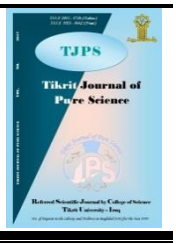
Tikrit Journal of Pure Science 23 (4) 2018

ISSN: 1813 – 1662 (Print)
E-ISSN: 2415 – 1726 (On Line)

TJPS

TIKRIT JOURNAL OF PURE SCIENCE

Journal Homepage: http://main.tu-jo.com/ojs/index.php/TJPS/index



Solutions of diagnosis of security issues and attacks for storage in cloud computing

Ahmed Ibrahim Turki [1] , Qasim Mohammed Hussein[2]

[1] *Department of Physics , College of Education , University of Samarra , Samarra , Iraq*
[2] *Department of Control, College of Petroleum and Minerals Engineering, University of Tikrit , Tikrit , Iraq*

ARTICLE INFO.

Article history:
-Received: 16 / 11 / 2017
-Accepted: 27 / 2 / 2018
-Available online: / / 2018

Keywords: Cloud computing, Cloud security, Storage based attacks, storage models, Denial-of-service Countermeasures.

Corresponding Author:

Name: Ahmed Ibrahim Turki
E-mail:
ahmed.ibrahim@uosamarra.edu.iq

Tel:

Abstract

Cloud computing is technique cost-effective, flexible, and convenient in remote access to applications and storage services, making it easy to provide information technology services and business across the Internet. Nevertheless, the use of cloud computing is an additional source of security risk due to third-party outsourcing, as makes maintaining the privacy, availability and security of data is very difficult. Cloud computing has many of its supporting technologies (virtualization, Web 2.0, service-oriented architecture), which inherits many security issues and makes them susceptible to attacks. Most of the previous work focused on storing data in the cloud without taking security issues and attacks into consideration. In this paper, we provide an analysis of security issues in cloud storage and possible solutions. With regard to the attacks on the data stored in the clouds, parametric comparison including all the details and countermeasures are provided. Finally, this paper provides a significant contribution to building a secure cloud environment for data storage, its privacy and recovery in disaster situations.

1- Introduction

Cloud computing is a generation of distributed computing that provides widespread access to the network, self-service on demand, quick flexibility, resource pooling (e.g. services, applications, storage, networks, servers), measured service and saving time [1]. Store sensitive data and applications in the cloud environment is a concern for companies and organizations because they are not under their control. In order to reduce these concerns, ensure that customers still have the same privacy security controls on their data, services and applications, and be assured by the cloud provider [2]. These data can also be exposed to attacks that lead to Infringement of data protection, in addition to denial or theft of service or lack of service to all customers [3]. In this section, many previous papers that dealt with the security aspect of cloud computing will be presented and gaps will be identified. The paper [4] provided a classification of many security issues related to cloud security. Several recommendations have been made for various open issues that are important in the research field. The paper [5] addresses the issue of privacy in the cloud of electronic health only. Provided countermeasures to the privacy issue, which is not considered a solution to all security problems. The paper [6] addresses several security issues such as legal security, compliance, architectural security, and security of communications. Several unresolved issues have been discussed so far. The paper [7] Only security issues were discussed in private and public clouds. In addition to discussing access control issues, data storage issues, availability of services, without providing solutions to these security issues.

In this paper, we have provided several security issues related to cloud storage to cover the gaps in previous work above. This paper also provides appropriate solutions, summarized in Table 1. In addition, cloud storage attacks that have not been addressed in most previous research have been identified with a parametric analysis of these attacks that includes all information including countermeasures.

2- Selection of resource

The selection of sources of this paper relies on researches and scientific expertise authors. Thus, there are some limitations and conditions have been

adopted: The sources must be available on the Internet as well as written in English. For this reason, the following sources have been adopted: Google Scholar, ScienceDirect, ACM digital library, springer, and IEEE digital library. In addition to the above, there are also other restrictions that have been adopted (influencing factor, important journals, famous authors, and receiving cites). The approved studies include issues linked to cloud security, threats, attacks, risks, and vulnerabilities.

