УДК 004.9

Риски безопасности данных в облачных вычислениях

Арифа Ашрафи
Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых
магистрант

Градусов Денис Александрович
Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых
к.э.н., доцент кафедры «Вычислительная техника и системы управления»

Аннотация
В данной статье рассмотрены вопросы, связанные с оценкой безопасности данных при использовании облачных вычислений. Рассмотрены возможные риски и методик снижения рисков, а также механизмы шифрования позволяющие обеспечить сохранность данных в облачных сервисах.
Ключевые слова: облачные вычисления, безопасность данных, риски и угрозы облачной безопасности, кибербезопасность, информационная безопасность

Data Security Risks in Cloud Computing

Arifa Ashrafi
Vladimir State University named after Alexander and Nikolay Stoletovs
Post Graduate Student

Gradusov Denis Aleksandrovich
Vladimir State University named after Alexander and Nikolay Stoletovs
Ph. D., associate Professor of the Department «Computer engineering and control systems»

Abstract
This article discusses about issues related to the assessment of data security risks in cloud computing. Possible risks, risk mitigation techniques, as well as encryption mechanisms for data integrity in cloud services, are analyzed here.
Keywords: cloud computing, data security, cloud security risks and threats, cyber security

Introduction

Cloud computing is considered as a bridge of unlimited connectivity. Almost everything in internet is connected to the cloud in some way or another. In 10-15 years most of the works in digital world will be available via cloud, shows

some surveys. Cost effectiveness, efficiency, scalability makes it possible for cloud computing to gain that unbelievable success. But still cloud computing is not free of risks and threats. It can leave your personal data or business in a vulnerable condition by any kind of data security failure.

Goal

Cloud computing provides a simple way to access servers, storage, databases and a board set of application services over the internet. It is predicted that in a few years we will see that the clouds will bring much more benefits to the world than one can imagine now. Not only big companies but also more and more middle and small business are moving to cloud computing services. This trend is confirmed by reliable survey. Advantages like lower cost, faster time to market, scalability, availability of cloud computing driving business owner to use different cloud services. However data security risks and threats considered as major disadvantages of cloud computing. Data loss, compliance violation, increase APIs, weak authentication, shared vulnerabilities etc. are some of the security risks facing every company.

Data Security Issues

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 [1]. The major issues in the cloud computing include data loss, account hacking, insecure infrastructure, malicious insider etc. Data security issues in cloud computing can be described in two ways: 1) Virtual Security Issues and, 2) Physical Security Issues.

One of the main virtual security issues in the cloud are attacks on the network between VM's, and the trust between different VM's [2].

Virtual Security Issues	Distributed Denial of Service(DDoS)
	DNS Attacks
	Network Attacks in Virtual Cloud

Fig.1. Virtual Security Issues in cloud computing

Physical security in the cloud represents the physical machines and storage in the datacenter. Physical security issues shows as a loss of physical control, human attacks, power failure, access control, and third party trust [3].

Fig.2. Physical Security Issues in cloud computing

Primary Security Issues in Cloud Computing

Since data in the public cloud is being stored by a third party and accessed over the internet, several issues arise in the ability to maintain a secure cloud. These are:

Visibility into cloud data — in many cases, cloud services are accessed outside of the corporate network and from devices not managed by IT. This means that the IT team needs the ability to see into the cloud service itself to have full visibility over data, as opposed to traditional means of monitoring network traffic [9].

Control over cloud data — in a third-party cloud service provider's environment, IT teams have less access to data than when they controlled servers and applications on their own premises. They also have little to no oversight of bring-your-own-device (BYOD) technology that can access the cloud, as compared to managed devices such as laptops and smartphones they issued themselves. Cloud customers are given limited control by default, and access to underlying physical infrastructure is unavailable [9].

Cloud computing and storage provides users with capabilities to store and process their data in third-party data centers.[4] Organizations use the cloud in a variety of different service models (with acronyms such as SaaS, PaaS, and IaaS) and deployment models (private, public, hybrid, and community).[5] Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud) [6].

