The Cloud’s Computing Security

MILICA D. ĐEKIĆ, Subotica

Professional Paper
UDC: 004.722.035
DOI: 10.5937/tehnika1802300D

The emerging technologies are getting adopted massively worldwide and they are finding their applications in both – private and public sector. One of the well-known technological advancements being used today is a cloud’s computing. This sort of system is still in its development and every single day we are facing on the new improvements in that area of IT industry. The main challenge to the majority of emerging systems including the cloud’s computing is still a security. The role of this article would be to make a comprehensive discussion how cloud’s solutions work, what the critical pillars in their defense are and how we could improve our user experience applying those systems. Also, we would stress out some cloud’s technology service and deployment models trying to figure out how they operate and why it’s important to get familiar with those findings. Finally, it could be quite helpful to make a perspective on socio-economical impacts of this quite recent paradigm and provide some thoughts on the purpose of cloud-based systems in this modern time.

Key words: *cloud’s systems, technology, web, intelligence, security, etc.*

1. INTRODUCTION

The cloud’s computing has become one of the biggest IT paradigms of today. It would drag the attention of academic, expert’s and defense communities and make those groups put a lot of effort in order to better research, develop and understand such a concept. Dealing with the cloud’s technologies is a quite convenient and user-friendly experience and that sort of a system would offer us nearly limitless opportunities in terms of data storage and sharing. Many people would wonder why cloud matters nowadays and what it would make such a technology so useful in this modern time.

First, it’s important to say that the cloud’s concept would cope with so many web-based systems that would get correlated with some accounts offering an access to the environment that would give us a chance to upload there some helpful information, applications or even apply it as a developer’s surrounding. In other words, the cloud is a paradigm that would grow and grow in the future providing an opportunity to many industry’s leaders to make the good profit selling such a service.

One of the main challenges to the cloud’s solutions of today is their access control. Apparently, many experts would agree that the cloud’s security is still an open concern and the entire industry would work hard in order to figure out how such a problem could get tackled. Also, the cloud’s technology would deal with so many data centers that would include servers and another IT infrastructure and those resources would get vulnerable to the hacker’s attacks, breaches and operations. On the other hand, the cloud’s solutions are quite handy, because they can store so many data for a quite reasonable cost. In addition, there is an opportunity to combine some of the cloud’s capabilities and make such a technology being pretty convenient in many ways. For instance, it’s possible to configure the optimal solution for your organization that would offer you a chance to cope with the quite secure and cost-effective option.

Finally, we should mention that there is still a huge risk being supported from the criminal underground and it’s about the privileges sharing. As everyone would realize, the cloud’s accounts could get easily approached using the login details such as username and password. In such a case, it’s quite clear that so many actors could share the same account without any owner’s permission. That scenario would open on so many alternatives to the malicious actors to threaten the resources of both – civilians and defense community. Through this effort, we would also talk how critical information could get protected in the cloud’s

Author’s address: Milica Đekić, Subotica, Vase Pelagića 39a

e-mail: milicadjekic82@gmail.com

Paper received: 02.03.2018.

Paper accepted: 22.03.2018.

environment and try to explain why it's significant to manage the risk within the cloud's systems. At this stage, we cannot suggest that we deal with the absolute security, but rather with the weak or strong assurance. That's practically the case with the entire IT sector and right here, the cloud's concept is not an exemption. In a summary, the main question of this article is the cloud's computing security and we would mostly concentrate on so, while some other topics would get discussed further as well.

2. THE CLOUD'S MODELS

The cloud's computing would start developing more than a decade back and right now, that technology would get widely accepted. As any computing paradigm – it would deal with its basic models that could – in some cases – get combined in order to provide the best feasible outcome. The cloud's systems could get distinguished based on their way of content storage and according to the user's experience they cope with. In such a case, we can suggest that there are two fundamental sorts of cloud's models. First, we would pay some attention to the cloud's deployment models and second, we would attempt to talk a bit more about the cloud's service opportunities. As it's quite obvious through the previous discussion – the cloud's deployment models would get linked with the cloud's storage capacities, while the cloud's service models would correspond with the end user's experience.

