NAME : PRANAY PRAKASH RAI

REGISTRATION No. : 20BIT0129

SLOT : E2+TE2

ITE4001

NETWORK AND INFORMATION SECURITY

THEORY DA

TOPIC : CLOUD SECURITY MEASURES , PRACTICES AND RISKS .

***

Abstract

The world has witnessed a rapid shift from physical storage devices to vast virtual data centres, all made possible by cloud storage technologies. This has led to data transfer and sharing between several people and organisations became possible, making it one of the most widely utilised services on the cloud platform. Businesses have developed into scalable entities that continuously satisfy customer wants. Security and privacy are now top priorities due to the significant advancements in this area.Concerns like poor data visibility, storage sinks without secured pointers, cases of enormous data spills, etc. can harm people's finances and information on a large scale. In light of this, one of the main difficulties we now face is current data security and advisory ways to monitor data sinks. This paper attempts to examine various security issues and the most recent state-of-the-art solutions to address them.

Introduction

A solution for data storage that is outsourced is cloud-based internet security. Users save data on servers that are connected to the Internet rather than local hard discs. To keep the data accessible and safe, data centres oversee these servers. You access the cloud whenever you access a file that was stored elsewhere. How does local storage compare to cloud storage? The main difference is that the cloud provider uses the internet to move data from secure data centres to specific devices that access the cloud. This centralises cloud computing. There are different sorts of clouds, as is clear.

Three different cloud kinds are covered by network security: public, private, and hybrid clouds. Cloud computing refers to a shared system that is accessible from beyond the firewall of an enterprise. In this case, the infrastructure is under the control of the cloud service provider. A private cloud, on the other hand, uses the same platform but is managed by the company's IT department inside the corporate firewall.

A private cloud is intended to provide the same capabilities and advantages as public cloud systems but removing several common cloud computing model objections, such as control over customer and business data, security concerns, and challenges with regulatory compliance.

A hybrid cloud platform combines the aforementioned two, storing sensitive data on a private cloud while huge volume data files are retained on a public cloud. The platform at this moment is popular with larger corporations. Additionally providing extensibility in terms of customising is this technique. In order to protect our data in a cloud, a variety of rules, technologies, and controls are utilised. This is referred to as cloud computing security. It falls under the umbrellas of network security, information security, and cloud security. Modern security procedures are applied to each and every file saved on a cloud platform. Some of the common cloud security procedures include advanced firewalls, event logging, intrusion detection, internal firewalls, and security.

Literature Survey

Businesses use cloud services because they cut down on upfront costs for building data centres, recruiting qualified IT staff internally, and paying for cloud services on a pay-as-you-go basis. Additionally, it aids in escaping the restrictions of application upgrading and the cost of data centre maintenance. Threats to the cloud and its users are growing along with the demand for cloud services. A third party can be given the responsibility of security and manage it as a service. They can choose which methods to deploy in accordance with the circumstance by using the agents' autonomy. Agents can utilise RSA-based two-way security protocols to maintain highly sensitive data in accordance with the various cloud data classifications. For a distinct environment that makes use

of mobile devices to access cloud services, a virtualization and security management strategy is recommended.

Managing and ensuring a secure usage over multi-provider Inter-Cloud settings with specialised communication infrastructures, security mechanisms, processes, and rules is one of the most significant security concerns in the context of cloud computing. From the standpoint of functional security management, the goal of security controls in cloud computing is the same as the goal of security controls in any other IT system. It is suggested to adapt and reuse current traditional security management areas that need to be improved for particular requirements of cloud computing (such as dynamic reconfiguration, distributed services, etc.). Using a variety of Inter-Cloud use cases and scenarios from the corporate and public sectors, including DMTF (Distributed Management Task Force), NIST (National Institute of Standards and Technology), GICTF (Global Inter Cloud Technology Forum) and ENISA (European Network and Information Security Agency). A variety of security management requirements have been examined and compiled. The development of a security management architecture for the Inter-Cloud will build on this collection in the future.

One of the biggest changes in information technology is cloud computing, which makes it possible to offer cloud-based security services like Security-as-a-Service (SECaaS). The old SIEM paradigm can switch to cloud-based security services thanks to advancements in cloud computing technology. The SECaaS platform, which was created for the purpose of analysing and identifying intelligent cyber-threat based on virtualization technologies, can be equipped with SIEM architecture, which holds the key to the solution.

