Cloud technology: opportunities for cybercriminals and security challenges

by Leo Santoso

Submission date: 13-Aug-2019 04:55PM (UTC+0700)
Submission ID: 1159804894
File name: Camera_Ready_Ubi-Media_2019.pdf (258.2K)
Word count: 6412
Character count: 33160

2019 Twelfth International Conference on Ubi-Media Computing (Ubi-Media)

Cloud Technology: Opportunities for Cybercriminals and Security Challenges

Leo Willyanto Santoso
Informatics Department
Petra Christian University
Surabaya, Indonesia
leow@petra.ac.id

***Abstract*—Nowadays, there is a growing of interest about cloud technology to many companies around the world. That's why many companies trying and implementing cloud computing technologies in their business processes. This research will examine the security requirements that will apply for companies and organizations when they choose to move to a cloud service solution. The study is carried out because cloud services are very desirable in many industries today. Migrating to cloud services would often results in great benefits both financially and administratively. The concerns raised by the transition are how security should be handled. Many companies suffer from a lack of knowledge and it is seen as a big risk to make the transition. This leads to the question that the research strive to answer - which security demands will the transition to a cloud service implicate? In this paper we explain which security requirements are available both for local solutions and cloud solutions. We draw conclusions about what differences there are, what requirements are mutual, which ones are new and which ones are absent if a transition is made to cloud services. The result of this research is an evaluation that companies and organizations can use as a basis when they plan to implement this particular transition.**

Keywords— cloud, cloud technology, transitions, security

I. INTRODUCTION

Cloud services are something new and up to date on the corporate sky, as it brings many advantages to most companies and organizations that today have some kind of local solution to their data management [1]. A big advantage of using cloud services instead of storing data locally is that everything is stored dynamically, which means that companies and organizations do not have to pay for more space than they actually use, which is very cost effective compared to handling it at a local level. Using local solution requires the company to know exactly how much space they need at the present time and also how much they will need for several years to come.

A large number of companies agree that cloud services are the future and want to implement it as quickly as possible in their operations [1]. The problems encountered by many stakeholders in cloud services today are how they will work to achieve the same level of security in today's local solutions [2]. Major ignorance and uncertainty prevail, of which many companies and organizations see this as an excessive risk of switching to cloud services [2]. This causes them to lose sight of the improvements that the transition can result in.

Cloud services offer functionality that a local solution can not provide [3]. Companies are constantly striving to expand and the elasticity offered by cloud services means that companies do not have to expose themselves to the same financial risk as they plan to provide a service to their customers [3]. The general concern is based on the ignorance of what this means for safety. Some parties claim that security is improving and other parties claim the opposite.

With the progress made in the development of cloud services and what they can offer companies that see opportunities in choosing a cloud service instead of a local solution, there are several security issues that have been added [2]. This is no new phenomenon regarding the development of IT services over the years.

Cloud services are something that is relatively new in the market and there is a skepticism towards security that is justified. However, cloud services also offer the opportunity to structure security in such a way that it can deal with the unprecedented disorder. The effort lies in creating a solid material as a basis for safety. Based on this, arguments can be made that if resources are invested in security, it may also be as attractive as the functionality cloud services offer today to companies and organizations.

Media reporting on cloud services is often very simplified and unilateral in its execution, which affects public opinion in a negative sense. Companies and organizations that have an interest in choosing a cloud service as a solution are no exceptions to this. The benefits of choosing a cloud service can be seen as very positive in terms of operating profit, which causes the security aspect to end up in the dark when reporting cloud services.

The purpose of this research is to identify which security differences exist between local solutions and cloud services, and then identify what security requirements the reader needs to take into account when switching to cloud service. This study can be used as a basis for companies and organizations that are interested in cloud services in general and just the transition in particular.

The aim of this research is to clarify the safety requirements and aspects that companies need to take into account when switching to cloud services. It will serve as a basis for companies and organizations when they consider shifting to a cloud service. This paper should also serve as a source of information for people with general concerns about how safety changes in a transition to cloud service from a local solution.

The method that the paper follows to achieve the result is inductive. This means that the work begins with an observation and study phase. Then the next step follows identifying patterns found in the observations made, which are then used to draw conclusions and answer the problem formulation contained in the paper. The engineering-related

978-1-7281-2820-7/19/$31.00 ©2019 IEEE
DOI 10.1109/Ubi-Media.2019.00013

methodology is based on the pattern mentioned above and is designed to model how architectural safety aspects are designed for local solutions in relation to cloud services. From this we can also identify similarities and differences, where there are differences that give the answer to the problem. This results in a clear overview for the reader about the current relationship.