At this point, let's begin with the cloud's deployment models. As we've indicated before, these solutions would deal with some cloud's storage capabilities. In a practice, there are two basic ways to store some content – inside some organization and outside so. The third approach would be the combination of those two and in many practical usages – it would find its place in practice. What we would try to suggest here is that the cloud's deployment models could include three variations of content storage capacities and they are (1) public, (2) private and (3) hybrid clouds. [1, 2] The public cloud's model would mean that the data, information and applications got saved outside of the organization and they would mainly rely on IT resources of some big company that would sell the memory space and processing power to its clients. Some researchers would argue that those solutions got less secure, but that's quite questionable for a reason the experiences would be diverse. Also, many people would believe that the public cloud got more cost-effective than any other cloud's solutions. This also could run a debate, because everything would depend from case to case. Second, we would mention the private cloud as a way of storing the resources within the organization. Some literature would suggest that this is more secure and less cost-effective way of saving the content. Finally, it's important to mention the hybrid cloud being the combination of the previous two options. In that case, less sensitive data would get saved within the public infrastructure, while the more sensitive storage would get put into the private asset. Also, it's significant to say that the cloud's content would be saved in data centers covering on servers and some IT infrastructures and dealing with the well-developed disaster recovering and backup procedures and policies. The illustration of the main cloud's deployment models is shown in a Figure 1 as follows.

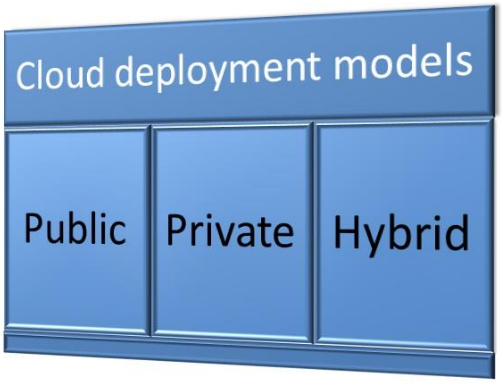

Figure 1 - The cloud's deployment models

Next, we would continue to explain what the cloud's service models are, how they work and what their usages could be. The quite basic way to introduce the cloud's web delivery models is to say they could be (1) Software as a Service or SaaS, (2) Platform as a Service or PaaS and (3) Infrastructure as a Service or IaaS. Let's start with the SaaS!

The SaaS model would allow the end users deal with the software being brought to them through their web browser. It's quite clear that we would talk about the web-based solutions such as social media, e-mail services, task management software and so on.

This sort of advancements would get useful to the end clients who would have their user's accounts being more or less protected there. On the other hand, the PaaS would be so handy environment for developers who would work on their projects in the web-based surrounding. [4, 5] The main limitation of this option would be that it would support only restricted number of programming languages and tools and it would not let developers downloading their efforts on any computer.

At the end, we would mention the IaaS solutions letting you make the infrastructure out of your web browser. The main advantage of these systems is that they would offer you a chance to upload any application to that surrounding and use it and in such a case, those solutions would be so suitable to the system administrators. The graphical representation of these cloud's models is given in a Figure 2 as follows.

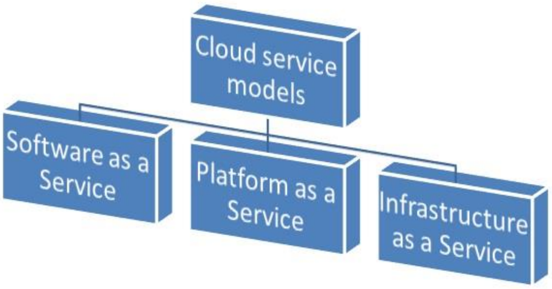

Figure 2 - The cloud's service models

In order to recapitulate this section, we would say that these two basic cloud's models are only as their attribute would suggest – so fundamentals ones. The experience shows that there are much more variations of these opportunities – but, at this level, we wanted to illustrate some most used solutions. The literature would suggest that, for instance, there is the serverless cloud that would rely on the Function as a Service or FaaS concept and such a solution would offer the amazing alternatives to the developers. Right here, we would not talk about the other cloud's options – because that would be outside of the scope to this effort.