The term "cyber-physical system" (CPS) refers to a wide variety of intricate, multifaceted, physically aware next-generation designed systems that incorporate embedded computing technologies (cyber component) with the real environment. Cyber-Physical Systems (CPSs) are advanced designed systems that mix embedded computing technology (the "cyber component") into physical phenomena. They are multidisciplinary, complicated, and physically aware. From a multi-disciplinary perspective, this integration primarily entails observation, communication, and control components of physical systems. Modern cloud computing solutions that have been successful in addressing the requirements of enterprise applications do not easily translate to addressing the workflows of cyber-physical systems. Existing cloud platforms, for instance, do not currently offer the strict assurances on many concurrent quality of service (QoS) aspects required by CPS applications, such as reliability, security, and punctuality. Cyber physical systems based in the cloud are therefore unique. The concepts and resources needed for its design are not available through systemic or object-oriented methods. To meet the needs of such a design, we must enhance the unified modelling language (UML). The Meta-Object Facility is a metamodeling architecture created by the Object Management Group (OMG) to define the UML. According to the metamodeling technique, the model that makes up UML is specified using a metamodel. According to the proponents of this strategy, most implementers and practitioners will find it to be more intuitive and practical.

There are mainly 5 types of threats:

A. Account Management

Attackers have access to private and sensitive data through hijacking. Subscription accounts or cloud service accounts are the accounts most at risk in cloud systems.

B. Negative insiders

Insiders can access networks, data, and systems because they don't need to get past firewalls, VPNs, and other security measures because they operate on a trusted level. This information could be sold or used by a malevolent insider for their own gain or the loss of the target user as a whole (s).

C. Data Management

Any attack or occurrence in which confidential data is taken, read, or used by an unauthorised party qualifies as a data breach. Lack of data control is demonstrated by unpatched systems, excessive permissions, and unsecure data storage containers.

D. Management Console Security UIs and APIs are the components of a system that are the most exposed. These must be created to avoid security breaches, from authentication to access control.

Multi-tenancy Problems, E For a cloud service provider, ensuring data isolation, traffic bandwidth, etc. must come first. The key to resolving this is logical security, trust, access control, and encryption of both keys and data.

Due to numerous implementations, security management in diverse delivery formats is challenging.Thus, creating a consistent, standalone security paradigm becomes difficult and ineffective. Furthermore, since many service delivery models could coexist in the same cloud platform, security management becomes challenging. Elasticity and multitenancy are two of the cloud computing model's key attributes, according to some.Elasticity entails adjusting the amount of resources allocated to services in response to changing demand. Security restrictions are met via the employment of placement engines for resource management under elasticity. In order to prevent assaults aimed at locating the assets of victims, the concept of secure multi-tenancy is offered through isolation and location transparency. An overview of model layers in cloud computing is provided with a brief discussion of dependency stack, then the paper delves into difficulties with IaaS, PaaS, and SaaS security. Key ideas in the fields of security, multitenancy, and security management are covered in the conclusion. Adaptive environment changes, integration support, holistic security wrappers, and other solutions are suggested as responses to the different issues described above.

Security Risks

The most alluring application of the cloud platform seems to be storage, as it does away with the expense of the necessary physical gear. Its other features, such extendable memory and on-demand remote access, make it a very helpful tool for both individuals and businesses. However, the security mechanisms that safeguard your data come in a variety of forms based on the cloud architecture.

A. Lack of Control

On the one side, you won't have to handle your data, but on the other, the cloud uses a third party to do it. Because you have no influence over how your data is stored, everything that restricts your vendor's storage options also affects your ability to access data. Being shut out of your own storage platform is one of the major risks of cloud storage. Choosing a safe and secure vendor is hence, very important.

B. Shared Servers

Cloud-based storage systems employ local servers to store data from many users on servers that are located on-site. Although users cannot access these servers directly, the nature of the material

provided on the server could present risks. If your data is shared on the same server, anomalous data uploads can also pose a security risk .

