All threats in Cloud Security & Cloud Privacy

YOUSRA ABDUL ALSAHIB S.ALDEEN

Lecturer at Baghdad University / College of Education, IbnRushd for Humanities

Abstract

Cloud computing is an expression for distributed computing over a network and also means the ability to run a program on many connected computers at the same time. It offers users the ability to connect to computing resources and access IT managed services. A user believes that a cloud has become wide ground of a new generation of products and services. Cloud computing have given rise to the popularityand success. However, while outsourcing the data and business application to a third party causes the security and privacy issues to become a major concern. Throughout the study at hand, this paper obtains a common goal to provide a comprehensive review of the existing security and privacy issues in cloud environments. It could be identified five most representative security and privacy attributes (i.e., confidentiality, integrity, availability, accountability, and privacy-preservability). From these attributes, it can present the relationships among them, the vulnerabilities that may be exploited by attackers, the threat models, as well as existing defence strategies in a cloud scenario.

Keywords: cloud computing, security, privacy, trust, confidentiality, integrity, accountability, availability

1. Introduction

Cloud computing is a new model and computing pattern that enables on- demand provisioning of computational and storage resources. Due to the fact that cloud computing provides an active way to reduce capital expense and operational expense, cloud computing services the economic too much. From this point, it can be consider the definition of cloud computing as a large-scale distributed computing modelwhich is driven by economies of scale, in which a pool of abstracted, virtualized, dynamically- scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet(Xiao, Xiao, & Member, 2012).

Despite of cloud computing has many benefits improving the IT industry, it has security issues and privacy issues (Dev, Sen, Basak, & Ali, 2012). The security and privacy concerns supported by cloud vendors nowadays are not enough so consequently result in a big obstacle for users to adapt into the Cloud Computing systems(Zhou, Zhang, Xie, Qian, & Zhou, 2010).

There are a few security attributes directly or indirectly affect privacy, including confidentiality, integrity, accountability. Clearly, to preserve private data from being disclosed, confidentiality becomes essential. The attribute which is integrity that ensures the data/computation are not corrupted, which preserves privacy(J. Liu et

al., 2012). As mentioned above, the privacy conflict with security due to the fact that the methods of achieving the two issues usually conflict so that in the future we will design proposalachieving the security and privacy together.

There is a main point that it should separate privacy from security due to that privacy has importance level in cloud environments. There is relationship between Privacy and security, as well as other security attributes that have positive or negative effects on privacy.The figure-1 shows the security and privacy issues in the cloud computing.

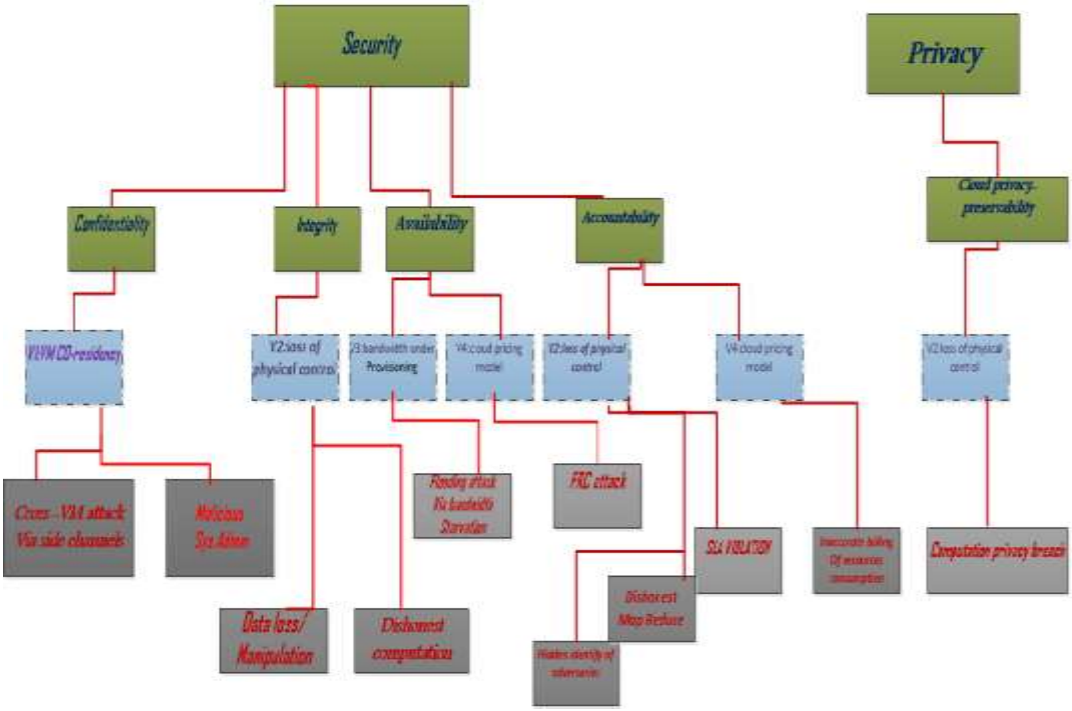
Security
Privacy
Confidentiality
Integrity
Availability
Accountability
Cloud privacy-preservability
V1:VM CO-residency
V2:loss of physical control
V3 bandwidth under Provisioning
V4:cloud pricing model
V2:loss of physical control
V4 cloud pricing model
V2 loss of physical control
Cross-VM attack Via side channels
Malicious Sys Admin
Flooding attack Via bandwidth Starvation
FRC attack
SLA VIOLATION
Inaccurate billing Of resources consumption
Computation privacy breach
Dishonest Map Reduce
Hides identity of adversaries
Data loss/ Manipulation
Dishonest computation

