SECURITY ISSUES AND CHALLENGES IN CLOUD COMPUTING

[1]Muthu Dayalan
[1]Senior Software Developer & Researcher
[1]Chennai & TamilNadu

Abstract— Cloud computing are the modern way of staring data and other important resources the company wants to retrieve safely and conveniently. It offers an innovative way of investment especially to start up enterprises and adopt IT operations without high upfront costs. Despite its potential, cloud computing is affected by various security issues. These include account highjacking, data breaches, malware injection, data recovery, wicked inside attackers, segregation of data, lack of investigative support, and shared vulnerabilities. The challenges facing cloud computing include security and privacy, application issues, accessibility, continuous evolvement, interoperability issues, service level agreements and data center issues.

Keywords: cloud computing, security issues, data, malware

INTRODUCTION

Cloud computing is a revolutionary way of storing data and application software by allowing a third party to host the storage device for all the data and application [22]. The new technology has allowed accessing of one's data and resources from anywhere in the world by just a connection to the internet. From individuals to large corporations, cloud computing are the modern way of storing data and other important resources the company wants to retrieve safely and conveniently. Cloud computing has offered an innovative way of investment especially to start up enterprises; the can now adopt IT operations without high upfront costs. The innovation also other great advantages such as high flexibility and scalability, resilience and allows organizations to outsource activities that do not form their core business. Large corporations such as s Amazon, Microsoft’s ‘Azure,' ‘Dropbox,' IBM, Apple’s ‘iCloud,' Google’s applications are the major companies in the provision of cloud computing services though there exit smaller companies that are also in this business [17]. However, despite the many potential advantages highlighted by this technology, many companies are still hesitant to adopt. The issue of handing personal and important data to third party is a sensitive issue, especially in matters of security[23]. This paper contains a detailed discussion of the challenges and security issues that surround the cloud computing technology.

SECURITY ISSUES AFFECTING CLOUD COMPUTING

Account High Jacking

There are different ways through which attackers use to accesses cloud accounts. Some of these are the use of reused passwords, which they try to different customers account until they open them [6]. Further, cloud account hijackers have developed skills that enable them to use a person’s login information to access any data that has been stored in the cloud. Other methods are scripts bugs, which also allow them to gain access to clients’ accounts [1]. With these methods, the cloud attackers can get critical information of a company or individuals from the clouds without being detected. They can also expose sensitive information or data concerning a company or an individual.

Data Breaches

Data breaching is a situation where stored data is stolen by unauthorized persons and used in an unauthorized manner. Data breaching is usually believed to take place mainly on other computing services and data storages [2]. Cloud computing has been being perceived to be a new service provider which is much secure from this data security threat. However, it has not been exempted from data breaching [7]. It is believed from a survey that data breaching in cloud computing is likely to occur three times compared to other computing service making it even more insecure for critical data and information storage [3].

Malware Injection

Just like other computing service providers, cloud computing is also affected by malware injections. These are embedded codes that are usually made to behave as software services. They are then injected in the cloud servers such that they are seen to operate as part of the cloud soft wares [9]. When these take place, attackers of the cloud data can access critical information or interfere with data stored in the clouds. These lead to the compromise of the integrity of any information stored in the clouds. Malware injection is one of the major security threats as most consumers may not have full knowledge of the genuine software being used and leads to most stored data being at risk of being compromised with by attackers.

Data Recovery

One of the main plans in any running businesses is to recover any data in case of a data loss. One of the major issues that affect cloud computing is recovering data in case of a breakdown. Usually, data stored in the clouds is usually not shareable to a third party [11]. As a result, in case of a breakdown, these data may not be recovered leading to loss of critical information. Recoverability may also be hindered by data being subjected to a virus by attackers or being high jacked.

Wicked Inside Attackers

Another major issue affecting cloud computing is the attack of data by insiders. The fact that the service providers are more exposed to the information makes cloud-stored data and information more prone to wicked inside attackers [16]. In most cases, consumers of the cloud services usually do not have clear information about these service providers as well as their procedures and policies. This can give room to wicked attackers to access the consumers' information unauthorized and never be held responsible. This ends up lowering the integrity over which consumers of cloud services may have.