C. Data Leakage

One aspect of security is ensuring that no unauthorised person may access your organization's data; another is preventing your data from being given to anyone outside of your organisation (without carrying out the necessary checks, etc.). Data leaks could make private and sensitive information available to outsiders. Even if the organisation has data security procedures in place, the cloud counterpart heavily relies on the storage provider's security protections.

D. API and Storage Sinks

Utilizing the storage APIs and storage gateways of the cloud can frequently make the laborious process of cloud migration easier. However, because these technologies act as a middleman between the user and the platform, a security breach could occur here. Choose only services that have robust all-encompassing security throughout data transit, as an unsafe API or gateway might lead to data leaks.

It is standard procedure to inform consumers about data sharing capabilities, usage restrictions, device setups, and security mapping. However, it is nearly impossible to mitigate cloud security problems. A better path to secure storage is to remain watchful and put some security measures in place. We now examine some best practises to guarantee a secure cloud.

Security Practices

It is vital to establish a cloud storage framework with these practices –

A. Assessing cloud framework

To prevent unauthorised access, all companies must keep track of connected devices, update currently accessible devices, and get rid of outdated or unneeded equipment. A closer look at how data moves across systems, programmes, and hardware will be possible with data flow mapping. Numerous cloud services enable services to make this easier.

B. Security Encryption

Understanding data security is a crucial necessity of any cloud storage technology (especially in a transit between data centers, servers, etc.). Additional security is provided by effective user management and machine intelligence algorithms that examine accesses' IP addresses and geo-locations. The cloud engineer monitoring services also benefit from an additional layer of abstraction provided by learned filters regarding common areas of access and exhibiting the same in event logging.

C. Data Classification

Not all cloud-stored data is equal in terms of significance and sensitivity. Maintaining classification techniques to separate data can aid in data security by alerting users to save data locally rather than on a cloud or disc. This is crucial for businesses that employ large hybrid clouds and have a surplus of unstructured data.

D. Multi Factor authentication

The majority of the time, careless device usage puts cloud security in danger. This includes leaving obsolete equipment connected to the cloud, where they might be accessed by unauthorised users. Data storage is made safer by using multifactor authentication across all systems and apps.

Advanced Security Measures

What we have observed thus far are common security procedures. However, no amount of protection is sufficient when dealing with sensitive data and business-related information. A more dedicated safe storage platform is created by continually improving security protocols and incorporating additional checkpoints. Here are a few examples of the cutting-edge security precautions such a platform would take:

A. Private Encryption

It keeps your data from being read by anyone besides you and is also known as Zero Knowledge. The encryption key is exclusive and only you have access to it; not even the cloud provider. As a result, no sensitive data can be harmed in the event of a data leak or breach. The use of such encryption does have a drawback, though, in that if you lose the password key for the data, it is permanently lost. A zero knowledge service doesn't handle password management or resets.

B. In-Transit Encryption

AES, the most recent encryption algorithm on the market, is also the most secure one to date. Depending on the length of the key, it has varied levels of security. The strongest encryption currently in use, 256-bit, has never been broken. This is utilised for data that is at rest, not in transit. The TLS protocol employs a handshake between machines that uses cyphers, authentication, and key exchanges to protect cloud data in transit from eavesdropping.

C. Ransomware Protection

While encryption is desired, it can only be achieved when a cypher is available. Upon locating sensitive data files, ransomware encrypts them, preventing you from accessing your own data. Even if the offender receives monetary compensation, using a decryption key to obtain access to data is risky. A scanning service that uses machine intelligence to study data accesses and flow could eventually contribute to the development of an AI ransomware detection system. The current accepted technique is to employ "versioning," a roll-back that enables version control in the cloud.

Of course, the question is: Which services uphold such stringent security standards? Some of the most recent services offer proper content management, authorization and access scrutiny, etc. Modern systems like Sync.com have become well-known for their superior security procedures and offer zero-knowledge encryption at no additional cost. Another comparable cloud storage platform is pCloud, but some consider Dropbox to be the established industry standard.

