Privacy and Data Security in Cloud Computing

Asis. Prof. Nuri Abrahem Elshamam
Dep. of Information Technology
Asmarya Islamic University
nurishammam67@gmail.com

الخلاصة

أصبحت حماية البيانات وتأمينها مسألة أساسية في بيئة الحوسبة السحابية، ونظرًا لوجود البيانات في أماكن مختلفة، فإن خصوصيتها وأمانها هما العاملين الرئيسيين الذين يثيران قلق المستخدم. ومع ذلك، تعد الحوسبة السحابية واعدة وفعالة، وهناك العديد من التحديات لأمن البيانات التي يجب أن يأخذها مستخدم السحابة في الاعتبار. توضح هذه الورقة هذه التحديات والاستراتيجيات المتبعة لتأمين البيانات والتقنيات المستخدمة لحماية نقل البيانات عبر السحابة. بالإضافة إلى ذلك، سيتم أيضًا التطرق إلى مشاكل الحوسبة السحابية المتعلقة بالأجهزة المحمولة.

Abstract

In the Cloud Computing environment, it becomes an essential issue to protect and secure data. Since data is located in different places, its privacy and security means becoming the two main factors of user’s concern. However, Cloud Computing is promising and efficient; there are many challenges for data security that should be considered by the cloud user. This paper illustrates these challenges, the strategies followed to secure data and the techniques used to protect data transmission over the cloud. In addition to that, Mobile Cloud Computing Issues will be considered too.

Keywords
Cloud Computing, data protection, data security, security issues, privacy issues

Introduction

Data security has consistently been a major issue in IT. It has been considered as an important issue for deploying applications into the cloud. Data security becomes particularly serious in cloud computing environment, because data are scattered in different machines and storage devices including servers, PCs, and various mobile devices such as wireless sensor networks and smart phones. Data security in cloud computing is more complicated than data security in traditional information systems. Once the client host data to the cloud, there should be some guarantee that access to that data will be restricted and limited only to authorized persons. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices, privacy policies, and procedures should take place to assure the cloud users of the data safety [1]. I will discuss the basic concepts behind the cloud and introduce the security issues underlying cloud computing. In particular, I will define the model for data security in cloud computing, focusing on a set of crucial security issues dealing to storing and accessing data in cloud computing; data confidentiality, secure data access, integrity, availability, regulations & compliances, and audition [2].

1. Cloud Computing Security Challenges

Dealing with data, enterprises worry whether they can trust their employees or need to implement additional controls inside the private cloud, and whether third-party providers can provide adequate protection in multiusers environments. There should be also an intensive concern implemented about the safety of moving data between the enterprise and the cloud, as well as the way to ensure that no data remains or lost upon moving to another cloud service provider.

In Cloud Computing Security, there are some challenges that can be listed below;

- Cloud service models with multiple users sharing the same infrastructure.
- Data mobility over the cloud according to certain rules.
- Necessity to protect confidential business, or governmental data.
- Loss of key security and operational intelligence that is needed to secure IT intelligence and risk management.

- Lack of standards about how cloud service providers deal with data exchange over the cloud.
- Types of workers who are not members of your company, but may have control and visibility into your data.

2. Strategies followed to secure data

Traditional models of data security could not provide sufficient protection against **A**dvanced **P**ersistent **T**hreats (**APT**s), privileged users, or other insidious types of security attacks. This compels many enterprises to use **D**atabase **A**udit and **P**rotection (**DAP**) and **S**ecurity **I**nformation and **E**vent **M**anagement (**SIEM**) solutions to protect their data. Some companies implement data security strategies that provide a veritable firewall around the data itself for comprehensive protection. Advanced data security solutions provide them with an early warning system about an attack, render the content unusable, and provide automation and big data analytics to continuously analyze logs and other information about their environment such as security events and data flow. While many enterprises have implemented encryption to protect data, they often overlook inherent weaknesses in key management, access control, and monitoring of data access. If encryption is not securely implemented, it is vulnerable to theft by malicious hackers. In the access control too, if keys are properly protected, but access is not sufficiently controlled, malicious personnel can access sensitive data using the authority of an authorized person. The encryption implementation must provide assurance that the keys are sufficiently protected, it works in concert with other data security techniques to provide a comprehensive protection for data against risk in or out of the cloud. Hence, any data-centric procedure must include encryption, key management, strong access controls, and security intelligence to protect data in the cloud and provide the highest level of security. By implementing these critical tools, enterprises can improve their security means more effectively and efficiently than by focusing exclusively on traditional network-centric security procedures. Best strategies of any enterprise should include protecting sensitive data, establishing duty separation between IT normal operators and IT security ones, ensuring that the use of cloud data conforms to existing enterprise policies, as well as strong key management and control access policies [3].

