ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW ON SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING

Gulshan Kumar*, Dr.Vijay Laxmi
[*] UCCA Guru Kashi University Talwandi Sabo,India

DOI: 10.5281/zenodo.546305

ABSTRACT

Cloud computing is an upcoming paradigm that offers tremendous advantages in economical aspects, such as reduced time to market, flexible computing capabilities, and limitless computing power. To use the full potential of cloud computing, data is transferred, processed and stored by external cloud providers. However, data owners are very skeptical to place their data outside their own control sphere. Cloud computing is a new development of grid, parallel, and distributed computing with visualization techniques. It is changing the IT industry in a prominent way. Cloud computing has grown due to its advantages like storage capacity, resources pooling and multi-tenancy. On the other hand, the cloud is an open environment and since all the services are offered over the Internet, there is a great deal of uncertainty about security and privacy at various levels. Proposed work aims to address security and privacy issues threatening the cloud computing adoption by end users. Cloud providers are mindful of cloud security and privacy issues and are working hardly to address them. Few of these threats have been addressed, but many more threats still unsolved. Proposed work focused on cloud computing security and privacy threats, challenges, and issues. Furthermore, some of the countermeasures to these threats will be discussed and synthesized. Finally, possible solutions for each type of threats will be introduced before we end with conclusions and future work.

KEYWORDS: Cloud Computing; Security; Privacy in Cloud computing; Confidentiality in Cloud Computing environment.

INTRODUCTION

While the storage of corporate data on remote servers is not a new development, current expansion of cloud computing justifies a more careful look at its actual consequences involving privacy and confidentiality issues. We introduce in this paper a secure privacy preserving cloud database storage architecture.

As the Internet grew more popular, many new technologies such as a cloud computing appeared and caught the attention of many industries. Cloud computing (CC) became popular because of its unique features like dynamic massive scalability, elasticity, measured service and self-provisioning of resources, convenient and on demand network access, and a shared pool of resources.

This means that the cloud is an open and shared environment, which makes the privacy and security of users' data a complex issue. CC exhibits a lot of security threats like sensitive data loss, cloning and data leakage. The cloud providers are mindful of the cloud security and privacy issues and are working on addressing them. Only few of those threats have been addressed, but many more threats still unsolved. Security is one of the most significant challenges that face the cloud, and privacy makes the cloud more complex to maintain [1]. When we think about the benefits of cloud computing which revolves around sharing resources, information and applications by computer devices connected to the cloud. CC aims to produce a super computer from many normal computers; having more powerful computation capabilities with lowest cost creates a strong cloud [2]. This paper will focus on the major security and privacy issues in cloud computing. Furthermore, it shows the corresponding countermeasures of these issues. The rest of the paper will be organized as the following: The next section summarizes work related to security threats and their solution, followed by privacy concerns and their solutions. Finally, conclusions and future work will be depicted at the end.

LITERATURE SURVEY

R.Rogini[1], In the field of computing, cloud computing visualize consistent growth and evolving spontaneously . Still the threats and security problems deal with it. The main focus of this paper is surveying on various privacy preserving concept in cloud computing. This paper is go to handle and examine different steps such as cryptographic step processing, segregation or fragmentation of data, deals with writing access rights and policies. These sort of approaches would preserves the end user data privacy and during public auditing of cloud data privacy preserving is achieved. The inspected approaches are demonstrated and distinguished with one another by stating their merits and demerits. Finally, the concentrated issues to be drawn out in future and centralized results are produced. Earlier outsourcing of encrypted sensitive data, Data access notification to the data owner, providing complete permission of control to user over his/her data. All this function has a capacity to nullify the issues in privacy. In the process of enhancing the privacy preserving approaches in cloud this would serve as a note.

K. Ullah[2], Cloud computing is emerging as a powerful architecture to perform large-scale and complex computing. It extends the information technology (IT) capability by providing on-demand access to computer resources for dedicated use. The information security and privacy are the major concerns over the cloud from user perspective. This paper surveys and evaluates the architecture, data security and privacy issues in cloud computing like data confidentiality, integrity, authentication, trust, service level agreements and regulatory issues. The objective of this paper is to review comprehensively the current challenges of data security and privacy being faced by cloud computing and critically analyze these issues.

Rabi Prasad Padhy[3], Cloud computing is an architecture for providing computing service via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider like Google, Amazon, Salesforce.som and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper outlines what cloud computing is, the various cloud models and the main security risks and issues that are currently present within the cloud computing industry. This research paper also analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.

