International Journal of Grid and Distributed Computing
Vol. 9, No. 1 (2016), pp.49-56
http://dx.doi.org/10.14257/ijgdc.2016.9.1.05

Security Techniques for Data Protection in Cloud Computing

Kire Jakimoski

Faculty of Informatics, FON University, Skopje, Republic of Macedonia
kire.jakimoski@fon.edu.mk; kire_jakimoski@yahoo.com

Abstract

Cloud computing has a lot of security issues that are gaining great attention nowadays, including the data protection, network security, virtualization security, application integrity, and identity management. Data protection is one of the most important security issues, because organizations won't transfer its data to remote machines if there is no guaranteed data protection from the cloud service providers. Many techniques are suggested for data protection in cloud computing, but there are still a lot of challenges in this subject. The most popular security techniques include SSL (Secure Socket Layer) Encryption, Intrusion Detection System; Multi Tenancy based Access Control, etc. Goal of this paper is to analyze and evaluate the most important security techniques for data protection in cloud computing. Furthermore, security techniques for data protection will be recommended in order to have improved security in cloud computing.

Keywords*: access control, authentication, authorization, cloud computing, confidentiality, data protection.*

1. Introduction

Cloud computing includes a group of computers that are jointly used to provide different computations and tasks. Cloud computing is one of the most important IT paradigms in the last few years. One of the key benefits that is offered from this IT technology for the companies is reduced time and costs on the market. Cloud computing is providing companies and organizations to use shared storage and computing resources. It is better than to develop and operate with the own infrastructure. Cloud computing also provides organizations and companies to have a flexible, secure, and cost-effective IT infrastructure. It can be compared with the national electric grids that permit organizations and homes to plug into a centrally managed, efficient and cost-effective energy source. Main corporations including Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP, Oracle, and Novell have invested in cloud computing and propose a range of cloud-based solutions to individuals and businesses.

There are different types and models in cloud computing regarding the different provided services. So, the cloud computing involve public cloud, private cloud, hybrid cloud, and community cloud. Service delivery models, on the other hand, could be categorized as SaaS (Software as a service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). Cloud computing could be usually classified by two ways: by cloud computing location, and by the offered types of services. By the location of the cloud, cloud computing is typically classified in: public cloud (where the computing infrastructure is hosted by the cloud vendor); private cloud (where the computing infrastructure is assigned to a specific organization and not shared with other organizations); hybrid cloud (the usage of private and public clouds together); and community cloud (it involves sharing of IT infrastructure in between organizations of the same community) [1]. If the classification is based on type of offered services, clouds are classified in these ways: IaaS (Infrastructure as a service), PaaS (Platform as a Service), and Software as a Service (SaaS) [1].

ISSN: 2005-4262 IJGDC
Copyright ⓒ 2016 SERSC

Cloud computing as a novel technology for processing and transferring data electronically is nowadays used in almost every computer system. It runs on a network infrastructure that is opened for different types of attacks. DDoS (Distributed Denial of Service) is one of the most known attacks that are used. Syn cookies as well as limitation of the users that are connected with the cloud technology to the server could be used as measures for stopping Distributed Denial of Service.

Other type of attack on the cloud computing technology is man in the middle attack. Secure Socket Layer (SSL) is security technique to overcome this kind of attack. So, if this security technique is not configured properly, authentication of the client and the server might not perform as it should to protect the users of the cloud technology from man in the middle.

So, security challenges of data protection when using cloud computing must be appropriately solved and minimized. When we utilize cloud computing we run our software on hard disks and CPUs that are not in front of us. That is why users are having more doubts about the security issues when they are using this technology. So, a lot of different types of attacks could happen in the cloud technology. Besides the above mentioned, most known attacks involve phishing, IP spoofing, message modification, traffic analysis, IP ports, etc. There are a lot of security techniques for data protection that are accepted from the cloud computing providers, and they all provide authentication, confidentiality, access control and authorization.

2. Authentication in Cloud Computing

Authentication in cloud computing ensures that the proper entity or person is getting access to the provided data from the cloud technology provider. When authentication is ensured in the cloud computing, it means that the user's identity is proved to the cloud service provider when accessing the stored information in the cloud. Public and private types of cloud are using various designs for authentication with RSA. RSA cryptosystem accepted different models for authentication like two factor authentication, knowledge-based authentication, and adaptive authentication. AWS (Amazon Web Services) is concentrated on the confidential information transfer between the web server and the browser including virtual private cloud [2]. In this context different authentication schemes are implemented, such as multifactor authentication, access management, AWS identity. Figure 1 presents the multifactor authentication procedure from AWS. There is also a technique for authentication that is allowing users to use just one password in order to authenticate themselves to multiple services [3]. With this technique the users are prone to honeypot and dictionary attacks. The most famous IT companies are using this technique like Google, Microsoft, and Facebook.