Conclusion

Large corporations frequently use cloud services, but independent groups and small businesses have also recently switched to cloud platforms. Because of this, security is of the utmost importance and is at the forefront of digital data protection. As a result, cloud computing is still in its infancy and requires a boost in research-based security applications. Users and vendors are both accountable for security. Both the service providers and the clients must manage this issue by maintaining security procedures on their end. Data abstraction and usage should be an intraorganizational security measure, while data visibility should be checked by the vendor services. Clouds should adhere to

approved GRC (governance, risk, and compliance) practises as set forth by the industry. Due to the cloud's intricate structure, it is nearly difficult to achieve end-to-end security, but protecting data and adhering to encryption standards whenever possible greatly reduces the dangers associated with sharing data.

References

1. A. Hendre and K. P. Joshi, "A Semantic Approach to Cloud Security and Compliance," 2015 IEEE 8th International Conference on Cloud Computing, 2015, pp. 1081-1084, doi: 10.1109/CLOUD.2015.157.

2. M. Kretzschmar, M. Golling and S. Hanigk, "Security Management Areas in the Inter-cloud," 2011 IEEE 4th International Conference on Cloud Computing, 2011, pp. 762-763, doi: 10.1109/CLOUD.2011.83.

3. J. -H. Lee, Y. S. Kim, J. H. Kim and I. K. Kim, "Toward the SIEM architecture for cloud-based security services," 2017 IEEE Conference on Communications and Network Security (CNS), 2017, pp. 398-399, doi: 10.1109/CNS.2017.8228696.

4. W. Nie, X. Xiao, Z. Wu, Y. Wu, F. Shen and X. Luo, "The Research of Information Security for The Education Cloud Platform Based on AppScan Technology," 2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), 2018, pp. 185-189, doi: 10.1109/CSCloud/EdgeCom.2018.00040.

5. D. R. Bharadwaj, A. Bhattacharya and M. Chakkaravarthy, "Cloud Threat Defense – A Threat Protection and Security Compliance Solution," 2018 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM), 2018, pp. 95-99, doi: 10.1109/CCEM.2018.00024.

6. A. Sun, G. Gao, T. Ji and X. Tu, "One Quantifiable Security Evaluation Model for Cloud Computing Platform," 2018 Sixth International Conference on Advanced Cloud and Big Data (CBD), 2018, pp. 197-201, doi: 10.1109/CBD.2018.00043.

7. J. Koo, Y. -G. Kim and S. -H. Lee, "Security Requirements for Cloud-based C4I Security Architecture," 2019 International Conference on Platform Technology and Service (PlatCon), 2019, pp. 1-4, doi: 10.1109/PlatCon.2019.8668963.

8. A. Abuhussein, H. Bedi and S. Shiva, "Towards a Stakeholder-Oriented Taxonomical Approach for Secure Cloud Computing," 2013 IEEE Sixth International Conference on Cloud Computing, 2013, pp. 958-959, doi: 10.1109/CLOUD.2013.132.

9. M. Lacoste, A. Wailly, A. Tabourin, L. Habermacher, X. L. Guillou and J. -P. Wary, "Flying over Mobile Clouds with Security Planes: Select Your Class of SLA for End-to-End Security," 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing, 2013, pp. 50-59, doi: 10.1109/UCC.2013.25.

10. A. Nhlabatsi et al., "Traceability for Adaptive Information Security in the Cloud," 2014 IEEE 7th International Conference on Cloud Computing, 2014, pp. 958-959, doi: 10.1109/CLOUD.2014.141.

11. C. Di Giulio, R. Sprabery, C. Kamhoua, K. Kwiat, R. H. Campbell and M. N. Bashir, "Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security?," 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), 2017, pp. 50-57, doi: 10.1109/CLOUD.2017.16.

12. A. Gordon, "The Hybrid Cloud Security Professional," in IEEE Cloud Computing, vol. 3, no. 1, pp. 82-86, Jan.-Feb. 2016, doi: 10.1109/MCC.2016.21.

13. P. Mell, "What's Special about Cloud Security?," in IT Professional, vol. 14, no. 4, pp. 6-8, July-Aug. 2012, doi: 10.1109/MITP.2012.84.

14. M. Jensen, J. Schwenk, J. -M. Bohli, N. Gruschka and L. L. Iacono, "Security Prospects through Cloud Computing by Adopting Multiple Clouds," 2011 IEEE 4th International Conference on Cloud Computing, 2011, pp. 565-572, doi: 10.1109/CLOUD.2011.85.