The remaining part of this paper is organized as follows. Section 2 presents the background and the related work. Sections 3 presents the examination of computer security and information security. Section 4 presents the discussion and analysis. Finally, the conclusions are drawn in Section 5.

II. Literature Study

The cloud services offered to local solutions are that instead of the user being required for maintenance and operation of servers, it will be managed by an external supplier [3]. This means that the supplier is responsible for everything stored in the cloud and also the operation, and the company does not need to have IT experts because it is managed by the cloud supplier.

Cloud services for companies are a change in how the infrastructure is designed as they transition from having stored data locally to hire a supplier who manages all storage and provides as much space as requested by the company [3, 4]. Many companies and organizations regard it as attractive to be able to use the cloud service architecture to transfer hardware and storage management to a cloud supplier. In this way, the company or organization avoids the investment risk that a local solution would cause, and instead, they only pay for the resources actually utilized by the cloud supplier.

A. Cloud Service Model

There are three models for cloud service can offer to customers or users by cloud provider [5]. Each of these models offers its own pros and cons. The choice of model depends on the needs the company or organization has and which model best suits these needs. The potential gain of switching to cloud service is directly linked to the type of model that suits the company or organization. The three different models affect the safety to a varying extent, one model can be very beneficial while another can directly complicate safety. Using cloud services may also cause problems as it is unlikely that competing companies or organizations are using the same cloud [6]. Below is a description of the standard models. There are also hybrid models that are a combination of two or more of the following models.

A local cloud means that it is only a company or organization that uses the cloud and its cloud services [5]. In order for it to be beneficial with a local cloud, the company or organization needs to be in need of large computer resources, as the benefits that cloud services offer come with handling large volumes of data. One reason for choosing a local cloud model is the safety. Securing a local cloud is advantageous in the sense that the company or organization can design the cloud architecture just after their security needs. For military (such as the Armed Forces) or other organizations with very strict security and integrity requirements, this model is preferred.

Common clouds are the model where a group of companies or organizations with similar needs use the same cloud [5]. This model is advantageous in that a cloud supplier can develop his cloud against a group of companies and organizations that share the same needs. In this way cloud service can be developed according to these needs, and it will be profitable for companies and organizations to choose a cloud solution instead of a local solution.

A public cloud is the model where the cloud is open to the public, it is a cloud supplier who offers a cloud service to anyone in principle [5]. Services developed in public clouds aim to reach as many people as possible. The security of a public cloud does not in itself need to be more problematic than in other solutions, but it implies a certain addition of complexity, since users of the service can be basically anyone. Public clouds are a model that fits companies or organizations that do not necessarily seek specific security solutions from the cloud provider, but rather they seek the dynamic and flexible allocation of Cloud Services. However, this does not mean that security is neglected in a public cloud.

B. Security in Cloud Service

Cloud services provide the impression that there are endless resources in such a way that if more resources are needed, they are automatically assigned. The user thus has no control or insight into how this happens and never needs to handle this aspect. This is primarily done by virtualization using virtual machines; an alternate word for cloud service might be virtual data center. The resources of a cloud provider are shared with virtual machines, ie, a resource consists of multiple virtual machines, and when a user needs increased resources, it is assigned to the user by accessing multiple virtual machines. This means that multiple users can be placed on the same hardware at the same time.

When data structures are abstracted for companies or organizations, a dilemma arises which can be used as a basis for doubt about the security of cloud services. However, it can be seen as positive to transfer the distribution of hardware to a cloud supplier but negatively to transfer control of security. Control over security is no longer controlled at a local level at each company. It is instead managed centrally by experts from the cloud service provider, which in turn takes care of many companies using similar types of cloud solutions. If you consider it over time, it can lead to more stable and better security as experts' knowledge increases and several companies use similar solutions, as it is in the interests of both parties to maximize their security.

The repetitive nature of cloud services is the basis for designing a security structure that is sought. This means that when resources are allocated in a cloud architecture, it happens dynamically without any manual interaction, in contrast to how this is normally managed in a local solution, where a system administrator usually manages this manually.