Segregation of data

In the clouds, a lot of data, as well as information from various consumers, are stored. The data is so much that it is usually stored in such a manner that it is in a shared environment [8]. This means that each consumer has to secure their information to avoid cases of mixing with one from other consumers. One of the main ways through which data is secured is through encryption. This method of data security has not been fully effective and has led to the interference of consumers' cloud-stored information, as separating consumers' data from the unwanted information may be difficult. Additionally, in case of separation, some information may end up being exposed to unauthorized persons.

Lack of investigative support

Cloud service providers are usually not known to their customers. Consumers believe and build trust in the services that they provide [18]. Like in other case, consumers may not be able to carry out investigations on the service providers in case of an issue. Further, due to the huge data, a single host may not hold it all hence, some are distributed to other hosts as well as other non-constant data centers. This means that in case data has been compromised, a consumer may not be in a position carry out investigations on any particular server.

Shared vulnerabilities

The security of any data stored in the clouds depends on both the provider and the customers. This makes it difficult to hold any of them fully responsible [13]. It, therefore, requires the customer to take more care of their data even though the provider of the cloud services is providing security but the main business is to the client.

CHALLENGES AFFECTING CLOUD COMPUTING

Security and privacy

Security of information and data is usually a major concern for both individuals and companies especially on issues of technology. Most companies are wary of their trade secrets being accessed by their competitors and other malicious people [14]. In the cloud, computing security and privacy is a major challenge, especially where computing models such as Software-as-a-service (SaaS) cloud models are being used. This is because the organizations sometimes subcontract other service providers for backups which is a major concern for the privacy of the data. Additionally, SaaS compliance processes are believed to be difficult as data is usually kept in their datacenters and the service provider enforces regulatory issues. Consumers may have to comply with the enforced regulations for the security of their data to be guaranteed.

Application issues

In SaaS cloud computing model, application security is a major challenge. This is mainly since even though they are delivered through a web browser, attackers who mostly use the internet can take advantage of it [18]. This may lead to consumers' data being stolen or are compromised. The challenge has been experienced in other web using technologies where measures have been taken to deal with the challenge though they have not yet proven effective [4].

Accessibility

Another major challenge facing cloud computing is data accessibility. Because most applications have to be achieved through the internet, data from the cloud has been exposed to various risks [10]. Consumers are as likely to suffer from insecure networks, proximity-based hacking as well as information stealing malware [14].This makes the cloud services more insecure for critical data storage by companies as well as individuals.

Continuous evolvement

Today's world is greatly changing as time goes by especially in matters of technology. The requirements and demands by cloud consumers are also evolving [21]. Also, other service providers that cloud computing are still advancing. This hence calls for the clouds to change too. This can be a great challenge, especially where many resources are needed.

Interoperability issues

Today, cloud-computing companies have their way of operating their clouds; how they store their data, retrieve, secure and how their users interact with the cloud. This had led to a "hazy cloud" phenomenon, which hinders the development of cloud ecosystems and usually locking vendors. Cloud users are unable to choose from alternative vendors simultaneously in attempts to optimize their services. Other interoperability issues involve the cloud sources failing to integrate with the existing IT assets in organization hindering the optimization of assets and resources an organization owns. The initial prime goal was to able seamless data exchange between clouds and from localized stations to the clouds. However, to achieve the cloud vendors need to standardize their equipment to allow this interoperability. This has not been made possible to date and is hurting many clients who may wish to have their assets stored in clouds communicate with each other.

Service level agreements

Usually, cloud consumers do not have control over the third party hosting company. However, they need to ensure the availability, performance, reliability, and quality of these cloud providers to ensure their services are not hampered by the incompetence on the cloud service providers. It can be very damaging to a business to migrate its core business to the clouds only to be failed by the issues that relate to a third party company. Therefore, it is important for consumers to obtain service level agreements with their cloud hosts to be guaranteed of reliable and quality performance when they migrate their resources to them. The organizations should pose several questions to the providers to ensure a quality service is guaranteed. Such questions may include; where does the data reside, procedures to audit the data, how the data is secured by the service provided, how long it takes to back data to the cloud, and the procedures of extracting data when moving it to other places.