In order to enable authentication of the required IP addresses to some external site when cloud computing is used, Proxy setting could be used. Proxy URL enables only trusted sites to be accessed.

Hence, we can conclude here that for data protection of the cloud technology the most used authentication mechanisms are: knowledge based authentication, two factor authentication, adaptive authentication, multifactor authentication and single password authentication. Knowledge based authentication, two factor authentication and adaptive authentication are enabled with RSA and benefits of them are reduced costs and improved security.

Multifactor authentication is used by AWS to secure the data in the cloud. Benefits of this authentication mechanism are that it enables identity management and access management. Single password authentication is used from Facebook to enable data protection in the cloud. Benefits of this kind of authentication mechanism are that it enables security from honeypot attacks and dictionary attacks.

 Copyright ⓒ 2016 SERSC

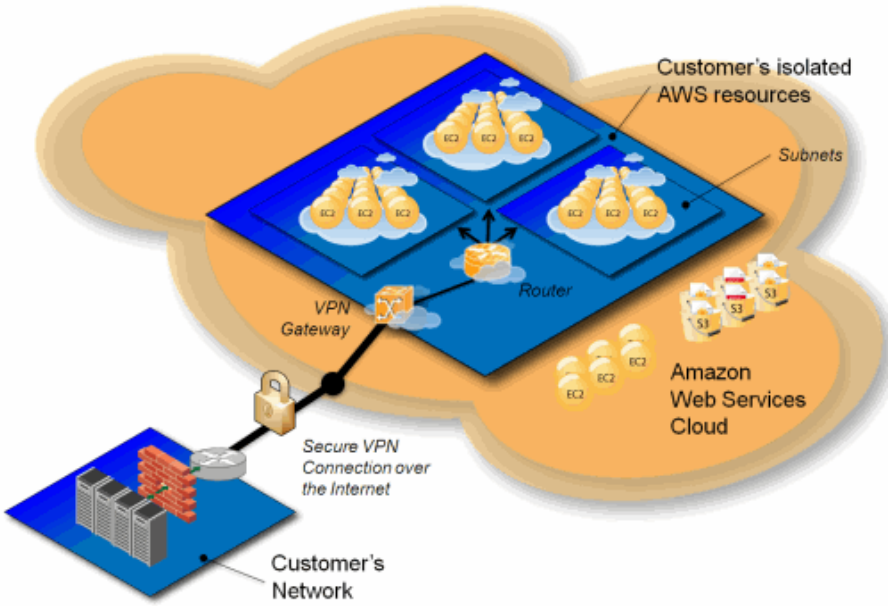

Figure 1. Multi-Factor Authentication from AWS

3. Confidentiality in Cloud Computing

Confidentiality is one of the most important security mechanisms for users' data protection in the cloud. It includes encryption of the plaintext in cipher text before the data is stored in the cloud. This technique protects the users' data and even cloud service providers cannot modify or read the content that is stored in this way in the cloud.

This kind of protection is offered from Dell data protection and encryption where users' data is protected when it is stored on the external drive or media. Encryption could be done either using software or hardware. Great benefit of this kind of protection is that users don't need to bother with the enforce policies of Dell data protection and encryption. Dell also uses Transparent File Encryption to control the users that are accessing the data.

Wuala cloud is another vendor that enables encryption for the data in the cloud. Encryption is enabled here before personal computers are sending the data to the cloud. This is excellent protection because even the provider cannot access the data. Authors in [4] are proposing encryption method for cloud computing that is based on hierarchical attribute. This proposed security technique for confidentiality in cloud computing gives high performances and great access control. Authors in [5] are proposing encryption method where owners can control the data they possess in the cloud.

Confidentiality is also provided by the vendor Online Tech which obtains confidentiality in the cloud computing using encryption methods (like Full Disk Encryption) that encrypt stored data on hard disk throughout the booting process. Whole Disk Encryption is also used for encrypting the data with the well known AES (Advanced Encryption Standard) algorithm. If the device that is using cloud computing technology is lost or stolen there is also a bit locker password which protects the data on the lost or stolen device.