This has mostly positive effects, but it can also be negative. Considering it from an economic point of view, it is positive in the sense that it does not require as much staff as the process becomes much larger extensively automated. Only a few people can handle large volumes of data architecture. What this means for security is that, as mentioned above, it becomes a centralization of expertise and that in a certain sense it becomes easier to design good security about repeat processes, unlike when events occur randomly and unpredictably. However, it is important to be aware that new cybercrime opportunities can occur, as there is a change in architecture when the system administrator is replaced by software to perform these processes. Another possible scenario is that if the cloud service provider is subjected to any

malfunction or other type of problem that causes the service to malfunction, since the companies do not have the control that at a local solution, they need to rely on that the supplier solves it as quickly as possible. There are also risks that if several companies rely on similar solutions that are physically located in the same server hall at the supplier, as companies can not control and review how the other companies load the supplier's servers. Another risk is if any page-side attacks occur [6].

With the development of cloud services, cloud providers are offered the opportunity to develop their own security solutions [7]. Proposed in the form of security modules that are developed and subsequently offered to customers with the cloud supplier as a service, such as authorization. Many customers, as needed, have to perform authorization for some form of login to their services located with the cloud provider. Instead of each company developing its own authorization process, the cloud provider can provide its customers with this functionality in the cloud service. In this way, the supplier can develop an authorization service, which can then be used by customers as a module if they are in need of authorization, that is, security as a service in the cloud.

III. Examinations of Computer Security and Information Security

This chapter describes the various security aspects that exist and how they affect local solutions and, above all, cloud services. The model presented is divided into two parts, one for information security and the other deals with computer security, where the components contain the various security aspects relevant to each area.

Below is illustrated how the construction of a local solution or cloud service can be designed, see Figures 1 and Figures 2.

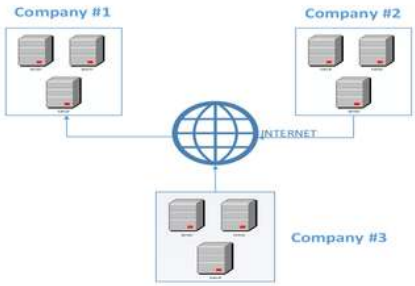

Fig. 1. Illustration of how a local solution can be built

A. Information Security

There are several aspects in information security, namely: integrity, availability, authenticity and non-repudiation.

Integrity is about maintaining and ensuring that data stored remains the same throughout its life span [8]. In particular, it means that the information stored can not be destroyed or altered by mistake, and protect it from users who do not have rights to access the information. To protect and preserve the information, there are different variants of encryption used. A current issue for companies and organizations wishing to transition to a cloud service is the integrity of the data stored, as they lose control over it [9]. This places high demands on the cloud service provider to keep this data intact. The impact of lost integrity in cloud services has more impact than in a local solution, as it means that more companies and organizations operating in the same cloud are also exposed to the attack.

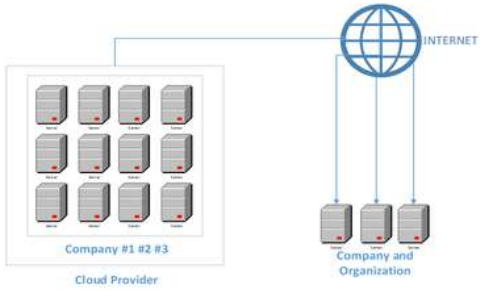

Fig. 2. Illustration of how a cloud service can be built up for example

Availability is that the information is available to the user in a timely and continuous manner [10]. This implies that high demands are made on the cloud supplier to provide customers with good performance in security, infrastructure and networks. Availability is nothing that sets any special requirements for a cloud service versus local solution, but these are no matter what solution is used, which focuses on the information being always available to the user [11].

Authenticity is about verifying that the user is the person it claims to be [10]. This protects the system from incorrect information being stored, which could compromise system security. In order to maintain the security of the system, it is important that users are what it claims to be and that unauthorized persons use the system to intro-duce malicious software or create security risks. As mentioned above, the requirements are the same regardless of which solution is used, where the focus is on the user being the person it claims to be [12].

Non-repudiation means there is an assurance that messages and data sent be-tween two parties are delivered and received correctly. This is based on the sender's ability to verify that the recipient has received the message and vice versa, that is, the recipient can verify that the sender has sent the message. This can be accomplished with tools already designed, such as digital signatures, time stamps and "confirmation receipt services".

B. Issues in Information Security

The following is a statement about computer safety aspects. Here are various types of attacks and attack strategies presented.