Data Center Issues

Many consumers today are wary of the reliability of the data centers in the clouds. While consumers are ready to surrender their data to third parties, the major underlying question underlying the minds of many people, what could happen if the third party agents collapse [15]. What is a disaster happens to the cloud center? There is fear that failures can occur to the cloud service providers, which can easily cripple many businesses and organizations hosted there. A recovery procedure is therefore supposed to be explained in the service agreements to eliminate doubts of such failures from clients.

CONCLUSION

Government agencies, organizations and even private players are all hosting their services in the clouds. This has allowed easier access cost efficiency, high scalability amongst other great advantages of the revolutionary technology. Businesses today, especially e-commerce services and software companies are the major beneficiaries of the cloud computing. However, there is a lot to be cautious about cloud computing. Robust policies and agreements need to be applied in the cloud computing technology to ensure enough security and quality performance is guaranteed by the cloud computing service providers. The paper has analyzed the major security issues that surround cloud computing and other challenges that concern consumers over cloud computing issues.

REFERENCES

[1] Ahmed, M., & Hossain, M. A. (2014). Cloud computing and security issues in the cloud. International Journal of Network Security & Its Applications, 6(1), 25.

[2] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information Sciences, 305, 357-383.

[3] Almorsy, M., Grundy, J., & Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[4] Avram, M. G. (2014). Advantages and challenges of adopting cloud computing from an enterprise perspective. Procedia Technology, 12, 529-534.

[5] Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. Journal of Network and Computer Applications, 67, 99-117.

[6] Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2012). Security issues for cloud computing. Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies, 150.

[7] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 5.

[8] Joshi, B., Joshi, B., & Rani, K. (2017). Mitigating Data Segregation and Privacy Issues in Cloud Computing. In Proceedings of International Conference on Communication and Networks (pp. 175-182). Springer, Singapore.

[9] Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: a survey. Computers, 3(1), 1-35.

[10] Meetei, M. Z., & Goel, A. (2012, October). Security issues in cloud computing. In Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on (pp. 1321-1325). IEEE.

[11] Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing, 63(2), 561-592.

[12] Moreno-Vozmediano, R., Montero, R. S., & Llorente, I. M. (2013). Key challenges in cloud computing: Enabling the future internet of services. IEEE Internet Computing, 17(4), 18-25.

[13] Onwubiko, C. (2010). Security issues to cloud computing. In Cloud Computing (pp. 271-288). Springer London.

[14] Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S. (2015, January). Cloud computing features, issues, and challenges: a big picture. In Computational Intelligence and Networks (CINE), 2015 International Conference on (pp. 116-123). IEEE.

[15] Reddy, V. Krishna, B. Thirumala Rao, and L. S. S. Reddy,(2011). "Research issues in cloud computing." Global Journal of Computer Science and Technology 11.11

[16] Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC press.

[17] Rong, C., Nguyen, S. T., & Jaatun, M. G. (2013). Beyond lightning: A survey on security challenges in cloud computing. Computers & Electrical Engineering, 39(1), 47-54

[18] Shah, H., & Anandane, S. S. (2013). Security issues on cloud computing. arXiv preprint arXiv:1308.5996.

[19] Sharma, P., Sood, S. K., & Kaur, S. (2011). Security issues in cloud computing. High Performance Architecture and Grid Computing, 36-45.

[20] Tari, Z. (2014) Security and privacy in cloud computing, IEEE Cloud Comput. 1 (1) 54–57.

[21] Tianfield, H. (2012, October). Security issues in cloud computing. In Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on (pp. 1082-1089). IEEE.

[22] Youssef, A. E. (2012). Exploring cloud computing services and applications. Journal of Emerging Trends in Computing and Information Sciences, 3(6), 838-847.

[23] Muthu Dayalan (2017). Research on Emerging Developments in Data Privacy and security in the technologically advanced corporate sector. International Journal of Emerging Technologies and Innovative Research, Volume (4), Issue (10), Pages 296-299