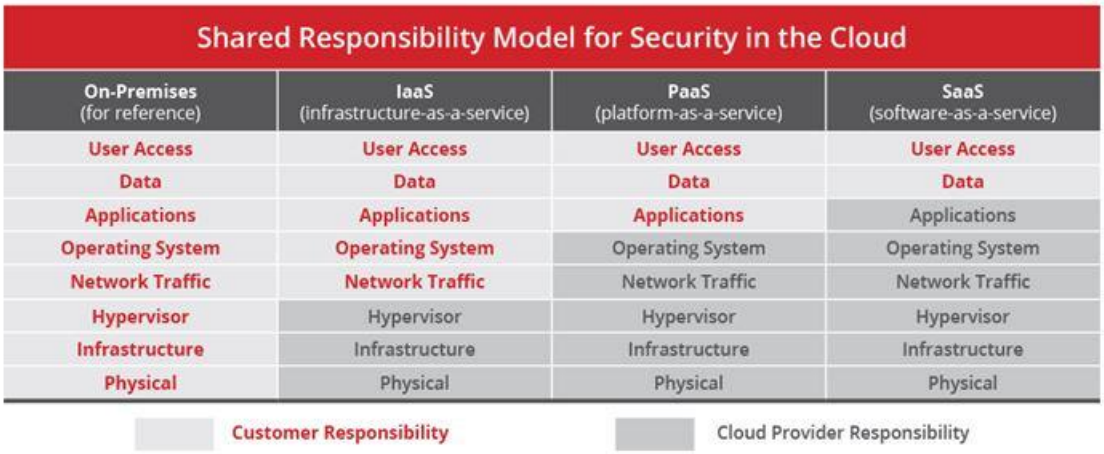

Fig.3. Shared responsibility for data security [9]

Top data security risks of cloud computing are given below:

- Data Loss,
- Inadequate due Diligence,
- Denial of service,
- Security threats due to Shared Vulnerabilities,
- Data Breaches,
- Insider Threats,
- Insecure Applications,
- Account Hacking,
- Malware injection.

Recommended practices

To mitigate cloud computing security risks, there are three best practices recommended by *mcafee* team which are given below -

- DevSecOps processes: DevSecOps integrates an organization's security team into the traditional DevOps organization. While DevOps integrates software development and production teams to produce bug-free applications, DevSecOps takes the added step of ensuring those applications are secure. The goal of DevSecOps is to embed security checks into every aspect of software development and production, adding another layer of prevention against data breaches and cyberattacks [9].
- Automated application deployment and management tools: The shortage of security skills, combined with the increasing volume and pace of security threats, means that even the most experienced security professional cannot keep up. Automation that removes mundane tasks and augments human advantages with machine advantages is a fundamental component of modern IT operations [9].
- Unified security with centralized management across all services and providers: No one product or vendor can deliver everything, but multiple management tools make it too easy for something to slip through. A unified management system with an open integration fabric reduces complexity by bringing the parts together and streamlining workflows [9].

Various Encryption techniques for usage

Use of these Encryption techniques can be differing from one scenario to another. Some encryption techniques are discussed below-

Block Ciphers

A block cipher is an algorithm for encrypting data (to produce cipher text) in which a cryptographic key and algorithm are applied to a block of data instead of per bit at a time [7].

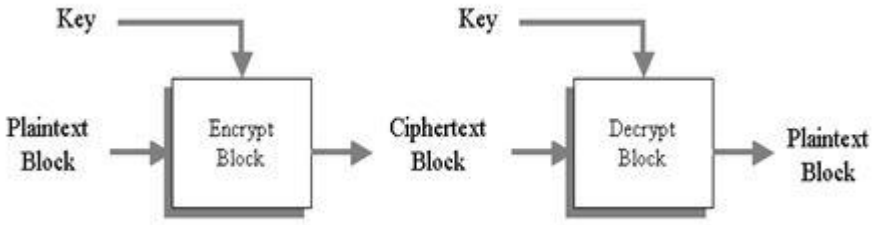

Fig.4. Block Cipher Encryption

Stream Ciphers

This technique of encrypting data is also called state cipher since it depends on the current state of cipher. In this technique, each bit is encrypted instead of blocks of data. An encryption key and an algorithm are applied to each and every bit, one at a time [8].