Backdoor is when an unauthorized person can access system or sensitive information by avoiding the intended security protocols. Software developers often create their own "backdoors" to avoid long-term security protocols during the development stage of a software. The problem arises if this feature is not properly removed or the developers themselves are not aware of the potential risk they have introduced into the system, and if an outside unauthorized person accesses this particular backdoor. In cloud services, there's really no change as compared to a local solution when it comes to the problem of a so-called backdoor [12]. If an unauthorized person finds and uses a backdoor in a cloud service, it breaks the security protocol within just the virtual environment in which the software is located, ie it would result in the same consistency as in a local solution. All of this is counteracted during the

development stage of the software itself and does not concern the architecture of a cloud environment in a direct sense.

A denial of service attack (DoS), is performed via a system flooded by data traffic until the system can no longer handle data traffic and stops functioning properly. This is usually done on websites where people flood the website with requests to the server to send the page to a browser. This is done in massive amounts and eventually the server is unable to deliver the service. Distributed Denial of Service attacks (DDoS) follow the same concept, but with the addition that a network of computers is used to help complete the attack [13]. Which means more sources that help to flood the chosen target they attack. DDoS is also categorized under Indirect attacks. Which means that malicious software code is spread to multiple computers, which in turn are used to perform the DDoS attack, that is, a third party is used in the attack to achieve the target. The threat that consists of DoS strategies is something that is relevant to many industries today [14]. The threat is more serious for cloud services than for local solutions in two different sentences. Should the DoS or DDo attacks happen from a cloud environment, it would cause a lot of it potential computing power of the cloud supplier to exploit the attacks. This means, however, that those who perform the attack must manage to control more virtual machines with the cloud provider, which would normally happen through malicious software spread. Alternatively, the cloud service itself is the target of the attack, which would cause the effect to be much greater. Instead of affecting only the selected service being affected, the system of the cloud provider would be affected.

The concept of "eavesdropping", is a form of passive attack. This type of attack can be applied in different areas of computer security, but the concept is the same. The attack is considered passive in the sense that it is not an attack directly against the system it targets. Without it, the communication between users and the system in question is considered, then used to circumvent the security of the system applicable to the attack. This can be done by installing malicious software on a user's computer to record keystrokes and thus access passwords. Another way to perform this attack is to intercept data traffic sent from the user to the system and analyze this data to achieve the target of the attack.

The term "Exploit", means that attacks are taking place using specific weaknesses in the system. Often this is done through software developed solely for the purpose of exploiting a system weakness, such as "worms" or "viruses". System weaknesses may occur during the development stage of software used in the system. These are often very difficult to identify for developers as these weaknesses appear completely un-conscious in development. In order to counteract "Exploits", tests on the software are performed before it is deployed within a system, but it does not mean that the risk of "Exploits" is completely eliminated. This means, rather, that the risk of weaknesses in the system is minimized. Cloud architecture implies a certain complication for security officers with regard to "Exploits" when a potential target for this type of attack would be to target the "hypervisor" of the virtual environment. This means that the attack has the potential to affect all those customers of the cloud provider who share the same hardware as the virtual machine is located on. However, this can be avoided as much as possible by updating the software for the virtualization environment, as developers continually update the software to prevent incidents of this kind.

Direct access is when someone has direct access to the system and its hardware, allowing the unauthorized person to install different types of viruses and malware directly into the system [15]. The only way to protect the information against these types of attacks is to encrypt it. These attacks can be done through buffer overflow attacks and SQL injections [16]. To counteract this, a so-called Access Control System can be used which prevents users without rights from accessing the network and the system [17]. For example, if a user with unauthorized access accesses device configurations without having permission, then this user's login credentials will be blocked from accessing that device and other devices on the network. Because the user's login credentials are stored in an authentication server centrally, where all access is blocked when it is detected that the user has gained unauthorized access to any part of the system.

An alternative way to perform computer system attacks is by using "Social Engineering". This strategy is based on tricking people who use the system to install malicious software or share rights in the system to unauthorized users, usually to those who perform the attack. The strategy is to gain people's trust and often happens through the people who carry out the attack claiming to be something that it is not. They pretend to be an instance or source that people trust. Thus, for example, they may provide information or send to receive and install software that exposes the system of security risks.

