Assessment Task 2: Identify a Problem – Security vulnerability for cloud service and its solutions through encryption

ABSTRACT

The use of cloud service has been drastically increased on a daily basis and acknowledged as a mainstream method to operate an IT service over the internet. This is due to the economical benefits and flexibility that cloud service offers, however its transfer also produced new security problems to deal with. Since cloud service, particularly Infrastructure as a Service, are primarily targeted at low budget start-ups, they are frequently utilised to outsource to a third party, which results the reliance on the security and privacy of the cloud service provider rather than maintaining their own servers. This report aims to deliver security issues that the cloud provider can encounter, or is currently experiencing, as well as identifying the possible solutions against the problems using the method of encryptions.

INTRODUCTION

The growth of cloud services raised the attention of the importance of security problems in both public and enterprises. Gartner Inc [1] prospects that cloud implementation will be the top 10 most important technologies in successive years by companies and organizations. Cloud service follows up with the main benefits in cost-effectiveness, floor space utilization and efficiency compared to the past technology, on-premises servers [2]. However, this implementation doesn't always imply positive impacts, as there are some significant factors to consider after the adaptation. Security is the main factor that clouds service struggles and followed by issues regarding compliance, privacy, and legal matters [3]. Since cloud service is a newly developed technology, there is always uncertainty about the methods to deal with hacking, hijacking, and Denial of Service Attacks (DoS) [4]. This remains a source of uncertainty, resulting in an overwhelming concern for security factors among the enterprises. Through this, the use of encryption algorithms is arising as a solution to resolve security problems [9].

Security concerns in cloud service also refers to the lack of control, external data storage and complexity in internal security [5]. This is due to the transition from the traditional technology that the enterprise could manage physically and visually, to the cloud service, which is completely virtualized. And this causes the lack of resources to configure an organised managing system as it presents different issues that requires different solutions than the traditional way. Additionally, the virtual transformation produced the difficulty in controlling the network under their control, as well as the maintenance cannot no longer be performed themselves, which make it not to be able to fix the encountered problem immediately, unlike the on-premises server [6]. Although there are many encountering security issues arising with the cloud service, the benefits of cloud service are essential to be implemented in modern society. Thus, this report will demonstrate the main security issues in cloud service, challenges, and brief solutions about encryption method to overcome the current issues.

BACKGROUND & CONTEXT

The trend of implementing from on-premises servers to cloud service produced a large amount of user growth pool for many Software as a Service (SaaS) companies such as Amazon Web Services (AWS) and Google Cloud [7]. However, the condensation of sensitive information in to one server has led to a discussion on the security of the cloud service. This can be seen in the recent data breach happened in google cloud, a leading provider of cloud computing service was attacked by hackers from China in 2010 [8]. This is due to the cyber hackers treating the cloud service as a new frontier to steal private information, and course harm to the enterprise, as many businesses are implementing the cloud service nowadays. Furthermore, it conveys the weakness of cloud service that the loss of security from one provider can cause the hacking of other enterprises who employs the cloud service linked with the hacked provider.

PROBLEM DEFINITION

Security concerns rise within the implementation of cloud service in many industries. These problems are divided into two main categories: cloud provider security issues and client security issues [10]. Provider ensures that their infrastructure meets all requirements to protect the data, and to secure the clients' information, as well as the client needs to check whether the provider is appropriate to secure their data. Since cloud service can only be maintained by the provider, it is their responsibility to keep them safe.

MOTIVATION

Within the benefits of the cloud service, the usage of cloud computing in many ways such as Software as a Service, Platform as a service and Infrastructure as a Service will continue growing with the global use of internet service [11]. Therefore, the security issues along with the increasing attention is necessary to resolve before the full implementation over the world.

Security is more of a provider's responsibility with SaaS. Clients must rely on service providers for security precautions. Because public clouds are less safe than private clouds, they require more stringent security measures. In SaaS, it's also impossible for the user to know whether sufficient security is being maintained [12]. More extensibilities may be required by private clouds to fulfil unique requirements.