3. Techniques to protect data transmission over the cloud

While establishing security policies and maintaining control through a centralized management interface, enterprises solve cloud security problem by protecting data inside the operating environment. They can establish access policies and achieve complete control of data in private, public, or hybrid cloud environments. While transitioning to the cloud, both local data within the internal environment as well as cloud-based data within infrastructure or hosted application sites should be properly protected. Enterprises can rapidly deploy data security for cloud applications. Since no modification to the application or database is required, enterprises can securely leverage cloud agility. Data protection and security are the main factors for gaining user’s trust and making the cloud technology successfully used. A number of data protections and data security techniques have been proposed in the research field of cloud computing. However, data protection related techniques need to be further enhanced. Services of cloud computing are provided across the entire computing spectrum. Nowadays, organizations and enterprises are moving and extending their business by adopting cloud computing to lower their cost. This can contribute to free more man-powers to focus on creating strategic differentiation and business division of labor is clearer. The meaning of security is plentiful. Security is the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of unauthorized withholding of information [4].

4. Security in Cloud Computing

While deciding to move to the cloud, one would have to take into consideration some factors such as service availability, security, and system performance. among which the security is the main concern. However, the security issue of Cloud Computing is in fact complicated, which can be explained by the fact that Cloud Computing is built on the top of existing techniques and architectures. In addition to that, the operation model of Cloud Computing will also reshape the trust model when cloud users move their applications from their enterprise area to the cloud. By doing so, cloud users may lose physical control over their applications and data. They have to rely on the cloud service providers for securing data.

4.1 *Security Issues*

Security is considered one of the main issues that must be taken into consideration. If the device gets lost or stolen, the confidentiality of the data stored is also lost. This is applicable to all secondary devices such as flash memory, external disks, where the passwords, PINs, Credentials, Corporate data like customers list, etc. Following are some of the attacks that affect the security issues in mobile cloud computing [5].

A. MOBILE OS

Mobile software vendors must take the responsibility of securing mobile operating system (MOS), which is not an easy job. Security relates not only to the data loss but also to the system down-time.

B. WIRELESS ATTACKS

There are varieties of attacks which leverage the wireless connectivity of the target. Since mobile devices support communication through wireless connection, they are often affected by eaves dropping to extract confidential and sensitive information, such as usernames and passwords.

C. VIRUS/ TROZAN HORSE/ WORM/ SPYWARE ATTACKS

Malware is software that is often masqueraded as a game, patch or other useful third party software applications. It passes into the mobile device as a Trojan which appears to provide some functionality but contains malicious program. Keystroke logging is another type of malware that records keystrokes on mobile device. Using these keystrokes, it captures the sensitive information and sends it to a cybercriminal’s website or email address. Malware also includes viruses, spyware etc.

D. OVERBILLING ATTACK

In this attack, the attacker sends random traffic to the IP address of the victim. The provider would not check if the traffic was requested by the victim or not, and bill the victim for it. The attack utilizes the 'always on' characteristics of GPRS, which is billed by the amount of traffic instead of the usage time.

E. INSIDER ATTACK

It is a non-technical attack. Due to the lack of awareness of security policies, many security breaches occur. Even though corporate has Standard Policies for mobile device security, employees don't understand the risks associated with it. In relation to those attacks, their effect can be reduced to the minimum level. Installing and running security software are the simplest ways to detect security threats.

4.2 *Privacy Issues in Mobile Cloud Computing*

Mobile Computing allows users to share information, data, applications, and software over networks. One unique privacy challenge for mobile devices is its utilization of location dependent information in support of dynamic location queries [6]. Due to their nature, mobile devices must support heterogeneous networking. This requires the device to support automatic discovery and configuration of local network services, such as local printers and DNS servers [7]. Location based services (LBS) faces a privacy issue on mobile users provide private information such as their current location. This problem becomes even worse if an adversary knows user's important information.

