PUBLISHED BY
JR
EDUCATION

Available online at http://ijite.jredu.id

IJITE

International Journal of Information Technology and Education (IJITE) 1(3), (June 2022) 117 - 123

International Journal of Information Technology and Education (IJITE)

http://ijite.jredu.id

Cloud Security Adoption Factors in Educational Institutions

Olivia E.S Liando [1]*, Marshel R. Kapahang [2], Johan Reimon Batmetan[2]

Department of Information and Communication Technology Education,
Universitas Negeri Manado

*Corresponding author : olivialiando@unima.ac.id

ARTICLE INFO

Article history:

Received: 20 March 2022; Received in revised form: 29 April 2022; Accepted: 20 June 2022;

Available online: 30 Juli 2022; Handling Editor: Fabiola Natasya Wauran

ABSTRACT

In recent years, cloud computing technology has emerged as one of the technologies that are currently hot or often used both in the world of work, online shopping (E-Commerce), and the world of education. Before we use any technology, we must first understand the security system that exists in that technology, including the security system in Cloud Computing Technology. In the world of education today, many schools and universities have implemented Cloud Computing Technology in learning systems and database storage. Currently, Cloud Computing provides 3 different services such as Saas, PaaS, and IaaS which can be used by organizations as private, public, and, Hybrid. Security is the main concern so that there is no data theft in the world of Education. This journal was created using the Literature Study by searching from several selected journals that already exist as knowledge, in order to better understand the Cloud Computing security system.

Keywords: Cloud Computing, Technology, Security Systems, Education World

INTRODUCTION

The impact of technological advances on human life is very significant. This is considered to be the era of the technological revolution. The rapid advancement of information technology has the potential to change people's lives as a whole. Technological advances have the potential to change the global economy and commercial environment. Cloud Computing is one result of the improvement of information technology (Cloud Computing). The changing educational environment is forcing educators to rethink their strategies to respond to global shifts in science, technology, and business, and these conditions may have an impact on an organization's bottom line. Cloud computing is a type of computing that utilizes the Internet to access resources.

Cloud computing is the application of technology across a network combined with web-based development. Cloud Computing has a number of advantages, including cost savings, increased storage capacity, ease of automation, flexibility, and increased data security. With all the benefits it provides, cloud computing is sure to be beneficial in the education industry. Information technology is currently developing into an inventive, dynamic, and economically profitable answer. All difficulties and challenges faced by the world of education can be solved with information technology. Cloud computing is changing the way information technology services are delivered and disseminated, enabling educational institutions to easily access a wide range of educational and scientific resources.

The development of cloud computing systems can facilitate educational institutions in providing information, student data, processing grades, and various academic reports. All activities in the academic environment can be controlled remotely via mobile devices, tablets, laptops, or PCs with the help of cloud computing that is connected to an automation system (Alfatih & Marco, 2015). Cloud Computing in Indonesia didn't start out that way, with many people hesitant to adopt it. Many misconceptions about cloud computing are fueled, including a lack of privacy because data from one company is stored alongside data from another, unmanaged security that makes consumers distrustful, immature conditions, productivity issues, and loss of ownership.

To improve the quality of education, the education system must be developed. Human resources are not only the responsibility of the government. Process Students who want to improve the quality of education can criticize traditional learning. Learning systems that rely solely on face-to-face meetings between educators and students will need supplements, as will advances in technology and devices that enable internet access. Learning is essential for implementing high effectiveness in today's world. Learning systems with the support of information technology can communicate information quickly and precisely. Since the discovery of multimedia communication media, traditional learning systems should have been abandoned. Due to the nature of the internet, which allows users to be connected at any time.

The main problem faced is that cloud computing users in the world of education do not know much about what security systems exist in cloud computing technology. This can result in frequent data leaks or theft. This journal aims to find out what security systems exist in cloud technology. This is very important to help or minimize the occurrence of data theft because by knowing the cloud computing security system we can take advantage of the security system.

METHOD

This research uses a qualitative descriptive method, which is to describe the cloud computing security system. A qualitative descriptive research method is a method that aims to describe an object of research through samples or data that have been collected and make conclusions that apply in general (Sugiyono, 2008). The author chooses this method because it is able to describe and evaluate various sources of data and information obtained so that the discussion of challenges and data analysis becomes easy to understand.

Data collection techniques using literature studies are used to obtain data. The term literature study is very well known, referring to a data collection procedure that involves examining related sources such as books, literature, records, and reports related to the subject to be examined. The literature used is library sources in the form of journals, research reports, books, and online news.