15. B. Albelooshi, K. Salah, T. Martin and E. Damiani, "Experimental Proof: Data Remanence in Cloud VMs," 2015 IEEE 8th International Conference on Cloud Computing, 2015, pp. 1017-1020, doi: 10.1109/CLOUD.2015.140.

16. O. Wenge, D. Schuller and R. Steinmetz, "Towards Establishing Security-Aware Cloud Markets," 2014 IEEE 6th International Conference on Cloud Computing Technology and Science, 2014, pp. 1027-1032, doi: 10.1109/CloudCom.2014.159.

17. H. Ming, H. Guihuai, L. Xu and X. Jiao, "A Dynamic Adjustment Model of Monitoring Frequency based on Cloud Security," 2018 IEEE 3rd International Conference on Cloud Computing and Internet of Things (CCIOT), 2018, pp. 1-4, doi: 10.1109/CCIOT45285.2018.9032652.

18. K. -K. R. Choo, "A Cloud Security Risk-Management Strategy," in IEEE Cloud Computing, vol. 1, no. 2, pp. 52-56, July 2014, doi: 10.1109/MCC.2014.27.

19. F. Doelitzscher, C. Fischer, D. Moskal, C. Reich, M. Knahl and N. Clarke, "Validating Cloud Infrastructure Changes by Cloud Audits," 2012 IEEE Eighth World Congress on Services, 2012, pp. 377-384, doi: 10.1109/SERVICES.2012.12.

20. A. Markandey, P. Dhamdhere and Y. Gajmal, "Data Access Security in Cloud Computing: A Review," 2018 International Conference on Computing, Power and Communication Technologies (GUCON), 2018, pp. 633-636, doi: 10.1109/GUCON.2018.8675033.

21. X. Weiquan and W. Houkui, "The Design Research of Data Security Model Based on Public Cloud," 2013 Ninth International Conference on Computational Intelligence and Security, 2013, pp. 607-609, doi: 10.1109/CIS.2013.133.

22. S. Ramamoorthy and R. Poorvadevi, "Security Solution for Hybrid Cloud Information Management Using Fuzzy Deductive Systems," 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), 2018, pp. 457-462, doi: 10.1109/ICSSIT.2018.8748395.

23. D. Zhe, W. Qinghong, S. Naizheng and Z. Yuhan, "Study on Data Security Policy Based on Cloud Storage," 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), 2017, pp. 145-149, doi: 10.1109/BigDataSecurity.2017.12.

24. X. Sun, "Critical Security Issues in Cloud Computing: A Survey," 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), 2018, pp. 216-221, doi: 10.1109/BDS/HPSC/IDS18.2018.00053.

25. K. El Makkaoui, A. Ezzati, A. Beni-Hssane and C. Motamed, "Cloud security and privacy model for providing secure cloud services," 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), 2016, pp. 81-86, doi: 10.1109/CloudTech.2016.7847682.

26. A. M. Sebastian and J. J. Kizhakkethottam, "A review on cloud security threats and solutions," 2015 International Conference on Soft-Computing and Networks Security (ICSNS), 2015, pp. 1-4, doi: 10.1109/ICSNS.2015.7292384.

27. Z. Yu, "Research on Cloud Computing Security Evaluation Model Based on Trust Management," 2018 IEEE 4th International Conference on Computer and Communications (ICCC), 2018, pp. 1934-1937, doi: 10.1109/CompComm.2018.8780657.

28. M. Joshi, S. Budhani, N. Tewari and S. Prakash, "Analytical Review of Data Security in Cloud Computing," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 362-366, doi: 10.1109/ICIEM51511.2021.9445355.

29. A. Syed, K. Purushotham and G. Shidaganti, "Cloud Storage Security Risks, Practices and Measures: A Review," 2020 IEEE International Conference for Innovation in Technology (INOCON), 2020, pp. 1-4, doi: 10.1109/INOCON50539.2020.9298281.

30. M. Malarvizhi, J. A. J. Sujana and T. Revathi, "Secure file sharing using cryptographic techniques in cloud," 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), 2014, pp. 1-6, doi: 10.1109/ICGCCEE.2014.6921421.

***