5. Data Security in Cloud Computing

Before transferring to the cloud, users need to identify data objects to be secured and classify data based on their security issues, and then define the security policy for data protection as well as the policy enforcement mechanisms. For most applications, it would be more convenient and cost-effective to move large volumes of data to the cloud by mobile media than transmitting over the Internet. Data objects may also include user identity information created by the user management model, service audit data produced by the auditing model, service profile information used to describe the service instance(s), temporary runtime data generated by the instance(s), and many other application data.

The basic security services for data security include:

1) ***Data confidentiality assurance:*** This service protects data from being disclosed to unauthorized parties. In Cloud Computing, data confidentiality is a basic security service to be considered. Although different applications may have different requirements in terms of what kind of data to be confidentially protected, this security service could be applicable to all data objects mentioned above [8].

2) ***Data integrity protection:*** This service protects data from malicious modification. Such a security service would have an intensive care for cloud users. When auditing cloud services, it is also critical to guarantee that all the audit data are authentic since these data would be of legal concerns. This security service is also applicable to all data objects mentioned above.

3) ***Guarantee of data availability:*** This service assures that data stored in the cloud is available on each user retrieval request. For long-term data storage services, data availability assurance is the most important service because of the increasing possibility of data loss or damage over the time.

4) ***Secure data access:*** This security service is to limit the disclosure of application data to unauthorized persons. In practical applications, disclosing data content to unauthorized users may threat the cloud user's business goal. For better protection of sensitive data, cloud users may need fine-grained data access control so that different users may have access to different type of data. This security service is applicable to most of the data objects mentioned above [9].

5) ***Regulations and compliances:*** In practical data applications, access and storage of sensitive data may have to achieve specific compliance. In addition to that, the data location would be of a great concern due to export-law violation issues. Cloud users should necessarily review these regulation and compliance issues before moving their data over the cloud [10].

6) ***Service audition:*** This service informs cloud users how their data are accessed and serviced. In the case of local storage, it is so simple to audit the system data. In Cloud Computing, however, it requires the service provider to support trustworthy transparency of data access.

Conclusions

Dealing with data protection in Cloud Computing, the two main factors to be taken in account are data security and privacy issues. Reducing data storage and processing cost is a necessary requirement for any organization, while analysis of data and information is always the most important tasks in all organizations for decision making, hence no organizations will transfer their data to the cloud until a trust is built between the cloud service providers and consumers. This paper illustrated number of techniques about privacy and data security to build trust between cloud service providers and consumers. Every cloud service(s) seeker either an individual or a company should ask the right questions to the cloud provider before hosting their data or applications on the cloud. Prospective cloud providers should let you know if they have good security policies and procedures and if the infrastructure meant to host your data shared with lots of other users, or will it be segregated by virtualization. As many companies move their data to the cloud the data undergoes many changes and there are many challenges to overcome. To be effective, cloud data security depends on more than simply applying appropriate data security procedures and countermeasures.

References

[1] A. Monaca, "A View Inside the Cloud," 7 June 2012. [Online]. Available: http://theinstitute.ieee.org/technology-focus/technology-topic/a-view-inside-the-cloud. [Accessed June 2013].

[2] https://www.ibm.com/cloud/learn/cloud-computing.

[3] http://www.vormetric.com/data-security-solutions/ overview/index.html

[4] A. Aviˇzienis, J. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” IEEE Transactions on Dependable and Secure Computing, vol.1, no.1, pp.11–33,2004.

[5] Naveen and Soniya, International Journal of Scientific & Engineering Research Volume 8, Issue 5, May-2017.

[6] Bal, G¨okhan. “Revealing Privacy-Impacting Behavior Patterns of Smartphone Applications”. Goethe University Frankfurt, Germany, April 2012.

[7] Satyanarayanan, M. “Fundamental Challenges in Mobile Computing”. School of Computer Science, Carnegie Mellon University, July 1999.

[8] Subedari Mithila, P. Pradeep Kumar, ”Data Security through Confidentiality in Cloud Computing Environment”, Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011.

[9] Zaigham Mahmood, “Data Location and Security Issues in Cloud Computing”, Proceedings of International Conference on Emerging Intelligent Data and Web Technologies-2011.

[10] William Stallings, “Network Security Essentials Applications and Standards”, Third Edition, Pearson Education, 2007.