RESULTS AND DISCUSSION

Data Security in Cloud Computing (Data Security on Cloud Computing) is very important, but improving the quality of cloud computing network security, where various data in it can be stolen or snooped by irresponsible parties, is still an obstacle for some people.

Cloud Security is a data protection system, application, or computing infrastructure that is stored online and concurrently via a cloud platform. The methods included in providing cloud security are firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPNs), and avoiding public internet connections. Cloud security is a form of cyber security.

There are 7 specific security issues in cloud computing:

1. Privileged user access. Sensitive data processed outside the company carries an inherent risk, as outsourced services bypass "physical, logical and personal controls". IT will usually look for / use in-house programs. Get as much information as possible about the people who manage your data. Ask providers to provide specific information about the administrators they hire and supervise and control over their access rights.
2. Regulatory compliance. Customers are ultimately responsible for the security and integrity of their own data, even when held by the service provider. Traditional service providers are subject to external audits and security certifications. Cloud computing providers who refuse to undergo these checks indicate that customers can only use them for the most non-essential functions. Do not use these providers for critical services.
3. Location data. When you use the cloud, you may not know exactly where your data is hosted. In fact, you may not even know which country will save it. Ask providers if they will commit to storing and processing data in a particular jurisdiction and whether they will make a contractual commitment to comply with local privacy requirements on behalf of their customers.
4. Data segregation. Data in the cloud is usually in an environment that is shared with data from other customers. Encryption is effective but not a complete cure. Find out what is being done to separate data when it is not in use. The cloud provider must provide evidence that the encryption scheme was designed and tested by experienced specialists. Encryption failure can render data completely unusable, and even normal encryption can make it difficult to provide availability.
5. Recovery. Even if you don't know where your data is, the cloud provider must tell you what will happen to your data and services in the event of a disaster. Any offering that doesn't replicate data infrastructure and

applications to multiple sites/machines at once is vulnerable and may lead to complete failure. Check with your provider if it has the capability to perform a total recovery and how long it will take.

6. Investigative support. Investigating unscrupulous or illegal activity may be difficult in cloud computing. Cloud services are very difficult to investigate, as logs and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you are unable to secure a contractual commitment to support specific forms of investigation, together with evidence that the vendor has attempted to support the activity, then your safe assumption is that inquiry and discovery requests will not be possible.

7. Long-term viability. Ideally, your cloud computing provider will never go bankrupt or be acquired and swallowed up by a bigger company. But you should be sure that your data will remain available even after such an event. Ask the potential provider how you will get your data back and if it will be in a format you can import into a replacement application.

So what is the importance of using Cloud Security?

Concerns on Data Security. For cloud providers, security is a big concern. They must not only please customers but also comply with various rules and regulations regarding the storage of sensitive data such as credit card numbers and medical records. Third-party audits of cloud providers' security systems and procedures assist in the protection of user data. Data breaches, data loss, account hijacking, traffic hijacking, and other threats are very dangerous in this situation. As a result, you must ensure that the supplier can be trusted to provide cloud security.

Access System Security. It takes more than just securing the cloud to keep data secure in the cloud. Access to the cloud must also be protected from data stored on other devices or unauthorized logins. Data stored in other cloud-hosted countries must also be protected, and various privacy policies, processes, and regulations may apply. You should be able to see the guidelines offered by the provider regarding the access used before deciding to implement cloud security, especially with regard to certain data. As a result, with clear transparency, security controls can be used to their full potential, and people can trust each other.

Product Standards. Some vendors provide many offers related to some of the products provided, especially for cloud security. At this stage, the most important thing is that you can see the standards that exist and have been determined. This is a common concern, so understanding and knowing the standards provided makes the process run properly.

Important Factors to Maintain Cloud Security

Talking about cloud technology, of course, you are no stranger to the security system. As it is known that this technology makes it easier for you to store data online. But if you're not careful, your data can be stolen. Therefore, pay attention to the following so that cloud security is maintained:

1. When starting to decide to use cloud technology, make sure the data protection must be safe from the provider. You should know what kind of methods they use to keep the data safe. Also, ask about the location of the data storage because this is related to the data center.

2. In order to experience the benefits of using cloud security, you should know what access is like. You must first understand the rules set by the provider. One of them knows who can access file A and so on. This is related to security control.

3. If you want to get real benefits from this technology, first understand the vendor's standards. For example using ISO 27001 or COBIT. So from here when there is a problem, you can solve it quickly. Because you already know the standard cloud used from the start.