PaaS service provides to the customer to create their own apps within their service [13]. As a result, customers are responsible for protecting their applications, whereas providers are merely responsible for isolating customers' apps and workspaces from one another. As a result, the key security requirements in PaaS include ensuring the integrity of applications and implementing authentication checks [14].

The major application of IaaS is as a delivery model [15]. The primary security problem in IaaS is maintaining control over client data housed on the provider's hardware. The security of operating systems, programmes, and content is the responsibility of the users. Low-level data protection must be provided by the cloud provider [16].

Public clouds are less secure than other cloud models due to their deployment approach, which allows users to access data via a broad area network. Additional security measures, such as trust, are required in the public cloud to ensure that all applications and data accessed on the cloud are not vulnerable to possible threats [17]. Because it is customised for a specific enterprise, using the private cloud is far more secure than using the public cloud. A private cloud that is linked to one or more public clouds is known as a hybrid cloud [10]. Because everything is handled centrally, hybrid clouds allow more secure control of data and applications. The enterprises use distributed computing for different purposes.

The cloud is utilized by medical organizations to foster customized Health therapies [6]. While financial administrations organizations use cloud for misrepresentation identification and ongoing obstructing. Fundamentally, cloud figuring isn't an application situated maybe it is administration arranged. The security and protection of information is one of the central issues in distributed computing [18]. The cloud specialist organizations should safeguard the assurance of items from different malware and for that there are various approaches and instruments of Cloud specialist organizations.

CURRENT SOLUTIONS

There are steps for cloud providers to protect against security threats in the current stage as an undertaking cloud client. These include understanding the cloud structure, reinforcing the internal security, and to monitor the development or changes in the cloud technology [19]. By having an in-depth understanding of cloud service, the cloud supplier can supply definite data on its security engineering and can make changes relying upon the weakness that ran overall through the audit. Reinforcing internal security can be done by using advanced firewalls and access controls to avoid any future threat that can occur due to the leak of technology [20]. Observing the advancement isn't the arrangement that can be applied in this stage, in any case, is quite possibly the most significant and straightforward demonstration to be finished. Assuming any progressions are produced using the advancement to further develop the security issue, by essentially applying its update, the greater part of the potential dangers can be settled. As cloud administration is a developing innovation, the update can be delivered frequently over the time.

CHALLENGES

As the technology is developing, and cloud service can be used on most of the modern areas, various organizations of different type, size and industry utilize the cloud in a wide range of information handling cases like data backup, disaster recovery, virtual work areas, software development and testing and online web-based customer service [21]. However, this popularity and flexibility encounters as a main issue to reinforce the security problem, as the variety disrupt to build a unified security system. Since different industries maintains different types of data that need to be stored and handled depends on the area, it also requires different security methods to avoid the threats. For example, telecommunication service requires more focus on network aspects, meanwhile the banking service focuses on privacy and backup/recovery issues. Different areas desire for their specific needs, which makes it difficult for a cloud service provider to reinforce the entire security.

Data shared between different organizations is one of the major advantages or cloud computing, but this advantage also imposes a risk as data can be misused by other users [10]. Although cloud structure and internal security are developed, it does not change the main issue of the cloud service that the loss of control from the provider causes the loss of entire data who area associated with the provider. Infections, trojans, malware, and so forth, are unapproved ways of taking advantage of clients' data [18]. Now and again an association should deal with information stays, this is to safeguard the privacy of a representative's data even after his information is eliminated or deleted.

Finally, security dangers can happen from both outside of and inside associations. Internal actors were responsible for 43% of data loss, half of which was intentional, and half accidental [22]. The accidental breaches were usually occurred through misconfiguration, since cloud infrastructure offers simple data sharing, which makes it difficult for associations to guarantee avoiding other access to their cloud service.

