INTERNATIONAL JOURNAL OF RESEARCH – GRANTHAALAYAH
A knowledge Repository

RACSIT - 17

A REVIEW ON CLOUD COMPUTING SECURITY ISSUES AND CHALLENGES

Madhumala R B [1], Dr. Harshavardhan Tiwari [2]
[1] Assistant Professor, Department of CSE, SET- Jain University, India
[2] Assistant Professor, Department of ISE, Jyothy Institute of Technology, India

DOI: https://doi.org/10.29121/granthaalayah.v5.i4RACSIT.2017.3357

Abstract

The new developments in the field of information technology offered the people enjoyment, comforts and convenience. Cloud computing is one of the latest developments in the IT industry also known as on-demand computing. It provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. It is the application provided in the form of service over the internet and system hardware in the data centers that gives these services. This technology has the capacity to admittance a common collection of resources on request. It is proving extremely striking to cash-strapped IT departments that are wanted to deliver better services under pressure. When this cloud is made available for the general customer on pay per use basis, then it is called public cloud. When customer develops their own applications and run their own internal infrastructure then is called private cloud. Integration and consolidation of public and private cloud is called hybrid cloud.

Keywords: Cloud Computing; Security Issues.

Cite This Article: Madhumala R B, and Dr. Harshavardhan Tiwari. (2017). "A REVIEW ON CLOUD COMPUTING SECURITY ISSUES AND CHALLENGES." *International Journal of Research - Granthaalayah*, 5(4) RACSIT, 76-80.

1. Introduction

Data is stored on peer nodes (called *vaults*) and accessed via a distributed hash table. MaidSafe splits the data into self-contained chunks and encrypts it at the source, removing the trust requirement. Data integrity can be validated against the hash without knowing the contents. MaidSafe can replicate data on multiple nodes, significantly enhancing robustness. Encryption is independent of the user's credentials, so identical files of different users map to identical secure data chunks. Between 75 and 90 percent of data on corporate networks is duplicated, so even with replication, Maid Safe reduces storage requirements. Because it's a P2P system, each user provides a vault, and operation is checked by neighbors using the chunk hash values.

When a user retrieves data, the neighbor of the requesting node stores a cached copy. In addition to offering improved performance, this makes the network resistant to distributed denial-of-service attacks. Furthermore, MaidSafe is as simple to use as traditional centralized solutions, with the encrypted files represented as a virtual file system providing application-independent access. MaidSafe is currently undergoing extensive testing with a leading healthcare provider.

The SAFE (Secure Access For Everyone) Network is made up of the unused hard drive space, processing power and data connection of its users. It offers a level of security and privacy not currently available on the existing Internet and turns the tables on companies, putting users in control of their data, rather than trusting it to organisations. A number of features make this possible. No need to give your password to anyone, or ask a third party's permission to access your data. Your PIN and Keyword are used to locate your data on the network and your password, which never leaves your machine, is then used to decrypt it locally. This means that no one needs to hold a record of your files, or your login details and there's no need to ask anyone for permission to access it. This process is called Self-Authentication and enables you to find, unlock and decrypt your own data. Files uploaded to the network are broken into pieces, encrypted and distributed across the network. This process is called Self-Encryption.

When a user uploads (or saves) a file to the network, via one of the SAFE Network apps, the file is automatically broken up into chunks. These chunks are then encrypted (encoded so that only authorized parties can read it), randomized and stored on the computers of other SAFE Network users. These encrypted chunks are completely unreadable and inaccessible to anyone other than the owner.

Cloud computing is latest trend in IT world. It is Internet-based computing, whereby shared resources, software and information, are provided to computers and other devices on-demand, like the electric grid. This technology has the capacity to admittance a common collection of resources on request. It is proving extremely striking to cash strapped IT departments that are wanted to deliver better services under pressure. Concept of this new trend started from 1960 used by telecommunication companies until 1990 offered point to point data circuits and then offered virtual private networks. But due to network traffic and make network bandwidth more efficient introduced cloud to both servers and infrastructure. The development of this Amazon played vital role by making modern data centers. In 2007 Google, IBM and many remarkable universities and companies adopted it. And in 2008 Gartner highlighted its characteristics for customer as well service providers [1].