This type of attack is aimed only at the user in a system and thus does not have a direct meaning with the system to do. There is no perspective to stand against each other when it comes to cloud service versus local solution. The security risks that a successful attack of this kind would result in is treated by other areas of this section such as "Backdoor" or "Exploit", as a successful attack results in the application of any of these techniques in connection with the attack.

IV. Discussion and Analysis

Many of the benefits that companies and organizations consider attractive with cloud services are based on the results of the molten services. It is not the actual virtualization that companies and organizations are interested in, but instead, for ex-ample, the elasticity and scalability that cloud services offer [18].

A. Virtual Machines and Virtualization

Whoever uses a cloud service experiences it as infinite resources in the system as the processes behind are automated and the user never needs to handle any of these functions himself. The result of these processes is by virtue of virtualization and using virtual machines [19]. Virtual machines are not themselves a security risk, but some security issues arise in their use of cloud services.

It is also possible to argue that the use of virtual machines allows for better security compared to local solutions. Virtualization made using virtual machines leads to the fact that cloud service users use the same hardware, and with this, new security aspects will arise, taking into account the fact that there are no local solutions. In a cloud service, however, the attacking party may be on the same computer as the party it is trying to attack. The virtual machines that users of a cloud service use are dynamically assigned, which complicates this further. This can be counteracted by tools that monitor virtual

machines, it is an aspect that a company or organization needs to be aware of when it plans to switch to a cloud solution.

B. Side Channel Attacks and Reverse Engineering

The fact that users use the same hardware also means that "Side Channel Attacks" are possible. This means that a user can access information about the system by utilizing something that is usually not interpreted as a security aspect, thus providing information that can be used to perform an attack. For example, users can measure the time it takes for the system to perform certain calculations and then use this information to design a strategy to attack the system. Memory of the hardware can be utilized to get information from other users on the same hardware. In such a situation, for example, caches of memory would be utilized to overcome information when users share the same physical memory modules and hence its caches.

The above also leads to additional aspects to consider as there may be competitors in the same industry that can use the same cloud service. This would mean that "side channel attacks" are not only relevant to the security of the system, but also for the integrity of users. This also follows the so-called reverse engineering, which means that a user analyzes the structure of a product and then exploits this information in order to harm a system or its users. In cloud services this brings additional problems. As mentioned earlier, users share the same hardware and there is a potential possibility that competitors within the same area of operation may use the same hardware. Reverse engineering can also be used to get information about its competitors in such a way that it could analyze the cloud service to gain insight into how a competitor uses cloud service, which in turn can be considered sensitive information.

C. Subsystems

The centralization of users and hardware that cloud services entail opens potential security solutions that could solve a lot in the aforementioned problem. A security solution would be to develop so-called sub systems, in the cloud architecture. Which means that the architecture is divided into smaller systems where security is developed for the smaller system in question. Thus, it would be possible to prevent, for example, "side channel attacks" by considering just the issues that such an attack involves and developing the subsystem to address this.

With subsystems, there is potential for developing security solutions that deliver a high security standard to customers. Multiple levels of security within cloud service can be developed that can be customized according to customers' different security needs. Which means that different parts of a cloud architecture can handle different security requirements to meet their customers' needs. This allows a cloud supplier to assure its customers that they are not affected by other customers who do not share the same security needs.

D. Isolation

Sharing a cloud architecture at different levels of security could be achieved through so-called "isolation". Something that also comes with virtualization in cloud services is that if an "Exploit" succeeds, there is a possibility to shut down the part of the sys-tem that is relevant to the security violation, thus cutting off other parts of the system from the incident. Which, in turn, causes as few users as possible to be affected by an incident. This is usually called "Defense in depths".

E. Hypervisor

Another area that comes from virtualization in a cloud service is that every virtual machine on the same hardware shares a hypervisor. Hypervisors are responsible for the communication between the various virtual machines and the hardware. So far, no one has managed to expose a hypervisor to a successful attack but this does not mean that it is impossible.

As interest in cloud services grows, the interest in attacking cloud services will in-crease and with that, hypervisors may be a potential target. Should an attack succeed against a hypervisor, it would pose a high security risk to users who use the hardware that the hypervisor is on. The effect would be that those who succeeded in the attack would have full access to the hardware subject to the attack and its software. With that, there are no restrictions on what a successful attack would result in except that it has potential to be of catastrophic effect to users and cloud providers.