Hence, we can conclude in this section that confidentiality is very important for protecting the data in the cloud and different vendors offer different security techniques for ensuring the confidentiality. Per example, DELL offers hardware and software based encryption, as well as transparent file encryption. The benefits of this kind of encryption techniques are that they are easy to implement and intervention of the user is not needed. Wuala is using encryption techniques on personal computers and this method for encryption in the cloud gives advantage of the users for accessing the data. Online Tech

Copyright ⓒ 2016 SERSC

offers Full Disk Encryption and Whole Disk Encryption in order to enable confidentiality of the data in the cloud. Benefits of these encryption methods are that data that are partitioned could be decrypted and data is encrypted at rest.

4. Access Control in Cloud Computing

Access control is very important security mechanism for enabling data protection in the cloud computing. It ensures that only authorized users have access to the requested data that is stored in the cloud. There are different security techniques that enable proper access control in the cloud computing. Intrusion detection systems, firewalls as well as segregation of obligations could be implemented on different network and cloud layers. Firewall is enabling only content that is filtered to pass through the cloud network. Firewall is usually configured according defined security policies set by the users. Firewalls are usually related to Demilitarized zones (DMZ) which provide additional security of the data.

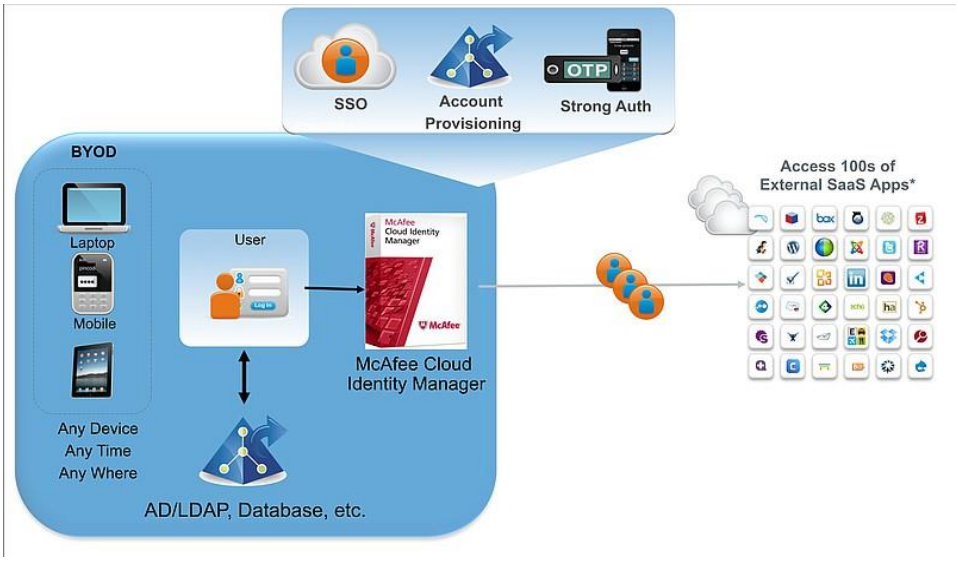

Figure 2. McAfee Cloud Identity Manager

McAfee is vendor that enables access control in the cloud computing. It offers different methods for access control as McAfee Single Sign On, McAfee Web Gateway, and McAfee one time password. These kinds of security techniques enable policy management and prevention of data to be lost. Figure 2 presents the cloud identity manager offered by McAfee for cloud computing.

Fujitsu is another vendor that offers access control with different authorization techniques like Virtual System Management and Central Management Authorization. These security techniques are effective for preventing cross-site scripting and injection attacks.

5. Authorization in Cloud Computing

Authorization in the cloud computing is important for the users when they login to some cloud service because it enables prove of their identities. So, authorization is usually employed after the authentication. Oracle Database Vault is an example of security technique that enables authorization in the cloud. This security technique is offered by the vendor Oracle. Application data from different administrative users are protected with this authorization method. Authors in [6] use policy based authorization method that is

 Copyright ⓒ 2016 SERSC

protecting the privacy of the users enabling them to set privacy policies by themselves. In this way users are protecting their data in effective way from unauthorized access.

Authorization in the cloud is also offered by VMware which integrates service providers' policies with the corporate directories and different policies. Certificates or soft tokens are used for authorization of the end users in secure way. OASIS Cloud authorization enables security techniques based on management of authorizations. Users logs are maintained with this method which give location of the users and information about the used devices from the users.

6. Recommendations for Improved Data Security in Cloud Computing

We will mention now the most important recommendations in order to have secured cloud environment. One of the recommendations is a cloud consumer to be ensured that efficient governance, risk and compliance processes exist. This means that security controls must exist in cloud computing similar to those used in traditional IT systems. Anyway, cloud computing may have different risks to an organization than traditional IT solutions. So, when the organization uses cloud computing, it is very important consumers to comprehend the level or risk tolerance.

