Scopus. https://www.elsevier.com/solutions/scopus.

[15] Jupyter Notebook. https://jupyter.org/, visited on 21/11/2019.

[16] Wikipedia. https://en.wikipedia.org/wiki/Web_crawler. .

[17] Wikipedia. Side Channel Attack. In *https://en.wikipedia.org/wiki/Side-channel_attack*, visited on 06/01/2020.

[18] Amazon Web Services. https://aws.amazon.com/ec2/. .

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

[20] 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.

[21] 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.

[22] Wikipedia. Denial of service attack. In *https://en.wikipedia.org/wiki/Denial-of-service_attack*, visited on 06/01/2020.

[23] 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.

[24] Wikipedia. IP spoofing. In *https://en.wikipedia.org/wiki/IP_address_spoofing*, visited on 06/01/2020.

[25] 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.

[26] Wikipedia. DNS spoofing. In *https://en.wikipedia.org/wiki/DNS_spoofing*, visited on 07/01/2020.

[27] Wikipedia. ARP spoofing. In *https://en.wikipedia.org/wiki/ARP_spoofing*, visited on 07/01/2020.

[28] 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.

[29] Wikipedia. Man in the middle attack. In *https://en.wikipedia.org/wiki/Man-in-the-middle_attack*, visited on 07/01/2020.

[30] 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.

[31] 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.

[32] 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.

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

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

[35] Article 83.6. General Data Protection Regulation (GDPR), Articles 83 penalties. In *https://gdpr-info.eu/art-83-gdpr/*, visited on, 26/01/2019.

[36] General Data Protection Regulation History Wikipedia. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation. .

[37] Wikipedia: The Cyber Kill Chain. https://en.wikipedia.org/wiki/Kill_chain.

[38] TripWire: Hire a DDoS Attack for as Little as Five Dollars. https://www.tripwire.com/state-of-security/featured/hire-a-ddos-attack-for-as-little-as-5/.