Figure 1 shows all the attacks in security &privacy

The remainder of the paper is organized as follows:Section 2 presents Cloud Vulnerabilities. Next, Section 3 presents the Threats to security and also the protection strategies for every one of them. Finally, section 4 provides some conclusions.

2-Cloud Vulnerabilities

i. **V1: VM co-residence: which means that multiple independent clients share the same physical infrastructure. Basically, virtual machines related to different clients may be put in the same physical machine. VM co-residence has effected on security issues, such as Cross-VM attack and Malicious SysAdmin (Aviram, Hu, & Ford, n.d.).**

ii. V2: Loss of Physical Control: which means that clients could not face certain attacks and accidents so the data or software may be altered, lost, or even deleted. In the same time, it is hard and unpractical to ensure data, computation integrity and confidentiality with traditional methods.

iii. V3 : Bandwidth Under-provisioning: in cloud computing ,there is a new type of DOS attack which takes advantage of the current under-provisioned cloud computing infrastructure(H. Liu, n.d.).

iv. V4: Cloud Pricing Model: requires the cost of services in terms of metrics such as server hours, bandwidth, storage, etc., so all cloud clients are financially responsible for the services they use. From this point the attackers will explore the pricing model. For instant, Economic Denial of Sustainability (EDoS) attack tamper the utility pricing model and causes high costs for cloud customers.

3- Threats to security

This section will talk about the threats for every attributes as follow and also presents the protection strategies for every one of them.

3.1 Threats to Cloud Confidentiality

A- Cross-VM attack via Side Channels: A Cross-VM attack exploits the nature of multitenancy, which could that VMs belonging to different clients may co-reside on the same physical machine. Aviram et al. (Aviram et al., n.d.) considers timing side-channels as an insidious threat to cloud computing security due to the nature of large parallelism and shared infrastructure the timing channels are difficult to control it as well as the another reason the malicious customers are able to steal information from other ones without leaving a trail or raising alarms. There are two main steps to great such an attack which are placement, an adversary wants to place a malicious VM on the physical server where the target client’s VM is located and extraction, after placement, a malicious VM has co-resided with the victim VM.

B- Malicious SysAdmin: Privileged sysadmin of the cloud provider can perform attacks by accessing the memory of a customer’s VMs.

3.2-Protection strategies

A - Placement Prevention: to minimize , cloud providers could obfuscate co-residence by having Dom0 not respond in traceroute, and/or by randomly assigning internal IP addresses to launch VMs. To reduce the success rate of placement, cloud providers might let

the users decide where to put their VMs; however, this method does not prevent a brute-force strategy.

B - Co-residency Detection: The ultimate solutionof cross-VM attack is to remove co-residency. Cloud customers (especially enterprises) may require physical isolation, which can even be written into the Service Level Agreements (SLAs).

C – No Hype: attempts to minimize the degree of shared infrastructure by removing the hypervisor while still retaining the key features of virtualization.

D - Trusted Cloud Computing Platform: Santos et al. (Santos, Gummadi, & Rodrigues, n.d.)propose a trusted cloud-computing platform (TCCP), which supports a closed box execution environment for IaaS services. TCCP ensures confidential execution of guest virtual machines. It also enables customers to identify to the IaaS provider and to determine if the service is secure before their VMs are launched into the cloud. The design goals of TCCP are: 1) to lock the VM execution inside the secure perimeter; 2) that a sys admin with root privileges is unable to access the memory of a VM hosted in a physical node. TCCP leverages existing techniques

3.3-Threats to Cloud Integrity

A-data loss/manipulation: The cloud servers are doubt in terms of both security and reliability (Ateniese, Di Pietro, Mancini, & Tsudik, 2008), that means that data may be lost or modified maliciously or accidentally. Administration errors may cause data loss such as backup and restore data migration. In addition,attackers may begin attacks by taking advantage of data owners' loss of control over their own data.