4. The nature of the cloud is generally resource sharing. So you must always be ready when a tenant commits fraud so that data security becomes insecure. However, the stored data can be one with the other. Therefore ask about multi-tenancy.

Advantages of using Security Cloud Computing

By simply uploading data to the cloud, it might be understood as an online data storage medium. So very easy to use. There are many types of clouds available today that can be used for personal and professional purposes. Following are some of the benefits of using cloud security for data storage:

1. It is undeniable that this technology has very good capacity flexibility. So you don't have to think about the capacity because it is unlimited. That way you can use it as needed without the addition of devices like conventional servers. So the advantages are clearly more efficient in cost and time.

2. The advantage of using other cloud security is quite safe. It has special encryption because it comes with it. Every piece of data is protected by multilayer security thanks to encryption. So that data confidentiality is always maintained, even if using manual storage media. This is one of the reasons why cloud security is so popular.

3. Generally, every cloud security is supported by a good data backing up process. So that any stored data is always maintained without problems and is not lost. So when one is lost, you can still use it again because there is a backup feature here.

Benefits of Cloud computing Security

1. Protection from DDoS attacks. Cyber attacks can be launched against local servers or databases. DDoS attacks are one of the most popular types of attacks. DDoS (Distributed Denial of Service) is a type of cyber attack that involves flooding the internet network with fake traffic generated by a server, system, or network. This can be done above if you are using a cloud service. To defend against DDoS attacks, cloud service provides great bandwidth and depth. With cloud security capabilities that can reroute internet traffic, backup resources can be provided.

2. Real time. Another benefit is the high level of availability and assistance. This means that cloud security has a function that allows it to work for up to 24 hours. Work in the sense of continuous observation and reporting. This function is very important because many business assets, such as websites and business applications, are available 24 hours a day. Companies can take advantage of this functionality to ensure that their app or company website is available 24 hours a day, seven days a week, whenever the user requests it. As a result of this feature, many businesses are turning to cloud services instead of traditional ones.

3. Fast in doing the deployment. Like most other cloud services, where when using the service, once it is obtained it is activated and then tells which one to protect. This is an advantageous benefit when using cloud security. When compared to some traditional security. Cloud security is far superior because traditional

security still requires installing network hardware and security tools. And traditional security has complex rules and policies designed, tested, and implemented.

4. Already implemented AI. Many cloud services are already implementing AI in their services. The function of the AI is to monitor events and can report abnormal activity. The use of AI itself is faster compared to traditional services which still require a lot of things such as regular patches, firmware updates, etc. With cloud services, all updates happen instantly and instantly. This feature is very important, because if the update is done only occasionally. Can cause outages across billions of operational instances.

5. Reducing operational costs. The main benefit of cloud security, apart from its ease of access and security, is cost reduction. The cost savings come from the specific hardware, applications, and personnel required to run it. Many local security tools are vulnerable to failure and attack. Such attacks will not be tolerated by cloud users. The workload of IT personnel can also be reduced through dashboards and alert solutions. As a result, they could only concentrate on operational difficulties.

Examples of Application of Security Cloud Computing in Education

Its application is very important in the world of education because it affects the continuity of data security for students and educators to prevent data theft, data falsification, and much more. Therefore the use of Security Cloud Computing is very important in Education.

CONCLUSION

Security cloud computing is important to be applied in the world of education. The use of cloud computing-based technology in the education sector can increase efficiency and effectiveness, so more knowledge about cloud computing is needed for lecturers and students. The benefits of Cloud computing Security are Protection from DDoS attacks and The main benefit of cloud security, apart from easy access and security, is cost reduction.

REFERENCES

Cloud: Tujuh Resiko Keamanan pada Cloud-Computing - OnnoWiki. (2022). dikunjungi 8 Juni 2022, dari https://lms.onnocenter.or.id/wiki/index.php/Cloud:_Tujuh_Resiko_Keamanan_pada_Cloud-Computing

Keamanan Cloud Computing, Begini Cara Memahaminya - Mitra Teleinformatika Perkasa. (2020). Dikunjungi 8 Juni 2022, dari https://mtp.co.id/keamanan-cloud-computing-begini-cara-memahaminya/

End-to-End Enterprise Security On the Cloud - Alibaba Cloud. (2022). dikunjungi 8 Juni 2022, dari https://www.alibabacloud.com/solutions/security?spm=5176.2020520001.9059645200.1.386ayp7W

lum, M. (2014). Keamanan Data Pada Cloud Computing. Dikunjungi 8 Juni 2022, dari https://blog.wowrack.co.id/2014/07/keamanan-data-pada-cloud-computing.html