TOOLS & METHODS

Encryption is proposed as an answer for secure data which is being transferred, stored or under some other operation [9]. Assuming somebody is imparting figuring assets to different organizations in a public cloud, the public authority might hold onto information with sensible reason and could bring about the openness of information. Encryption is the method to avoid this and protect data stored in the public cloud data. This dodges even cloud suppliers from approaching information or decryption keys [16]. Assuming the public authority or somebody wishes to get to information, individual permission to get down to the client. It helps in keeping up with clients' information in private yet at a similar level for information access to the cloud. This cryptographic method can prevent from losing data and protect data integrity while transmission.

STRATEGY

Encryption in cloud computing can be mainly listed as Advanced Encryption Standard (AES), and Ron Rivest, Adi Shamir, and Lenard Adleman (RSA) [9]. AES is a strong symmetric key encryption algorithm developed by NIST. It uses 10,12, or 14 rounds each of ciphers has a 128-bit block size with the key size of 128,192 and 256 bits respectively [23]. Through this, it ensures that the hash code is encrypted in highly secure manner. Additionally, RSA is an asymmetry key encryption algorithm that is commonly used conjunction with another secret key. RSA offers better numerically aspect but with lower speed to encrypt the small data than AES [24]. These two encryptions are both effective, and being used in different ways depends on the cases.

SUMMARY

As the cloud popularity is expanding every day, the security concerns in the cloud service are expanding too. Therefore, there is a need to take a gander at the cloud security a piece in a different aspect. Since dealing against the variety usage of cloud service in many cases encounters as a complex issue to resolve, as well as the internal security and breaches, the use of encryption provides the concept of enhancing security in cloud computing. It supports to reinforce the security problem with the encryption algorithm, which avoids the accidental breaches and hijacking data from the provider by requiring the decryption. This paper provided an overview of the major cloud computing security challenges discussed about the threats, current solution and brief explanation of tools and strategy that can be implemented to reinforce the security.

REFERENCES

[1] Gartner Inc, Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221

[2] Garrison, Gary, Sanghyun Kim, and Robin L. Wakefield. (2015, April 7) "Success factors for deploying cloud computing. Available: https://dl.acm.org/doi/abs/10.1145/2330667.2330685

[3] KPMG: From hype to future: KPMG's 2010 Cloud Computing survey. 2010. Available: http://www.techrepublic.com/whitepapers/from-hype-to-future-kpmgs-2010-cloud-computing-survey/2384291

[4] CheckPoint, Top 15 Cloud Security Issues, Threats and Concerns. Online. Available: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/

[5] Hashizume, K., Rosado, D.G., Fernández-Medina, E. et al. An analysis of security issues for cloud computing. J Internet Serv Appl 4, 5 (2013). Available: https://doi.org/10.1186/1869-0238-4-5

[6] Rashid, Aaqib & Chaturvedi, Amit. (2019). Cloud Computing Characteristics and Services: A Brief Review. INTERNATIONAL JOURNAL OF COMPUTER SCIENCES AND ENGINEERING. Available: https://www.researchgate.net/publication/331731714_Cloud_Computing_Characteristics_and_Services_A_Brief_Review

[7] RedHat, (April 6, 2018). What are cloud service providers? Online. Available: https://www.redhat.com/en/topics/cloud-computing/what-are-cloud-providers#:~:text=There%20are%20a%20handful%20of,providers%20all%20over%20the%20world.

[8] Markoff, John, and David Barboza. "2 china schools said to be tied to online attacks." (2010 Feb 18) Available: https://www.nytimes.com/2010/02/19/technology/19china.html

[9] Santosh Bulusu & Kalyan Sudia, (January 2012), A Study on Cloud Computing Security Challenges Online. Available: https://www.diva-portal.org/smash/get/diva2:830115/FULLTEXT01.pdf

[10] Verma, Amandeep & Kaushal, Sakshi. (2011). Cloud Computing Security Issues and Challenges: A Survey. Available: https://www.researchgate.net/publication/220790184_Cloud_Computing_Security_Issues_and_Challenges_A_Survey

[11] Naren.J, & Sowmya, S.K. & Deepika, P.. (2014). Layers of Cloud – IaaS, PaaS and SaaS: A Survey. International Journal of Computer Science and Information Technology. Vol. 5 Online. Available: https://www.researchgate.net/publication/264458816_Layers_of_Cloud_-_IaaS_PaaS_and_SaaS_A_Survey