3- cloud computing

According to U.S. NIST cloud computing " A model for enabling on-demand network access, convenient, and ubiquitous to a shared pool of services (like, services, applications, storage, servers, networks), Which can be used with minimal administrative effort at all times and places. cloud computing is the result of great inventions in networking, Web 2.0, security, content outsourcing, storage, grid computing, distributed computing, utility computing, and virtualization. It has five basic characteristics: measured service, rapid elasticity, resource pooling, broad network access, on demand self-service [8]. Cloud services can be classified into three delivery/service models: IaaS, PaaS, SaaS. There are also four models in cloud computing: private, public, hybrid, and community [9].

4- Analysis of security issues in cloud storage

The security issues associated with storage of data within the cloud and its solutions will focus. Because data is one of the most important parts of cloud computing. It should be unbreakable and isolated to the customers. However, customers are either irresolute to provide their information or have a permanent trepidation of losing it and falling into bad hands, or of unexpected consequences that arise during processing or manipulation. Therefore, data must be confidential at all stages of processing, permanently stored to update records, and must be consistent during calculations. The main problem with third-party storage or remote storage is that the data owner does not know the cloud storage location, does not realize what will happen to its data after storing it in the cloud. The security mechanisms used to protect cloud data are also unknown.

There are many security topics, and security issues like Data warehouse, Un-trusted computing, Malware, Cloud data recycling, Cryptography, and Data and service availability that affect cloud storage, many have been done on cloud storage [11-16] respectively. Table 1 presents a summary of these topics and its solutions by reliable and efficient storage technologies in the cloud.

Table 1: A comprehensive and detailed study of cloud storage

Security topics	Security issues	Security solutions
Data warehouse	Loss of control, remote data storage	Use a robust cloud storage system
	Data locality, data pooling	Use FADE system
	Multi-location	Use SecCloud protocol to preserve stored data
	composite model for integrity checking	
Un-trusted computing	Malicious users, Top down SLAs, slowdowns, downtimes	Non interactive solution
	Root level error in backup, Dishonest computing, restoring and Migration problem	Use low cost and light solutions for electronic banking services
Malware	Failed to Anti - Virus - based Signature, Malware based signature, Malware botnet attack	Use SnortFlow
Cloud data recycling	Deficient enforcement of data destruction policies, Drives die without backup	Keep data without deleting it
	Discard unused hard drive	
	Hard disk usage by multi-tenant	
	recycling of Resource	
Cryptography	Insecure cryptography technique, weak key management, incorrect cryptography algorithms	Encryption preservation of the system
	Dictionary and Brute force attack	Use cryptographic algorithms
service and Data availability	fake resource usage	Mechanisms to ensure data availability
	Cloud interruption	Proxy re-encryption system
	Hardware fault issue or Hardware availability	

4.1 Security solutions: In this section, we provide a brief explanation of each security solution for cloud storage security issues mentioned in Table 1

4.1.1 Security solutions for Data warehouse:

Use specialized techniques to protect data within the cloud (from owner to user), through three basic encryption standards: integrity, confidentiality, and availability. By using data security measures such as MAC, SSL 128-bit, and searchable encryption. As well as use a (FADE) system to secure data, where controls access to data based on authorization. Linking outsourcing files that have special access policies, and deleting files to prevent their retrieval to any unauthorized person. Moreover, use SecCloud protocol to link secure computation auditing with secure storage. And achieving probabilistic sampling techniques, batch verification, and privacy cheating discouragement.

4.1.2 Security solutions for Un-trusted computing: Using a protocol can allow the provider to return a non-interactive directory. It also provides privacy for customer input and output. In addition to the use system hPIN/hTAN that dependent on (a random number generator and a cryptographic hash function) , Which is used to counter the various threats to electronic banking systems. Where is considered a low-cost and lightweight solution, as complex systems suffer from software bugs and a lot of security vulnerabilities.

4.1.3 Security solutions for Malware: Use SnortFlow to detect Intrusion, penetrations, and deploy countermeasures. Which provides support through monitoring packet logging modes and packet sniffing, Furthermore; it provides analysis for NIDS mode. Alerts when malware is captured by using components logger, detection engine, pre-processor, and packet sniffer.