PENGANTAR CLOUD COMPUTING : (Model Keamanan Cloud Computing) - Cerita Hosting ☁. (2020). dikunjungi 8 June 2022, dari https://ceritahosting.com/2020/07/04/pengantar-cloud-computing-model-keamanan-cloud-computing/

Anon (2022). dikunjungi 9 Juni 2022, dari https://www.netmarks.co.id/post/pentingnya-menggunakan-cloudsecurity

Gravita, A. (2021). 5 Manfaat Cloud Security yang Perlu Kamu Ketahui - Coding Studio. dikunjungi 9 Juni 2022, dari https://codingstudio.id/manfaat-cloud-security/

Ika, N.A., Mufty Ali Hamdani, IYusuf Amrozi,"implementasi Sistem Basis Data Cloud Computing pada Sektor Pendidikan", KELUWIH: Jurnal Sains dan Teknologi, Vol.1 (2), 77-84, Agustus 2020

Brenda Karisoh, Hensy Watung, Putri Ante, "Memahami Pengguna Untuk Mengadopsi Teknologi Cloud Computing", Jurnal Internasional Teknologi Informasi dan Pendidikan (IJITE) Volume 1, Nomor 1, Desember 2021

Djubir Ruslan Eddy Kembuan, John Reimon Batmetan "Design e-Office Application for Population based on Cloud Computing", Jurnal Internasional Teknologi Informasi dan Pendidikan (IJITE) 1(2), (march 2022) 91-98 Published by JR EDUCATION

Johan Reimon Batmetan, Hensy Watung1 , Leyri Nayoan1 , Avandi E. Untu1 "Understanding Cyber Crime Behavior on E-Commerce Application Users", Jurnal Internasional Teknologi Informasi dan Pendidikan (IJITE), Vol. 1 No. 2 (2022): March, hal 8-15 Published by JR EDUCATION

Pedro Ramos Brandao, "Security Cloud Computing", ResearcGate, JCST Vol. 10, Edisi 1, Jan - Maret 2019,

Komeil Raisian, Jamaiah Yahaya, "Security Issues Model on Cloud Computing: A Case of Malaysia", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 8, 2015

Yuli Fauziah, "TINJAUAN KEAMANAN SISTEM PADA TEKNOLOGI CLOUD COMPUTING", JURNAL INFORMATIKA Vol. 8, No. 1, Januari 2014

Mella Marliana, "KEAMANAN DAN PENCEGAHAN DATABASE CLOUD COMPUTING UNTUK PENGGUNA LAYANAN", Jurnal PRODUKTIF, Vol 3 No.2 Edisi 2019 hal 331-336

Muqorobin1, Zul Hisyam1, Moch. Mashuri1, Hanafi1, Yudhi Setiyantara, "Implementasi Network Intrusion Detection System (NIDS) Dalam Sistem Keamanan Open Cloud Computing", Majalah Ilmiah Bahari Jogja (MIBJ) Vol. 17 No. 2, Juli 2019, (1-9)

Beny Nugraha, "Analisis Teknik-Teknik Keamanan Pada Cloud Computing dan NEBULA (Future Cloud): SurveyPaper", TEKNOSI, Vol. 02, No. 02, Agustus 2016

Aditya Dwi P.W.1, E.I.H. Ujianto2 "Analisis Sistem Keamanan Pada Cloud Computing Menggunakan Metode Attack-Centric (Security System Analysis of Cloud Computing Using Attack-Centric Method)", Vol. 16, No. 1, Februari 2020: 57- 68

Muhammad Aziz1, Achmad Fuad2, Mohamad Jamil3, "IMPLEMENTASI CLOUD COMPUTING SEBAGAI INFRASTRUKTUR LAYANAN MAIL SERVER PADA UNIVERSITAS KHAIRUN", JIKO (Jurnal Informatika dan Komputer) Ternate, Vol. 02 No. 1, April 2018

Wiwin Hartanto, "CLOUD COMPUTING DALAM PENGEMBANGAN SISTEM PEMBELAJARAN", Prog. Studi Ekonomi FKIP UNEJ

Livia Maukar, "VIRTUAL CLASSROOM DESIGN FOR THE DEAF BASED ON CLOUD COMPUTING", Jurnal Internasional Teknologi Informasi dan Pendidikan (IJITE), Vol. 1, No. 1, December 2021