Other recommendation is that cloud consumers must be assured that the cloud provider has functionality and processes that manages who has access to the consumer's applications and data. This is essential in order to have assurance that access to the cloud environment is managed and controlled. So management of people, roles and identities is crucial to be implemented in the cloud environment. When some consumer application is moving to the cloud it is very important the provider to allow the consumer to assign their user identities into access groups and roles that reflect their business and operational security policies [7].

Very important factor for secure cloud environment is insurance of adequate protection of data and information. Security considerations must be applied to data that is held on some form of storage system, as well as to data that is transferred over some communication link. Data for cloud computing have various forms of risk as risk of theft of unauthorized disclosure of data, risk of tampering, risk of loss or unavailability of data. In order to secure the data in cloud computing, adequate controls are needed as: consideration of all forms of data and privacy requirements, appliance of confidentiality, creation of data asset catalog, integrity and availability, as well as appliance of identity and access management [8].

Important recommendation to secure the data on the cloud is to be assured that cloud networks and connections are secure. Cloud consumers must be aware of internal network attacks like confidentiality breaches or disclosure of confidential data, integrity breaches as unauthorized modification of data, or availability breaches like denial of service. That is why it is important for cloud consumers to evaluate the internal network controls of the cloud service provider regarding their requirements and security policies that might have. One of the key recommendations is also the evaluation of security controls on physical infrastructure and facilities. Cloud consumer is in charge to get assurance from the provider that appropriate security controls are taken into consideration, because in the cloud computing, the infrastructure and facilities are usually controlled and owned by the cloud service provider.

6.1. Data Protection in the Cloud

Protection of data in the cloud is best accomplished when we have a mixture of encryption, data loss prevention techniques, integrity protection, authentication, and authorization techniques. When vendors and enterprises use cryptographic algorithms, it is very important these algorithms to be well known as identified by NIST. It is also

Copyright ⓒ 2016 SERSC

useful to have re-evaluation on an annual basis of the algorithms and keys that are utilized in order to be assured about the strength of the protection.

It is also very important organizations or corporations that are using cloud technology to understand the security controls that are related to the data in the cloud multi-tenant environment. Hardware Security Modules or HSMs are recommended to store the keys.

6.2. Proper Usage of Administrative Privileges

The organization that includes cloud computing should minimize administrative privileges and only to utilize administrative accounts when they are needed. Automated tools should be used to inventory all administrative accounts and validate that each user that has administrative privileges on laptops, desktops, and servers is authorized by senior executive. All administrative passwords should be complex including numbers, letters and special characters intermixed, without dictionary words in the password.

All default passwords for operating systems, applications, firewalls, routers, wireless access points, and other systems should be changed before deploying any new devices in the networked systems. Service accounts also should have long and difficult to guess passwords changed on a regular basis. Passwords in storage should be encrypted or hashed. Hashed passwords should follow the guidance supplied in NIST SP 800-132 or similar guidance.

Access control lists should be utilized to make sure that administrative accounts will be used only for system administration activities. Administrator must use unique and different passwords for their administrative and non-administrative accounts. This task can be fulfilled through policy and user awareness.

Operating systems should be configured in a way that passwords can't be reused in the next six months. When unsuccessful login to administrative account is tried, the system should issue a log entry and alert.

Multifactor authentication should be used for all administrative access, as well as domain administrative access. This kind of authentication could include different techniques, like using smart cards with certificates, biometrics, One Time Password (OTP) tokens *etc*. When enabling multifactor certificate-based authentication, the private keys must be protected using strong passwords or stored in secure and trusted hardware tokens. Administrators should be required to access the system with using non-administrative and fully logged account.

6.3. Wireless Access Control of the Data

Organization that is using cloud computing and possess wireless network(s) should employ commercial wireless tools for scanning, detection and discovery and commercial wireless intrusion detection systems. The security official from the organization should regularly capture wireless traffic from the borders of a facility and utilize commercial and free analysis tools to resolve whether the wireless traffic was transferred using the encryption that the organization authorizes or some weaker protocols. In this context the security officials should also use remote management tools on the wired part of the network in order to extract information about the wireless potential and devices connected to the systems that are managed.

6.4. Data Recovery in Cloud Computing

It is very important each system that is using cloud computing to has automatic back up procedure at least once a week, and for systems that store sensitive information even more frequently than once a week. The overall backup procedure should even include the operating system, application software and data on the machine. Multiple backups over time could be also implemented and policies of backup should be in compliance with any official or regulatory requirements.