B-Dishonest computation in remote servers: at theoutsourced computation, it is hard to judge whether the computation is executed with high integrity.

3.4-Protection strategies

1-Provable Data Possession (PDP): is a class of problems that provides efficient and practical approaches in order to determine whether the outsourced data is honestly stored. These methods for data integrity including

1-aPDP:

The success factors of this method are:

- **Supports both encrypted data and plain data.**
- **Efficient: only a small portion of file needs to be accessed to generate proof on the server.**

- 3- Offers public verifiability.

The issues of this method are:

- Only supports integrity checking for static data (i.e., append only).
- 2 - Probabilistic guarantees may result in false positive.

It depends on these theories: Homomorphic hashing: to compose multiple block inputs into a single value to reduce the size of proof.

1-bPOR

The success factors of this method are:

1- Ability to recover file with error-correcting code.

2- Efficient.

The issues of this method are:

1- Static data only.

2 - File needs to be encrypted be

3- Fore uploading to server.

4- Needs additional space to hide sentinels in.

Theories: Error-correcting code: to recover a partially corrupted file.

1-c-scalable PDP

The success factors are:

1- No bulk encryption is required.

2 - Allow outsourcing dynamic data in some degree.

3 - Rely on symmetric-key which is more efficient than public-key encryption.

The issues of this method are:

1- Does not offer public verifiability.

2- All challenges and answers are pre-computed.

3 - Number of updates is limited and fixed as a priori.

Theories: Symmetric-key cryptography, Message Authentication Code (MAC).

1-d-Dynamic PDP

The success factors are:

1-Support fully dynamic data operation (i.e., insert, modification, delete, and append).

2- All challenges and answers are dynamically generated.

The issues of this method areFully dynamic support causes relatively higher computational, communication, and storage overhead.

Theories:

1-Rank-based authenticated directory.

2- RSA-tree. 3- Authenticated skip list.

1-e-HAIL

The success factor of this method is Ability to check integrity in distributed storage via data redundancy.

The issue of this method is Static data only.

Theories:

1- Pseudorandom functions.
2- Message authentication codes (MACs).
3- Universal hash functions.

2-Third Party Auditor

Instead of letting customers verify data integrity, it is also possible to offload task of integrity checking to a third party which can be trusted by both cloud provider and customers.

3.5-Methods for computing integrity

1-Re-computation requires the local machine to re do the computation, and then compare the results. Re-computation guarantees 100% accuracy of mistake detection, and does not require trusting the cloud vendor.

2-Replication assigns one computation task to multiple machines, and then compares the results. The drawback that Intelligent adversaries that control certain amounts of machines may bypass replication checking by returning the same incorrect results.

3-Auditing usually works together with logging. One drawback of auditing is that if the attacker understands the computation better than the auditor, it is possible for the attacker to manipulate data bits without being detected.

4-Trusted Computing : enforces the computer to behave consistently in expected ways with hardware and software support.

3.6-Threats to Cloud Availability

A - Flooding Attack via Bandwidth Starvation: In a flooding attack, which can cause Deny of Service (DoS), a large amount of nonsensical requests are sent to a particular service to prevent it from working properly. In cloud computing, there are two kinds of flooding attacks:

- Direct DOS -the attacking target is specialized, and the availability of the targeting cloud service will be fully lost.
- Indirect DOS –which meaning is all services hosted in the same physical machine with the targetvictim will be affected and the attack is begun without a specific target

B -Fraudulent Resource Consumption (FRC) attack: In cloud computing, the aim of a FRC attack is to stop the victim of their long-term economic availability of hosting web contents that are publicly accessible. In other words, attackers, who act as legal cloud service

clients, continuously send requests to website hosting in cloud servers to consume bandwidth, which bills to the cloud customer owning the website; seems to the web server, those traffic does not reach the level of service denial, and it is difficult to identify FRC traffic from other legitimate traffic. A FRC attack succeeds when it causes financial burden on the victim.

3.7-Protection strategies

1-defending the new DOS attack: A DOS avoidance strategy called service migration has been developed to deal with the new flooding attack.

2- FRC attack detection: The key of FRC detection is to distinguish FRC traffic from normal activity traffic.