[12] Chou, David & Chou, Amy. (2008). Software as a Service (SaaS) as an outsourcing model: An economic analysis. Online. Available: https://www.researchgate.net/publication/228447677_Software_as_a_Service_SaaS_as_an_outsourcing_model_An_economic_analysis

[13] Chavan, Pragati & Kulkarni, Gurudatt. (2013). PaaS Cloud. International Journal of Computer Science and Information Security (IJCSIS). 1. 21-26. Available: https://www.researchgate.net/publication/258255287_PaaS_Cloud

[14] Kim, Donghoon & Schaffer, Henry & Vouk, Mladen. (2017). About PaaS security. International Journal of Cloud Computing. 6. 325. 10.1504/IJCC.2017.090200. Online. Available: https://www.researchgate.net/publication/323590280_About_PaaS_security

[15] Shahzadi, Sonia & Iqbal, Muddesar & Qayyum, Zia & Dagiuklas, Tasos. (2017). Infrastructure as a Service (IaaS): A Comparative Performance Analysis of Open-Source Cloud Platforms. 10.1109/CAMAD.2017.8031522. Available: https://www.researchgate.net/publication/318726045_Infrastructure_as_a_Service_IaaS_A_Comparative_Performance_Analysis_of_Open-Source_Cloud_Platforms

[16] Yunchuan Sun, (July 16, 2014) Data Security and Privacy in Cloud Computing, Online, Available: https://journals.sagepub.com/doi/full/10.1155/2014/190903

[17] Kazim, Muhammad & Zhu, Shao Ying. (2015). A survey on top security threats in cloud computing. International Journal of Advanced Computer Science and Applications Online. Available: https://www.researchgate.net/publication/273950623_A_survey_on_top_security_threats_in_cloud_computing

[18] Bouayad, Anas & Blilat, Asmae & Nour El Houda, Chaoui & El Ghazi, Mohammed. (2012). Cloud computing: Security challenges. 26-31. 10.1109/CIST.2012.6388058. Available: https://www.researchgate.net/publication/261447405_Cloud_computing_Security_challenges

[19] Hashizume, K., Rosado, D.G., Fernández-Medina, E. et al. An analysis of security issues for cloud computing. J Internet Serv Appl 4, 5 (2013). Available: https://doi.org/10.1186/1869-0238-4-5

[20] Kumar, Ravi & Raj, Herbert & Perianayagam, Jelciana. (2017). Exploring Security Issues and Solutions in Cloud Computing Services – A Survey. Cybernetics and Information Technologies. Available: https://www.researchgate.net/publication/321637905_Exploring_Security_Issues_and_Solutions_in_Cloud_Computing_Services_-_A_Survey

[21] Mihail Dimitrov & Ibrahim Osman, 2014, The Impact of Cloud Computing on Organizations in Regard to Cost and Security, Online, Available: http://www.diva-portal.org/smash/get/diva2:728880/FULLTEXT02.pdf

[22] Mozumder, Deba Prasead & Nayeen Mahi, Md.Julkar & Whaiduzzaman, Md. (2017). Cloud Computing Security Breaches and Threats Analysis. International Journal of Scientific and Engineering Research. 8. 1287 - 1297. Available: https://www.researchgate.net/profile/Mdjulkar-Nayeen-Mahi/publication/320124329_Cloud_Computing_Security_Breaches_and_Threats_Analysis/links/59cef3c8aca2721f434f0493/Cloud-Computing-Security-Breaches-and-Threats-Analysis.pdf

[23] Babitha M.P. and K. R. R. Babu, "Secure cloud storage using AES encryption," 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Available: https://ieeexplore.ieee.org/document/787770910.1109/ICACDOT.2016.7877709.

[24] U. Somani, K. Lakhani and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing," 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010), 2010, Available: https://ieeexplore.ieee.org/document/5679895