4.1.4 Security solutions for Cloud data recycling: Secure data deletion by many approaches such as the file system, the device driver, user-level applications, etc. Where the secure deletion feature is added to the physical medium interfaces by these approaches.

4.1.5 Security solutions for Cryptography: Use modular order-preserving encryption, which is a development of the order-preserving symmetric encryption, which does not allow leaking any information about the location of the plain text. In addition, use cryptographic algorithms to maintain private information retrieval, homomorphic encryption, proofs of irretrievability, broadcast encryption, and short signatures.

4.1.6 Security solutions for Service and Data availability: Use of a mechanism that ensures the integrity of flexible distributed storage, through the distribution of computerized data and the use of the homomorphic token. This mechanism ensures that the computation cost is reduced and communications made lightweight. As well as support for safe and dynamic operations on external data, including append, deletion, and block. finally, use a time-dependent proxy re-encoding scheme (TimePRE) to enable user access until expiration within a predetermined time period. This procedure allows the integration of the concept of time between proxy re-encryption and attribute-based encryption.

5- Storage-based attacks

Private data stored on storage devices may be stolen by a malicious inside or outside attacker. Many vulnerabilities are exploited to access sensitive information and manipulate their data. In order to avoid this, a strict control mechanism is implemented. There are two types of storage based attacks as presented below:

5.1 Data deduplication

Bandwidth can be increased and minimizing storage requirements by data deduplication, but this makes it possible to know the contents of files. It establishes a communication channel to access it through malware. When there are a specified number of copies of the file, one can only delete data deduplication in order to mitigate and reduce the risk of exploitation data deduplication [16].

5.2 Data scavenging

File systems do not remove data that has been completely erased from storage devices. The data can be retrieved by the attacker and this process is called scavenging data. Many different techniques in anti-data scavenging are detected [17].

6- Effects of attacks

The attack on the cloud has effects that may cause deterioration in the availability of services and data on platform of the cloud. These effects can be described as shown below:

6.1 Infringement of data protection

Data that is made available to users in violating their protection by other than data owners. A large number of threats can violate the protection of data through various technologies such as third-party clouds or data deduplication [18].

6.2 Denial-of-service

An attacker targets the cloud platform to disable services provided to users. For example but not limited to, the insidious insider can seize and occupy resources, deprive other clients of resources and respond to their requests with unavailability of resources [19].

7- Comparative analyze of attacks and their countermeasures

Services are provided through the cloud platform using the service delivery model. The various components in each layer of the service model are exploited by the attacker, for malicious purposes such as degradation of the service and Infringement of data protection. This section contributes to research by analyzing, detecting storage-based attacks and countermeasures. Table 2 presents a Comparison attacks, mechanisms, vulnerable components, effects, and layers.

Table 2: Comparison of storage-based attacks in the cloud

Attacks	Mechanisms	Vulnerable components	Effects	layers	Countermeasures
Data deduplication	Communication covert channel and keep track of contents\files through data deduplication	Network and cloud storage	Denial- of-Service, Infringement of data protection	PaaS and SaaS	Encryption, FRS techniques, Digital Signatures
Data scavenging	Data scavenging	Cloud storage	Infringement of data protection	IaaS and SaaS	federated identity management

7.1 Countermeasures for Data deduplication:

7.1.1 Encryption: To secure sensitive data, several encryption technologies are used. Encrypted data is safe when stored or sent. This is done via powerful cryptographic algorithms such as the Advanced Encryption Standard (AES), and Secure Sockets Layer (SSL) is used to protect data during transfer. The use of these algorithms and techniques stops channel side attacks on storage cloud deduplication [20].

7.1.2 FRS techniques: intrusion tolerance is the main objective of this technique to ensure safe cloud storage. By dividing the data into a set of non-important fragments distributed at different locations in the distributed system. Any fragments of these data is not considered important because it is considered incomplete data [17].