Hash Functions

In this technique, a mathematical function called a hash function is used to convert an input text in to an alphanumeric string.

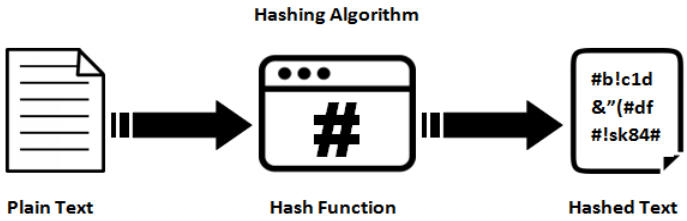

Fig.5. Hash Function Techniques

Proposed objectives and approaches for data security risks in cloud computing

Either it is personal or about business, any kind of data is one of the most valuable assets, yet often one of the most vulnerable. This is why IT professionals and cloud service providers try to do their best to provide top-notch data security. But still data security risks and treatments are one of the biggest challenge for cloud computing. Lack of physical control, on defined entrance and egress points, being a whole host of cloud data security issues are some serious discussable matters. Still need more research for fulfilling these following objectives:

- Show clients and providers existing cloud security challenges,
- Assessment of technical failure which can lead to cyber security risks and threats,
- Study new data security risks, threats and challenges for experimenting new opportunities,
- Grow awareness for both cloud providers and customers.

Research Approach in this field may include:

- Review and analysis of all existing cyber security risks and threats
- Study data security architecture and frame work for cloud computing

- Identification of data security policy rules
- Proposal of a methodology for assessing data security risks in cloud computing
- Evaluate proposal by case study
- Management presentation with specific recommendation for action.

Conclusion

According to Cloud Security Alliance (CSA), over 70 percent of the world's businesses now operate – at least in part – on the cloud. With benefits like lower fixed costs, higher flexibility, automatic software updates, increased collaboration, and the freedom to work from anywhere, 70 percent isn't a big surprise. Still, the cloud has its share of security issues. This is why we are very much interested in cloud computing security risks and threats. Hopefully our Successful research and studies can draw an outline to protect user's valuable data and also increase awareness into both cloud providers and customers.

References

1. Avizienis A., Laprie J.-C., Randell B., Landwehr C. Basic concepts and taxonomy of dependable and secure computing // IEEE Transactions on Dependable and Secure Computing. 2004. V. 1. No. 1. P. 11 - 33.
2. Vic J.R. Winkler Securing the Cloud: Cloud Computer Security Techniques and Tactics. Massachusetts: Syngress, 2011. 314 p.
3. Dana Al Tehmazi Inter-Cloud Trust Model Security: Issues and Challenges // researchgate. 2013. P. 7.
4. Haghighat M., Zonouz S., Abdel-Mottaleb M. CloudID: Trustworthy cloud-based and cross-enterprise biometric identification //Expert Systems with Applications. 2015. V. 42. No. 21. P. 7905-7916.
5. Srinivasan M. K., Sarukesi K., Rodrigues P., Sai Manoj M., Revathy P. State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment. NY.: Proceedings of the International Conference on Advances in Computing, Communications and Informatics, 2012 . P. 470-476.
6. Suresh K.S., Prof K.V. Prasad Security Issues and Security Algorithms in Cloud Computing // International Journal of Advanced Research in Computer Science and Software Engineering. 2012. P. 110-114.
7. He J., Qian H., Zhou Y., Li Z. Cryptanalysis and Improvement of a Block Cipher Based on Multiple Chaotic Systems // Mathematical Problems in Engineering. 2010. P. 14.
8. Gope P., Hwang T. Untraceable Sensor Movement in Distributed IoT Infrastructure // IEEE Sensors Journal. 2015. V. 15. No. 9. P. 5340 - 5348.
9. Cloud Computing Security Issues and Solutions // McAfee URL: https://www.mcafee.com/enterprise/en-sg/security-awareness/cloud/security-issues-in-cloud-computing.html