Finally, it's important to know that the cloud's computing is so fast-growing marketplace that would seek from the researchers, experts and scientists to constantly cope with its new trends and tendencies in order to make that field getting deeply convenient to everyone. The ultimate imperative to any technological advancement is a progress and sometimes it's not that easyto handle all those changes the time is bringing on.

3. HOW THIS TECHNOLOGY WORKS

The best method to describe how the cloud's technology works is through some graphical illustration. Before we do so, we would try to deal with some pre-knowledge of how internet communications work. It's well known that the cloud's systems are only data centers communicating with the clients. The cloud's computing would use the quite usual encryption simply being provided with your web browser. So, we would talk about server-client communications. On its way through, the servers and clients would cope with so many routers. The routers are devices that would get their IP addresses and manage the web traffic via the certain route. [3] The path your network devices would choose depends on their operating system configurations. The client would send its request to the server and that packet of information would go through the network of routers. For instance, the client would send the packet to the first router which would also get the TTL or Time-To-Live signal. Going to another router that TTL value would get decremented. If the value of TTL signal is 0 – the entire packet would get terminated by some router and the server would never get such a message being delivered. On the other hand, the response to any TTL signal would be an ICMP message or Internet Control Messaging Protocol. The purpose of that signal is to provide the response to any TTL input and signalize if the next member of the network is available to the communications. Some basic diagram how the cloud's communications appear is given in a Figure 3 as follows. The drawing is done applying the CADE computing tool.

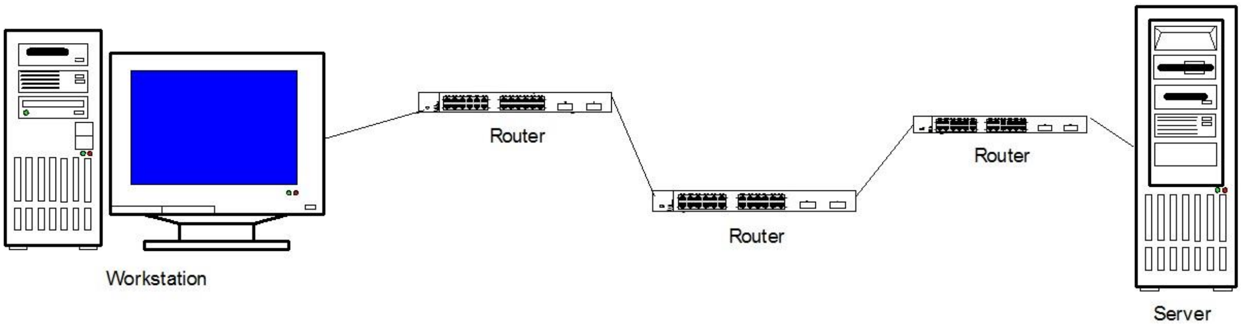

Figure 3 - How cloud works model

The Figure 3 would so clearly suggest how cloud's communications from workstation to server look like. We would strongly recommend to anyone coping with this effort to attempt to deal with the online trace route tools in order to figure out how we can get connected to some routers and finally to the server – all of them having some IP addresses. [1, 4] So, what we would notice here is that the cloud's computing systems would rely on three main parts being source as their data centers, transmission as their communications channels and destination as their client's devices. In other words, you would use the client to call some web location using your internet browser and such a call including the packet of information would go through the network of routing devices and apparently, come to the server. The server would respond to that request following the similar approach and you would get exactly what you want within your web browser.

At the end, it's important to mention that there is no any specific cryptography being applied to the cloud's systems. This would open up the big question how to assure our cloud's communications in some way. So commonly, the cloud's technologies would deal with the encryption being provided through the web browsers they use to appear on the client's machine. For such a reason, we would want to appeal on all industry leaders to try to think about somehow secured cloud's information transfer, because that part of the cloud's systems could be its gravest weakness. Finally, this could be the challenge for tomorrow to many defense and intelligence agencies because they would also so frequently use at least the SaaS cloud's solutions.