3.8-Threats to Cloud Accountability

A - SLA violation: when something goes wrong such as the machines in the cloud could not control or defective, may be due that to corrupt the customer's data or cause his computation to return incorrect results. Another point,the cloud provider can accidentally assign insufficient resources for the client, a role which can degrade the performance of the client's services and then violate the SLA .When something goes wrong such as data leaks to a competitor, or the computation returns incorrect results, it can be difficult for a customer and provider to assign which of them has caused the problem. As a result, when there is a difficult to find the robust evidence, it is nearly impossible for them to hold each other responsible for the problem when a dispute arises.

B -Dishonest MapReduce: is aparallel computing paradigmthat is widely used by major cloud providers (Google, Yahoo!, Facebook, etc.). The processing results returned by the cloud may be inaccurate due to the working machines may not be control or malicious. Moreover, it is difficult for customers to ensure the correctness of results other than by running the same task again locally.

C - Hidden Identity of Adversaries: Due to privacy concerns, cloud providers should not detect cloud customers' identity information. As a result, malicious users can harm the data integrity without being revealed.

D - Inaccurate Billing of Resource Consumption:The payasyou use model enables customers to decide how to outsource their business based on their needs as well as the financial situations. It is difficult for clients to verify the expenses of the resource consumption due to the black box and dynamic nature of cloud computing. From the

cloud vendor's view, to achieve maximum profitability, the cloud providers choose to multiplex applications belonging to different customers to keep high utilization. The multiplexing may cause providers to incorrectly attribute resource consumption to customers or implicitly bear additional costs, therefore reducing their cost effectiveness.

3.9-Protection strategies

1-Accountability on Service Level Agreement (SLA)
2-Accountable Virtual Machine
3-Collaborative Monitoring
4-Accountable Map Reduce
5-Secure Provenance
6-Verifiable Resource Accounting
7-Cloud Accountability Life Cycle (CALC)

3.10-Threats to cloud privacy

There is a strong relationship between Privacy and confidentiality due to the fact that they both prevent information leakage. For this reason, if cloud confidentiality is violated, privacy will also be violated. The meaning of cloud privacy includes data privacy and computation privacy. As mentioned above data mining based attacks consider a big dangerous for cloud computing(Xiao et al., 2012).

3.11-Protection Strategies

There are many researchers proposed strategies to protect the privacy, Chow et al. have categorized the privacy-preserving approaches into three groups(Chow et al., 2009). Gentry proposed Fully Homomorphic Encryption (FHE) to protect privacy in cloud computing(Gentry, 2009). FHE could be computation on encrypted data that are stored in the distrusted servers of the cloud provider. It can be processed the data without decryption. The cloud servers should not know about the input data, the processing function, the result, and any middle result values. For this reason, the outsourced computation happens in a fully privacy-preserving way. FHE has become a robust tool to perform privacy preserving in cloud computing but in other side, FHE schemes are too inactive for use in practice. However, researchers tried to reduce the complexity of FHE, it could be considered mitigate the power of FHE to recover efficiency.

Naehrig et al. has proposed comparatively homomorphic encryption that may only help a number of homomorphic operations, which may be much rapid and more compact than FHE. Pearson et al. propose privacy manager that depends on obfuscation techniques(Pearson, Shen, & Mowbray, n.d.),("IEEE Xplore Download," n.d.). The privacy

manager can offer obfuscation and de obfuscation service to reduce the amount of sensitive information stored in the cloud, to store the encrypted form of clients' private data in the cloud end. Instantly, processing data is performed on the encrypted data. One drawback that cloud vendors may not be ready to perform additional services for privacy protection so without provider's collaboration, this scheme will not work.

A novel privacy issue is explored by Squicciarini("IEEE Xplore Download2," n.d.). For indexing data and preventing information leakage, the researchers introduce three-tier data protection architecture providing different levels of privacy to cloud customers. A Privacy-as-a-Service is presented by Itani et al.(Itani, Kayssi, & Chehab, 2009), so it can be secure storage and computation of private data by lever aging the tamper proof capabilities of cryptographic coprocessors. It leads to protect customer data from unauthorized access. According to Sadeghi et al. (Sadeghi, Schneider, Winandy, & Horst, 2010),that debate homomorphic based pure cryptographic solutions due to fact that fully suffer high latency for providing practical secure outsourcing of computation to a distrusted cloud service provider. They propose merging a trusted hardware token with Secure Function Evaluation (SFE) to compute arbitrary functions on data when it is still in encrypted form. The objective of this work is to reduce the computation latency to be efficient, secure outsourcing in cloud computing. A hardware token is tamper-proof versus physical attacks. The data computation is confidential as well as being verifiable due to guarantee the possession of a token. The solution presented in only needs to deploy a tamper- proof token in the setup pre-processing phase. Below the figure.1 that summarize all the attacks in cloud security & privacy.