F. Fate Sharing

An additional aspect that needs to be considered due to the fact that companies and potential competitors share hardware are so-called "fate sharing". Which means that if an attack succeeds in a cloud service company, other companies using the same cloud service may be affected by the attack. The term "fate sharing" can thus trans-late to those who use the same cloud service sharing fate.

G. Business Reputation

The various companies and organizations that use a cloud service need to protect their reputation. This means that the cloud supplier needs to develop an architecture that takes into account the views of the different companies and organizations. Issues like "Is it reasonable for a customer with low security requirements to share hardware with a customer who has high security requirements?", Even this can be linked to what was previously discussed in this section when the term "isolation" was treated. It's about minimizing the impact of a successful attack and being aware of what effects a successful attack might involve for other customers and their companies that use the cloud service.

H. Distribution of Debt (Attribution of Blame)

The term "attribution of blame" or "distribution of debt", that is, if an attack succeeds, it should be possible to read which company or organization the attack is being conducted against. This includes even if the company or organization has no responsibility for any security risks or contributed to the attack, which means that companies and organizations that have adhered to the security requirements will not be retracted into the problem of who may accused of carrying out the attack. That it is possible to find out who is responsible for what can help for example authorities if there has been illegal activity in the cloud supplier's architecture. Other companies and organizations do not have to suffer if authorities seize hardware that is involved in illegal activities and that these authorities do not exceed their powers when investigating the situation.

I. Mutual Auditability

An advantage that companies and organizations use cloud services, and thus share resources and hardware, is that there is the possibility of performing mutual auditability. It means that if an attack is being made against the cloud supplier or any of its customers and any weaknesses in the system can be

detected through this attack. These weaknesses can then be solved and security improved for all customers in the cloud service. It can also mean that in an attack there is the possibility of an effective response or a recovery for the attack, as the cloud supplier has control over the entire architecture and its customer's software located on the hardware.

J. Botnets

Finally, the problem of so-called "botnets" needs to be addressed. When using a network of computers, in this context the cloud architecture, to perform DDoS attacks, it is commonly referred to as the "Botnets". With the architecture that cloud services mean, there are many resources to help with and potentially use this architecture to perform DDoS attacks. This means that those who perform a DDoS attack would hire themselves as customers at the cloud supplier to access these resources. However, this option is considered a costly way of performing this kind of attack and not particularly attractive to people who want to carry out the attack. Additionally, it is very easy for a cloud provider to shut down parts of the system if they find that it was used to carry out attacks.

V. Conclusion and Future Works

As cloud technology evolves, attack strategies against cloud services will also be developed. This is something that is very difficult to prepare as it becomes paradoxical to develop security when security attack attacks often look for new ways to get around or break through security. Since all the material underlying the essay is based on previous history of safety, it is crucial to understand this in the context. The result of the essay can not take into account what can change in the future, that is, it is possible that new methods of attack against cloud services are developed that are not covered by the content of this paper. As cloud services are becoming more and more current on the market, this phenomenon is not only possible but also likely.

After completing, studying and analyzing cloud services and the security issues that come with it, we can see that the benefits offered by cloud services absolutely warrant that companies should switch from local solution if they ignore economic aspects and speak in a general sense.

The security issue is not significantly different from that already in local solutions; there are still similar types of attacks that already affect local solutions in many cases. However, it should be mentioned that the question of safety exists and they need to be corrected. What we think is that over time, cloud services will be an even safer alternative than local solutions, precisely because the expertise is centralized and that it is investing very much from many different directions on cloud services in general. As many have already been in the articles we read - cloud services are the future. The reason for this is based on three factors: Dynamic allocation of resources, Centralized expertise, and Always available, only internet connection required.

However, for most companies and organizations, it is the economy and money that governs and it is often necessary for a transition to cloud service to be economically viable for the transition to become reality. There we recommend companies and organizations to calculate what a transition would mean purely financially, and to review what needs are and whether cloud services are justified or not. On the other hand, if it is a newly established company that stands and choose between the type of solution to be used for, then the recommendation for the most people choose a cloud service solution.

References

[1] A.T. Velte, T.J. Velte, and R. Elsenpeter, Cloud Computing – A practical approach. McGraw-Hill, USA, 2009.

[2] V. Winkler, Securing the Cloud – Cloud Computing Security, Techniques and Tactics. Wal-tham: Syngress, 2011.

[3] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communications of The ACM, vol. 53(4), April 2010, pp. 50-58.