4. THE CLOUD'S SECURITY

If we talk about the cloud's security – we should try to get that there are three main segments being critical in such a manner. They are client, network communications and data center defense. For example, many hackers' groups would obtain the access details of some cloud's account and try to exploit such an environment. For that purpose, we would suggest the better access control which is already the tendency within some cloud's solutions. Also, there is a concern that some cloud's internet traffic could get hacked. [2, 5] This is quite alarming getting into consideration that so many sensitive information could get exchanged between the server and clients. Above all, the data centers are also not immune on cyber attacks and they normally cope with the good security practice. Finally, we would find some recommendations in the literature suggesting that if we still need to deal with the unreliable access control – we should try to encrypt our contents and upload them to the cloud's environment as so.

5. THE ROLE OF A CLOUD TODAY

The cloud's computing has changed the modern private and business landscapes in so many ways. This new technology also brings a lot of advantages to the societies and economies worldwide. It's quite profitable investing into that technological area, because the returns are so promising. The quite helpful stuff with the cloud's computing is that this solution can store a large amount of data, information and applications and get available to multiple users relying on its network's communications. The significant disadvantage of this technology is still the security and the tendency would suggest that such a concern would get bridged in the coming years.

6. DISCUSSIONS

As it's known, the emerging technologies have made the entire human society being dependable on them. That's the case with the cloud's computing solutions, too. The cloud is still the recent paradigm and many experts would agree that it will keep developing as time goes on.

On the other hand, as we are getting so dependable on the new advancements – there will be the rising question how secure we could be relying on all those improvements. This is the open concern and the big challenge for tomorrow that will need a lot of time, effort and resources to get handled.

7. CONCLUSION

The purpose of this effort has been to illustrate some basic concept of the cloud's computing as well as provide some insights about its security. In our opinion, this paper could get used as a good starting point for the further research.

Finally, the cloud's technologies cover the quite wide area and our contribution would capture only a symbolic segment of that huge field.

REFERENCES

[1] Behl A, Emerging Security Challenges in Cloud Computing, *IEEE*, being available with IEEE database, 2011.

[2] Bouayad A, Blilat A, Mejhed N, El Ghazi M, Cloud computing: security challenges, *IEEE*, being available with IEEE database, 2012.

[3] Kandukuri B, Paturi R, Rakshit A, *Cloud Security Issues*, 2009 *IEEE International Conference on Services Computing*, being available with IEEE database, 2009.

[4] Lenkala S, Shetty S, Xiong K, Security Risk Assessment of Cloud Carrier, 2013 *13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing*, being available with IEEE database, 2013.

[5] Shaikh F, Haider S, Security Threats in Cloud Computing, *6th International Conference on Internet Technology and Secured Transactions*, 11-14 December 2011, Abu Dhabi, United Arab Emirates, being available with IEEE database, 2011.

REZIME

BEZBEDNOST CLOUD RAČUNARSTVA

Nove tehnologije se masovno usvajaju širom sveta i pronalaze svoje primene kako u privatnom, tako i u javnom sektoru. Jedno od dobro poznatih tehnoloških dostignuća koje se koristi danas je cloud računarstvo. Ovaj vid sistema je još uvek u svom razvoju i svakodnevno se susrećemo sa novim poboljšanjima u toj oblasti IT industrije. Glavni izazov za većinu novih tehnologija uključujući i cloud računarstvo je još uvek njihova bezbednost. Uloga ovog članka je da predstavi sveobuhvatnu diskusiju kako cloud rešenja funkcionišu, koji su ključni faktori u njihovoj bezbednosti i kako bismo mogli da unapredimo korisničko iskustvo primenjujući ove sisteme. Takođe, pretrešćemo neke cloud modele za uslugu i podršku nastojeći da shvatimo kako oni rade i zašto je bitno znati to o njima. Konačno, bilo bi prilično od pomoći da spomenemo društveno-ekonomske posledice ove krajnje skorije paradigme i razmotrimo svrhu cloud sistema u svaremenom dobu.

Ključne reči: *cloud sistemi, tehnologija, web, saznanja, bezbednost, itd.*