4. Conclusion

Cloud Computing is one of the most technology in recent years. It has a good number of benefits for its users; however, it also raises some security and privacy problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing influences many technologies, it also inherits their security issues. It should be studied the security and privacy issues in cloud computing based on an attribute-driven methodology, shown in Fig. 1. This paper have identified the most representative security/privacy attributes (e.g., confidentiality, integrity, availability, account- ability, and privacy-preservability), as well as discussing the vulnerabilities,

which may be exploited by adversaries in order to perform various attacks. It disseised Defence strategies and suggestions were discussed as well.

References

Ateniese, G., Di Pietro, R., Mancini, L. V., & Tsudik, G. (2008). Scalable and efficient provable data possession. Proceedings of the 4th international conference on Security and privacy in communication netowrks - SecureComm '08, 1. doi:10.1145/1460877.1460889

Aviram, A., Hu, S., & Ford, B. (n.d.). Determinating Timing Channels in Compute Clouds.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling Data in the Cloud : Outsourcing Computation without Outsourcing Control, 85–90.

Dev, H., Sen, T., Basak, M., & Ali, M. E. (2012). An Approach to Protect the Privacy of Cloud Data from Data Mining Based Attacks. 2012 SC Companion: High Performance Computing, Networking Storage and Analysis, 1106–1115. doi:10.1109/SC.Companion.2012.133

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. Proceedings of the 41st annual ACM symposium on Symposium on theory of computing - STOC '09, 169. doi:10.1145/1536414.1536440

IEEE Xplore Download. (n.d.).

IEEE Xplore Download2. (n.d.).

Itani, W., Kayssi, A., & Chehab, A. (2009). Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 711–716. doi:10.1109/DASC.2009.139

Liu, H. (n.d.). A New Form of DOS Attack in a Cloud, 65–75.

Liu, J., Xiao, Y., Member, S., Li, S., Liang, W., & Chen, C. L. P. (2012). Cyber Security and Privacy Issues in Smart Grids, 14(4), 981–997.

Pearson, S., Shen, Y., & Mowbray, M. (n.d.). A Privacy Manager for Cloud Computing.

Sadeghi, A., Schneider, T., Winandy, M., & Horst, G. (2010). Token-Based Cloud Computing, 2, 417–429.

Santos, N., Gummadi, K. P., & Rodrigues, R. (n.d.). Towards Trusted Cloud Computing.

Xiao, Z., Xiao, Y., & Member, S. (2012). Security and Privacy in Cloud Computing, 1–17.

Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey. 2010 Sixth International Conference on Semantics, Knowledge and Grids, 105–112. doi:10.1109/SKG.2010.19

J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," IEEE Commun. Surveys Tuts., DOI: 10.1109/SURV.2011.122111.00145, in press.

كل التهديدات الامنية والخصوصية التي تواجه الحوسبة السحابية

م.م. يسرى عبد الصاحب سيف الدين

الخلاصة باللغة العربية:

الحوسبة السحابية هي تعبير عن الحوسبة الموزعة عبر شبكة الانترنيت ويمكن تعريفه أيضا بانه القدرة على تشغيل البرنامج على العديد من أجهزة الكمبيوتر المتصلة في نفس الوقت . فإنه يوفر للمستخدمين القدرة على الاتصال و الوصول إلى الموارد الحاسوبية والخدمات المدارة لتكنولوجيا المعلومات. لذا يؤمن مستخدمي الحوسبة السحابية انها أصبحت تمثل ارضا واسعة من جيل جديد من المنتجات والخدمات. لقد أعطت الحوسبة السحابية ارتفاعاشعبيا و نجاح . ومع ذلك ، في حين أن الاستعانة بمصادر خارجية البيانات و تطبيقات الأعمال لطرف ثالث يتسبب في قضايا الأمن والخصوصية لتصبح مصدر قلق كبير. وهذا ما بينته الدراسات والبحوث التي تناولت خطر الذي يواجه امنية وخصوصية مستخدمي الحوسبة الضبابية. ان الهدف من هذا البحث هو تقديم استعراض شامل لقضايا الأمن والخصوصية الموجودة في البيئات السحابية وهذا يمكن التعرف عليه من خلال خمس سمات الأمان والخصوصية الأكثر تمثيلا (السرية والنزاهة و توافر ، والمساءلة، والخصوصية) . انه ايضا يعرض العلاقات فيما بينها ، و نقاط الضعف التي يمكن استغلالها من قبل المهاجمين ، ونماذج التهديد ، فضلا عن استراتيجيات الدفاع الموجودة في سيناريو السحابية.