 Copyright ⓒ 2016 SERSC

It is also recommended once per quarter a testing team to make evaluation of a random sample of system backups with trying to restore them on a test bed environment. Systems that are restored should be confirmed to guarantee that the operating system, application and data from the backup are all functional and intact. Hence, if there is malware infection, procedures of restore should utilize backup version which is considered to predate the original infection.

6.5. Boundary Defense of the Data in the Cloud

Boundary defense in one organization that is using cloud computing could be implemented by using free or commercial IDS and sniffers to detect attacks from external sources to the internal systems of DMZ of the organization or vice versa. It is also beneficial to deny communications with known malicious IP addresses or limit access only to trusted sites. Organization should include network based IPS devices as an addition to IDS to block known bad signatures or behavior of attacks. Two-factor authentication is obligation when using remote login access as VPN. Only DMZ systems should communicate with private network systems of the organization via application proxies or application-aware firewalls over authorized channels. Anomalous activities could be easily detected if NetFlow collection and analysis to DMZ network is deployed.

7. Conclusion

The main goal of this work was to analyze and evaluate the security techniques for data protection in the cloud computing. For that purpose we analyzed and evaluated the most important security techniques for data protection that are already accepted from the cloud computing providers. We classified them in four sections according to the security mechanisms that they provide: authentication, confidentiality, access control and authorization.

So, we successfully answered on the key questions in the cloud technology, or simply said should cloud computing be trusted in data protection. We can conclude that if all recommended measures are taken into account providing authentication, confidentiality, access control and authorization, then the cloud computing can be trusted in data protection.

We also focused on the security issues that should be taken into account in depth in order to have proper data security in the cloud. We recommended important security measures relating to data protection in the cloud that must be taken into account. We also proposed a lot of issues that should be considered in order to have improved data security in the cloud computing, like proper usage of administrative privileges, wireless access control of the data in systems that use wireless networks, data recovery and boundary defense in the cloud.

References

[1] L. Badger, T. Grance, R. Patt-Corner and J. Voas, “Cloud computing synopsis and recommendations (draft), nist special publication 800-146”, Recommendations of the National Institute of Standards and Technology, Tech. Rep. **(2011)**.
[2] U. Khalid, A. Ghafoor, M. Irum, and M. A. Shibli, “Cloud based secure and privacy enhanced authentication & authorization protocol”, Procedia Computer Science, 22, **(2013)**, 680-688.
[3] T. Acar, M. Belenkiy and A. Küpçü, “Single password authentication”, Computer Networks, 57(13), **(2013)**, 2597-2614.
[4] G. Wang, Q. Liu, J. Wu and M. Guo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers”, Computers & Security, 30(5), **(2011)**, 320-331.
[5] C. I. Fan and S. Y. Huang, “Controllable privacy preserving search based on symmetric predicate encryption in cloud storage”, Future Generation Computer Systems, 29(7), **(2013)**, 1716-1724.
[6] D. W. Chadwick and K. Fatema, “A privacy preserving authorisation system for the cloud”, Journal of Computer and System Sciences, 78(5), **(2012)**, 1359-1373.

Copyright ⓒ 2016 SERSC

[7] M. Hange, "Security Recommendations for Cloud Computing Providers", Federal Office for Information Security **(2011)**.
[8] G. Brunette and R. Mogull, "Security guidance for critical areas of focus in cloud computing v2", Cloud Security Alliance, **(2009)**, 1-76.

Authors

Kire Jakimoski, He received his B.Sc. degree in the field of Telecommunications from the Military Academy "Mihailo Apostolski" in Skopje, R. Macedonia in 2002, M.Sc. degree in Electrical Engineering in the field of Telecommunications from the Ss. Cyril and Methodius University in Skopje, R. Macedonia in 2007, and Ph.D. in technical sciences from the Ss. Cyril and Methodius University in Skopje, R. Macedonia in 2013. From 2002 to 2006 he works as an Officer for Telecommunications in the Ministry of Defense in the Republic of Macedonia. From January, 2006 to March, 2012 he works as an adviser for information security in the Directorate for Security of Classified Information in the Republic of Macedonia. From March, 2012 he is with the Faculty of Informatics, FON University in Skopje. Also, he is an author/co-author of around 30 published research papers and one book. He is an Assistant Professor and Vice Dean at the Faculty of Informatics, FON University in Skopje, Macedonia. His research interests include Wireless and Mobile Networks, Heterogeneous Wireless Networks, Computer Networks, Digital Telecommunications, Information Security.

 Copyright ⓒ 2016 SERSC