S. Kumar[4], Cloud computing is the development of parallel computing, distributed computing, grid computing and virtualization technologies which define the shape of a new era. Cloud computing is an emerging model of business computing. In this paper, authors explore the concept of cloud architecture and compares cloud computing with grid computing. We also address the characteristics and applications of several popular cloud computing platforms. In this paper, we aim to pinpoint the challenges and issues of cloud computing. We identified several challenges from the cloud computing adoption perspective and we also highlighted the cloud interoperability issue that deserves substantial further research and development. However, security and privacy issues present a strong barrier for users to adapt into cloud computing systems. In this paper, we investigate several cloud computing system providers about their concerns on security and privacy issues.

CLOUD DEPLOYMENT MODELS

Private Clouds

Also known as internal clouds, private clouds are designed for exclusive use (storage, computing...) by a single organization on a private network. A private cloud offers the highest degree of control over performance, reliability and security. However, they are purchased and completely managed by the organization, so private clouds don't benefit from lower costs due to shared environments unlike other models and requires internal IT expertise or delegate the management to third parties.

Public Clouds

Public clouds provide on-demand services to the general public over a common infrastructure hosted, operated and managed by a third-party vendor. Security management and day-to-day operations are relegated to the vendor. Public clouds offer several key benefits to customers, including no initial capital investment on infrastructure, lower costs and shifting of risks to providers' infrastructure.

However, customers have a low degree of control in these kind of control compared with private clouds, which raises a huge amounts of security and privacy concerns that are the basis of this document, as public clouds are the main traditional way of deploying Cloud Computing architectures.

Hybrid Clouds

A hybrid cloud is a combination of public and private cloud models that tries to address the limitations of each approach. In a hybrid cloud, part of the service infrastructure runs in private clouds (e.g. core applications, sensitive data) while the remaining part runs in public clouds (e.g. non-core applications). Hybrid clouds provide more control and security over data compared to public clouds while still facilitating on-demand service and elasticity. However, the design of hybrid clouds require to carefully determine what should be split into public and private cloud components.

CLOUD COMPUTING SERVICE MODELS

Software-as-a-Service

Software-as-a-Service (SaaS) is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

Platform-as-a-Service

Platform-as-a-Service (PaaS) is a model of software deployment whereby the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any needed program and database development tools. The development environment is typically special purpose, determined by the cloud provider and tailored to the design and architecture of its platform. The cloud subscriber has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud subscriber.

Infrastructure-as-a-Service

Infrastructure-as-a-Service (IaaS) is a model of software deployment whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface. The cloud subscriber generally has broad freedom to choose the operating system and development environment to be hosted. Security provisions beyond the basic infrastructure are carried out mainly by the cloud subscriber.

SECURITY PRACTICES IN CLOUD COMPUTING ENVIRONMENT

Protection Against Internal and External Threats

Security monitoring services help to improve the effectiveness of the security infrastructure of a customer by actively analyzing logs and alerts from infrastructure devices around the clock and in real time. Monitoring teams correlate information from various security devices to provide security analysts with the data they require to eliminate false positives and respond to true threats against the enterprise. Usually the skills required to maintain the level of service of an organization is very high. The information security team can assess system performance on a periodically recurring basis and provide recommendations for improvements as needed.

Early Detection

An early detection service detects and reports new security vulnerabilities shortly after they appear. Generally, the threats are correlated with third party sources, and an alert or report is issued to customers. Security vulnerability reports, aside from containing a detailed description of the vulnerability and the platforms affected, also include information on the impact the exploitation of this vulnerability would have on the systems or applications previously selected by the company receiving the report. Most often, the report also indicates specific actions to be taken to minimize the effect of the vulnerability, if that is known.

Platform, Control, and Services Monitoring

Platform, control, and services monitoring is often implemented as a dashboard interface and makes it possible to know the operational status of the platform being monitored at any time. It is accessible from a web interface, making remote access possible. Each operational element that is monitored usually provides an operational status indicator, always taking into account the critical impact of each element. This service aids in determining which elements may be operating at or near capacity or beyond the limits of established parameters. By detecting and identifying such problems, preventive measures can be taken to prevent loss of service.

Intelligent Log Centralization and Analysis

Intelligent log centralization and analysis is a monitoring solution based mainly on the correlation and matching of log entries. Such analysis helps to establish a baseline of operational performance and provides an index of security threat. Alarms can be raised in the event an incident moves the established baseline parameters beyond a stipulated threshold. These types of sophisticated tools are used by a team of security experts who are responsible for incident response once such a threshold has been crossed and the threat has generated an alarm or warning picked up by security analysts monitoring the systems.

Vulnerabilities Detection and Management

Vulnerabilities detection and management enables automated verification and management of the security level of information systems. The service periodically performs a series of automated tests for the purpose of identifying system weaknesses that may be exposed over the Internet, including the possibility of unauthorized access to administrative services, the existence of services that have not been updated, the detection of vulnerabilities such as phishing, etc. The service performs periodic follow-up of tasks performed by security professionals managing information systems security and provides reports that can be used to implement a plan for continuous improvement of the system’s security level.