7.1.3 Digital Signatures: Digital signature is one of the most important data security technologies, using it with a RSA algorithm to secure the data during transmission. The RSA algorithm was chosen because it is considered one of the most unique algorithms in protecting data stored in clouds.

data deduplication includes three different types of attack are described linked to data deduplication in the cloud that provides storage service. The first attack is to determine the contents of the file stored in the cloud. In the second attack all files that are downloaded to the cloud are selected. In the third attack, a secret communication channel is created to perform malicious activities. This channel makes communication between server and malware possible. The best countermeasures is the use of digital signatures through the use of RSA algorithm. Therefore, the Hash function is applied to create a message digest that is encrypted later. This only ensures that users are authorized to decrypt data

7.2 Countermeasures for Data scavenging:

7.2.1 Dynamic federated identity management: Is a mechanism to make cloud computing easier and safer to enable global scalability that contributes to the global deployment of cloud technologies. Identity management is provided through licensing and authentication mechanisms to monitor access to cloud environments such as the SAMLv2 / ID-FF standards [21].

The best countermeasures for data scavenging is the federated Identity Management System. It is integrated through the participation of many organizations in user information by the Shibboleth System for Identity Management. This is a system of authentication and authorization based on identity. This supports a single sign-on mechanism where identity information can be shared by several organizations with a federation. For this reason, user access does not require continuous login to resources multiple times. The identity management system uses a Security Assertion Markup Language in order to adapt to the dynamic cloud federation. XML used by Security Assertion Markup Language for communicating data for authorization and authentication between enterprises, as well as to provide secure access to cloud resources while maintaining user privacy.

8- Conclusion

Cloud computing offers many benefits such as big storage capacity, rapid deployment, comfortable access to the system any time and everywhere in the world, and cost efficiency. Cloud computing becomes widely accepted around the world. At the same time, cloud computing raises many security issues that become an obstacle to their adoption by organizations and companies. The storage problem is one of the significant security problems facing cloud computing. This feature (storage) allows customers to store their information remotely, unbreakable and isolated. This makes customers in permanent fear of having their data in the hands of pirates, making them reluctant to offer. Storage is therefore one of the concerns of customers. At the same time, all users of the cloud must have an awareness of the attacks that may be exposed to the cloud, especially with respect to storage, because this poses a danger to their data. Awareness of security attacks accelerates the process of accreditation of organizations and companies to cloud computing. In this paper, the security issues and attacks linked to storing data in the cloud are analysis. In addition, various solutions that address security issues linked to storage, as well as countermeasures to address storage-based attacks are presented. This paper includes a detailed tabular presentation of issues, security attacks and solutions. This gives researchers and readers a full visualization of the challenges (issues and attacks) facing cloud storage. At the end of the paper, some of the open future issues are discussed that motivate the academic community and researchers to pay attention to them.

References

1- Cloud computing – A Practical Approach by Velte, Tata McGraw Hill Edition (ISBN-13:978-0-07-068351-8).

2- Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press.

3- Minhaj Ahmad Khan, 2016. A survey of security issues for cloud computing, Journal of Network and Computer Applications 71, 11–29.

4- Fernandes, D.A., Soares, L.F., Gomes, J.V., Freire, M.M., Inácio, P.R., 2014. Security issues in cloud environments: a survey. Int. J. Inf. Secur. 13 (2), 113–170.

5- Abbas, A., Khan, S.U., 2014. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE J. Biomed. Health Inform. 18 (4), 1431–1441.

6- Ali, M., Khan, S.U., Vasilakos, A.V., 2015. Security in cloud computing: opportunities and challenges. Inf. Sci. 305, 357–383.

7- Tari, Z., Yi, X., Premarathne, U.S., Bertok, P., Khalil, I., 2015. Security and privacy in cloud computing: vision, trends, and challenges. IEEE Cloud Comput. 2 (2), 30–38.

8- Omar Ali, Jeffrey Soar, Jianming Yong, 2016. An investigation of the challenges and issues influencing the adoption of cloud computing in Australian regional municipal governments. journal of information security and applications 27-28 (2 0 1 6) 19–34.

9- Ali O, Soar J. Challenges and issues within cloud computing technology. In: The fifth international conference on cloud computing, GRIDs, and virtualization; 2014. p. 55–63.

10-Xiao, Z., Xiao, Y., 2013. Security and privacy in cloud computing. Ieee. Commun. Surv. Tutor. 15 (2), 843–859.