[4] A. Atayero, and O. Feyisetan, "Security issues in cloud computing: the potentials of homomorphic encryption," Journal of Emerging Trends in Computing and Information Sciences, vol. 2(10), Oct. 2011, pp. 546-552.

[5] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Generation Computer Systems, vol. 25, June 2009, pp. 599–616.

[6] Y. Chen, V. Paxson, and R. Katz, "What's New About Cloud Computing Security?" Homepage, http://www2.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf, last accessed 2018/11/10.

[7] J. Han, W. Susilo, and Y, Mu, "Identity-based data storage in cloud computing," Future Generation Computer Systems, vol. 29, March 2013, pp. 673–681.

[8] G. Sivathanu, C. Wright, and E. Zadok, "Ensuring data integrity in storage: techniques and applications," Proc. ACM workshop on Storage security and survivability (StorageSS '05), Nov. 2005, pp. 26-36.

[9] R. Kumar, and A. Saxena, "Data integrity proofs in cloud storage," Proc. Third International Conference on Communication Systems and Networks (COMSNETS 2011), 2011, pp. 1-4.

[10] W. Stallings, and B. Lawrie, Computer Security Principles and Practice. 3rd Edition, New Jersey: Pearson Education, Inc., 2012.

[11] A. Agarwal, and A. Agarwal, "The security risks associated with cloud computing," International Journal of Computer Applications in Engineering Sciences, vol. 1, 2011, pp. 257-259.

[12] S. Xue, W. Liu, Y. Peng, and P. You, "Security issues and solutions in cloud computing," Proc. 32nd International Conference on Distributed Computing Systems Workshops, June 2012, pp. 573-577.

[13] W. Dou, Q. Chen, and J. Chen, "A confidence-based filtering method for DDoS attack defense in cloud environment," Future Generation Computer Systems, vol. 29, Sept. 2013, pp. 1838–1850.

[14] G. Oikonomou, J. Mirkovic, P. Reiher, and M. Robinson, "A framework for a collaborative DDoS Defense," Proc. 22nd Annual Computer Security Applications Conference (ACSAC '06), Dec. 2006, pp. 33-42, doi: 10.1109/ACSAC.2006.5.

[15] E. Amoroso, Cyber Attacks – Protecting National Security. Burlington: Butterworth-Heinemann, 2012.

[16] W. Halfond, and A. Orso, "AMNESIA: Analysis and Monitoring for NEutralizing SQL-Injection Attacks," Proc. 20th IEEE/ACM international conference on automated software engineering (ASE '05), Nov. 2005, pp. 174-183.

[17] A. Emam, "Additional Authentication and Authorization using Registered Email-ID for Cloud Computing," International Journal of Soft Computing and Engineering, vol. 3(2), May 2013, pp. 110-113.

[18] S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud computing — The business perspective," Decision Support Systems, vol. 51, April 2011, pp. 176–189.

[19] W. Voorsluys, J. Broberg, and R. Buyya, "Introduction to Cloud Computing" In: R. Buyya, J. Broberg, A. Goscinski, (eds.) Cloud Computing: Principles and Paradigms, pp. 1-41. John Wiley & Sons, Inc., 2011.

Cloud technology: opportunities for cybercriminals and security challenges

ORIGINALITY REPORT

2%	1%	1%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	scitepress.org Internet Source	<1%
2	Submitted to Middlesex University Student Paper	<1%
3	Leo Willyanto Santoso. "Early Warning System for Academic using Data Mining", 2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA), 2018 Publication	<1%
4	www.klientsolutech.com Internet Source	<1%
5	Lecture Notes of the Institute for Computer Sciences Social Informatics and Telecommunications Engineering, 2013. Publication	<1%
6	K Raja, Sabibullah Mohamed Hanifa. "Bigdata Driven Cloud Security: A Survey", IOP Conference Series: Materials Science and	<1%

	Engineering, 2017 Publication	
7	Submitted to Arizona State University Student Paper	<1%
8	dl.acm.org Internet Source	<1%
9	www.iaeng.org Internet Source	<1%
10	www.icsd.aegean.gr Internet Source	<1%
11	Submitted to British University in Egypt Student Paper	<1%
12	dro.deakin.edu.au Internet Source	<1%
13	Submitted to University of Bradford Student Paper	<1%
14	www.ijcsi.org Internet Source	<1%

Exclude quotes	On	Exclude matches	< 5 words
Exclude bibliography	On		