Postprint: Cloud Computing Security Research for Monitoring Data in Broadcasting and Television

Authors: Wang Qiang

Date: 2023-10-08T00:00:00+00:00

Abstract

This paper first introduces the development of the broadcast monitoring industry, then discusses the security threats faced by cloud computing of monitoring data in the broadcast field and their countermeasures.

Full Text

Research on Cloud Computing Security for Monitoring Data in the Broadcasting and Television Field

Abstract: This paper first introduces the development of broadcasting and television monitoring, then discusses the security threats facing cloud computing for monitoring data in the broadcasting field and proposes corresponding countermeasures.

Keywords: cloud computing; security; broadcasting field; monitoring data
CLC Number: TP393
Document Code: A
Article ID: 1671-0134(2017)12-104-02
DOI: 10.19483/j.cnki.11-4653/n.2017.02.029

Author: Wang Qiang

2. Security Threats and Countermeasures for Cloud Computing of Monitoring Data in the Broadcasting and Television Field

Cloud computing represents a significant topic of societal concern today and a buzzword in current communications technology. Grounded in the techni-

cal philosophy of "distributed network computing" and the business vision of "making computing services as accessible as tap water," cloud computing can interconnect software, system, computing, and storage resources to construct large-scale virtual resource pools at the back-end, while delivering exceptionally powerful, on-demand IT services to front-end users. At present, academia has not yet established a unified, standardized definition of cloud computing; different conceptualizations exist. For instance, the Cloud Computing Expert Committee of the Chinese Institute of Electronics defines cloud computing as a publicly participatory computing model based on the Internet, characterized by dynamic, scalable, and virtualized computing resources delivered as services. Broadly speaking, two definitions emerge: narrowly defined, cloud computing refers to the architecture and service delivery model for IT infrastructure, utilizing network computing and other technical means to allocate, scale, and supply data or computing resources "like tap water" on demand; broadly defined, it emphasizes this utility-style delivery model, encompassing any service that can be rapidly allocated, scaled, and supplied on demand through network channels.

China's broadcasting and television monitoring enterprise began in the 1950s on a small scale with purely manual monitoring methods. Through gradual development and improvement, integrating resources, and establishing new monitoring centers, the field has transitioned from traditional to new media, achieving unified monitoring, supervision, and surveillance across cable, wireless, satellite, and Internet platforms. These achievements have been made possible by advances in computer technology, communications technology, network technology, and automation technology. Now, the wave of cloud computing is ushering in a major technological transformation for broadcasting and television monitoring. This section examines the security threats facing cloud computing for broadcasting monitoring data and proposes corresponding countermeasures.

2.1 Data Leakage

For security reasons, cloud computing networks for monitoring data are deployed as internal networks physically isolated from the Internet, thus preventing conventional data leakage. However, scholars in Europe and the United States demonstrated years ago that screen content could be intercepted and reconstructed in real-time from several kilometers away using antennas to capture electromagnetic radiation. Consequently, electromagnetic protection is critically important. From a security perspective, we must implement comprehensive electromagnetic shielding for all servers and computers comprising the cloud computing infrastructure.

2.2 Data Loss

User errors, hacker attacks, service provider mistakes, and disasters such as earthquakes or warfare can all lead to data loss. In distributed network computing environments, users cannot recover data through traditional physical restoration methods. Additionally, if users accidentally lose their encryption

keys, the very encryption intended to ensure security becomes problematic. The solution lies in implementing database backup mechanisms, maintaining at least one copy of data, with two or more copies for critical information.

2.3 Data Hijacking

If an organization's login credentials are compromised, hackers can eavesdrop on activities and transactions, manipulate data, and return false information to disrupt legitimate user access. While such threats have low probability in our context, they remain possible. One could imagine hackers infiltrating office premises to launch data hijacking attacks. The key to mitigating this threat lies in rigorously protecting login credentials from theft.

2.4 Insecure Interfaces

APIs (Application Programming Interfaces) are pre-defined functional interfaces widely used by cloud administrators to configure and manage cloud services. API management is crucial for ensuring cloud service availability and security for two primary reasons: first, organizations and third parties frequently develop additional services based on APIs, making API management complex as it involves coordination among organizations, third-party developers, and users; second, API publication requires organizations to provide third parties with system access credentials for communication, inevitably increasing system risk.

Organizations must clearly understand how API application, management, monitoring, and adjustment specifically impact cloud security, and strive to prevent security issues arising from poorly secured APIs. Highly secure APIs should simultaneously exhibit four characteristics: strong confidentiality, high integrity, high availability, and clearly defined accountability.

2.5 Denial of Service Attacks

Denial of Service (DoS) attacks involve various methods to disrupt target host services. In traditional IT environments, DoS and Distributed Denial of Service (DDoS) attacks pose enormous challenges to business continuity and are difficult to recover from. Even in the cloud computing era, DDoS attacks have caused substantial damage, such as the major U.S. Internet outage in October of last year and the April attack on Blizzard Entertainment's global Battle.net servers.

Although cloud architecture can effectively control DoS attack impact, large-scale DDoS attacks still severely affect services. Attackers may not completely cripple services but can consume substantial computing resources, dramatically increasing cloud provider operational costs and potentially causing user fees to surge, resulting in "Depletion of Bank" (DoB) scenarios that severely impact customer experience.

2.6 Malicious "Temporary Workers"

As platform operators, cloud service providers must ensure customer data security. However, in practice, provider employees, contractors, business partners, and system inspectors under contract all have greater physical proximity to data-bearing systems than customers. A securely architected cloud service system must implement effective control over data and business permissions to prevent malicious actors within the cloud provider from accessing, stealing, or destroying customer data through high-level access to Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) platforms.

Cloud providers can employ encryption to protect customer data, but only when encryption keys are exclusively held by customers can the system truly be protected against attacks from potentially malicious temporary workers within the service provider.

3. Conclusion

As cloud computing continues to develop, its adoption in the broadcasting industry has become an inevitable trend. This paper aims to stimulate further discussion and provide reference points for the popularization of cloud computing in the broadcasting field.

References

[1] Lin Chuang, et al. Cloud computing security: Architecture, mechanisms and model evaluation [J]. Chinese Journal of Computers, 2013, 36(9): 1765-1768.

[2] Feng Dengguo, et al. Research on cloud computing security [J]. Journal of Software, 2011, 22(1): 71-83.

[3] Chang Yufeng. The impact of cloud computing on news production models [J]. China Media Technology, 2012(21): 37-39.

Author Affiliation: National Press and Publication Administration Radio and Television Monitoring Data Processing Center

Note: Figure translations are in progress. See original paper for figures.