11-Rong, C., Nguyen, S.T., Jaatun, M.G., 2013. Beyond lightning: a survey on security Challenges in cloud computing. Comput. Electr. Eng. 39 (1), 47–54.

12-Li, Q., Clark, G., 2013. Mobile security: a look ahead. Ieee. Secur. Priv. 11 (1), 78–81.

13-Casale, A., 2013. The Dangers of Recycling in the Cloud. TheMakegood. Technologies, Mobility and Security (NTMS), pp.1–7.

14-Sood, S.K., 2012. A combined approach to ensure data security in cloud computing. J.
Netw. Comput. Appl. 35 (6), 1831–1838.

15-Ahuja, S.P., Komathukattil, D., 2012. A survey of the state of cloud security. Netw. Commun. Technol. 1 (2), 66–75.

16-Kaaniche, N., Laurent, M., 2014. A secure client side deduplication scheme in cloud storage environments. In: 2014 6th International Conference on New Technologies, Mobility and Security (NTMS), pp.1–7.

17-Hashizume, K., Rosado, D., Fernndez-Medina, E., Fernandez, E., 2013. An analysis of security issues for cloud computing. Journal of Internet Services and Applications. 4 (1).

18-Tebaa, M., ElHajji, S., ElGhazi, A., 2012. Homomorphic encryption method applied to cloud computing. In: 2012 National Days of Network Security and Systems (JNS2), pp.86–89.

19-Karnwal, T., Sivakumar, T., Aghila, G., 2012. A comber approach to protect cloud computing against xml ddos and http ddos attack. In: 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), pp.1–5.

20-Harnik D, Pinkas B, Shulman-Peleg A (2010) Side channels in Cloud services: deduplication in Cloud Storage. IEEE Security Privacy 8(6):40–47.

21-Sanchez, R., Almenares, F., Arias, P., Diaz-Sanchez, D., Marin, A., 2012. Enhancing privacy and dynamic federation in IdM for consumer cloud computing. IEEE Trans.Consum.Electron.58(1),95–103.

Tikrit Journal of Pure Science 23 (4) 2018 *ISSN: 1813 – 1662 (Print)*
E-ISSN: 2415 – 1726 (On Line)

حلول تشخيص القضايا الأمنية والهجمات للتخزين في الحوسبة السحابية

احمد ابراهيم[1] ، تركي قاسم محمد حسين[2]

[1]قسم الفيزياء ، كلية التربية ، جامعة سامراء ، سامراء ، العراق

[2]قسم السيطرة كلية هندسة النفط والمعادن ، جامعة تكريت ، تكريت ، العراق

الملخص

الحوسبة السحابية هي تقنية فعالة من حيث التكلفة ومرنة ومريحة في الوصول عن بعد إلى التطبيقات وخدمات التخزين، مما يجعل من السهل توفير خدمات تكنولوجيا المعلومات والأعمال عبر شبكة الإنترنت. ومع ذلك، فإن استخدام الحوسبة السحابية هو مصدر إضافي للمخاطر الأمنية بسبب الاستعانة بمصادر خارجية من طرف ثالث، حيث أن المحافظة على خصوصية البيانات وتوافرها وأمنها أمر صعب للغاية. الحوسبة السحابية لديها العديد من التقنيات الداعمة لها (الافتراضية، ويب 2.0، والهندسة المعمارية الموجهة نحو الخدمات)، التي ترث العديد من القضايا الأمنية ويجعلها عرضة للهجمات. ركزت معظم الأعمال السابقة على تخزين البيانات في السحابة دون أخذ قضايا الأمن والهجمات بعين الاعتبار. في هذه الورقة، ونحن نقدم تحليلا للمسائل الأمنية في سحابة التخزين والحلول الممكنة. وفيما يتعلق بالاعتداءات على البيانات المخزنة في السحب، يتم توفير مقارنة حدودي تشمل جميع التفاصيل والتدابير المضادة. وأخيرا، تقدم هذه الورقة إسهاما كبيرا في بناء بيئة سحابية آمنة لتخزين البيانات وخصوصيتها واستردادها في حالات الكوارث.