Continuous System Patching/Upgrade and Fortification

Security posture is enhanced with continuous system patching and upgrading of systems and application software. New patches, updates, and service packs for the equipment’s operating system are necessary to maintain adequate security levels and support new versions of installed products. Keeping abreast of all the changes to all the software and hardware requires a committed effort to stay informed and to communicate gaps in security that can appear in installed systems and applications.

Intervention, Forensics, and Help Desk Services

Quick intervention when a threat is detected is crucial to mitigating the effects of a threat. This requires security engineers with ample knowledge in the various technologies and with the ability to support applications as well as infrastructures on a 24/7 basis. MaaS platforms routinely provide this service to their customers. When a detected threat is analyzed, it often requires forensic analysis to determine what it is, how much effort it will take to fix the problem, and what effects are likely to be seen. When problems are encountered, the first thing customers tend to do is pick up the phone. Help desk services provide assistance on questions or issues about the operation of running systems. This service includes assistance in writing failure reports, managing operating problems, etc.

PRIVACY IN CLOUD COMPUTING ENVIRONMENT

Privacy protection in cloud computing environment is less of a technical issue and more of a policy and legal issue. Policies are required to be framed to conform to the legal framework protecting the privacy of individual and organizations. Policies have to empower people to control the collection, use, and distribution of their personal information. A very good framework on privacy protection is given by the Safe Harbor privacy principles developed by the U.S. Department of Commerce and the European Commission. It is based on 7 principles. These principles must provide:

Notice - Individuals must be informed that their data is being collected and about how it will be used.
Choice - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
Onward Transfer - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
Security - Reasonable efforts must be made to prevent loss of collected information.
Data Integrity - Data must be relevant and reliable for the purpose it was collected for.
Access - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
Enforcement - There must be effective means of enforcing these rules.

CONCLUSION

Data security and privacy is one of the biggest challenges in Cloud Computing. Cloud data must be protected not only against external attackers, but also corrupt insiders. The usage of cloud computing as a computing environment for information systems and data can place data outside the data owner's control. The amount of protection needed to secure data is directly proportional to the value of the data. When the value of data increases, the number and extensiveness of needed security controls also increase. It could be a problem if these security controls are not supported by the cloud provider. The uncertainty of how security can be guaranteed in external computing environments raises several security questions concerning the availability, integrity, and confidentiality of data in these cloud computing environments. In this paper we have discussed various cloud security and privacy issues and various solutions to solve these issues.

REFERENCES

[1] R.Rogini, N.Arun Balaji,"An Inspection On Privacy Preserving Methods In Cloud Computing",International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 5, May 2014 ,1392
[2] K. Ullah and M. N. A. Khan,"Security and Privacy Issues in Cloud Computing Environment: A Survey Paper", International Journal of Grid and Distributed Computing Vol.7, No.2 (2014), pp.89-98
[3] Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy, " Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011
[4] Santosh Kumar and R. H. Goudar, "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey", International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012
[5] Ulrich Greveler, Benjamin Justus, Dennis Loehr,"A Privacy Preserving System for Cloud Computing"
[6] Hasan Omar Al-Sakran,"ACCESSING SECURED DATA IN CLOUD COMPUTING ENVIRONMENT",International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.1, January 2015
[7] T. Jothi Neela and N. Saravanan,"Privacy Preserving Approaches in Cloud: a Survey", Indian Journal of Science and Technology
[8] R. Sumithra & Sujni Paul,"A SURVEY PAPER ON CLOUD COMPUTING SECURITY AND OUTSOURCING DATA MINING IN CLOUD PLATFORM",International Journal of Knowledge Management & e-Learning Volume 3 • Number 1 • January-June 2011 • pp. 43-48
[9] Yousef K. Sinjilawi, Mohammad Q. AL-Nabhan and Emad A. Abu-Shanab," Addressing Security and Privacy Issues in Cloud Computing", JOURNAL OF EMERGING TECHNOLOGIES IN WEB INTELLIGENCE, VOL. 6, NO. 2, MAY 2014
[10] Thota Reshma Kishore, D.Akhila Devi, S.Prathyusha, D.Bhagyasri, Bhuma Naresh,"Client and Data Confidentiality in Cloud Computing Using Fragmentation Method", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013
[11] Siani Pearson and Azzedine Benameur,"Privacy, Security and Trust Issues Arising from Cloud Computing",2nd IEEE International Conference on Cloud Computing Technology and Science
[12] Steven Y. Koy, Kyungho Jeony, Ramses Morales,"The HybrEx Model for Confidentiality and Privacy in Cloud Computing",2011
[13] Abhishek Goel, Shikha Goel,"Security Issues in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM),Volume 1, Issue 4, December 2012 G. Eason, B. Noble, and I.N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955. (references)