This paper provides the guidelines and considerations required to IT enterprises for the adoption of cloud computing technology. The paper provides the awareness of cloud computing power to the IT industry by addressing the global challenges. In Our context-aware system supports audio and video learning and has also storage capabilities. It augments physical objects in a classroom environment with visual icons using RFID, near-field communication (NFC), and QR Code tags. Each tag uniquely identifies the resource. The system can then integrate the RFID, NFC, and QR Code data, so users can see and interact with the objects with all three technologies For example, a student can point his or her mobile device at an object tagged with RFID, NFC, or QR Code, and the student selects the type of reader required to identify the object's tag. If the student uses

an RFID reader, then the system switches its mode to read the ISO 14443A Mifare tags, which contain data about learning activities related to that object.

The high-level ISO 14443A Protocol works in the 13.56 MHz frequency and has a reading distance of 10 cm, so the device must be close to the tagged object. After the reader decodes the tag information, the interface displays the learning resource, which the user can access online or download from the database for later use.

2. Literature Review

The literature identifies three different broad service models for cloud computing:

1) Software as a Service (SaaS), where applications are hosted and delivered online via a web browser offering traditional desktop functionality for example Google Docs, Gmail and MySAP.
2) Platform as a Service (PaaS), where the cloud provides the software platform for systems (as opposed to just software), the best current example being the Google App Engine.
3) Infrastructure as a Service (IaaS), where a set of virtualized computing resources, such as storage and computing capacity, are hosted in the cloud. Groups are usually dynamic in practice, e.g., new employee involvement and present employee revocation in an organisation.

The alteration of membership makes safe data sharing tremendously complex. The unidentified system challenges new approved cloud users to gain knowledge of the content of data files stored previous to their participation, since it is unattainable for new granted cloud users to contact with unidentified data owners, and find the consequent decryption keys. A well-organized membership revocation method exclusive of updating the secret keys of the remaining cloud users is also required to reduce the complication of key-management.

3. Quality of Service in Cloud Computing

Cloud computing aims to distribute a network of virtual services so that consumers can access them from anywherein the world on payment at competitive costs depending on their Quality of Service (QoS) requirements [6]. Cloud Computing systems may flock thousands of internationally dispersed consumers at any given time. These consumers may access diverse types of services that have varying requirements depending on the type of consumers, services and resources involved. Saravanan et al proposed a novel framework for ranking and advanced reservation of cloud services using Quality of Service (QoS) attributes. In some situations, due to the vast number of requests, the providers are not able to deliver the requested services within requested time. To avoid this scenario, ranking technique is very much useful. All QoS characteristics are explained. But for implementation all QoS characteristics are not used.

- Ani considers only few QoS constraints, such as deadline, budget, file size, penalty rate ratio and requested length. Deadline is the maximum time consumer would like to wait for the result. Budget is the amount consumer wishes to pay for the resources.
- Penalty Rate Ratio is a ratio for consumer's compensation if the SaaS provider misses the deadline. Input File Size is the size of input file provided by users. Request Length is the Millions of Instructions (MI) required to be executed to serve the request.

- Sonal Dubey et al. have investigated the crisis of choosing an optimal progression of infrastructure resources to outline an lengthwise path for QoS provisioning in Cloud computing location.

The authors embrace amplification of QoS aware services model and recitation two resourceful algorithms for selecting an optimal sequence of infrastructure resources for lengthwise QoS provisioning. The main optimization focus for Cloud service provisioning is how to make up a progression of service components from virtualized services into the Cloud service and afford it to consumers. It is a time consuming process. Cloud computing has been the hypothesis shift in distributed computing due to the way the resource provisioning and charging. Managing QoS is a crucial task in making such an innovative technology to a larger consultation. Several researchers have put forward their ideas for new and innovative solutions for handling this imperative area is resource management. In this paper, we have carried out a decisive review of the most recent work carried out in this area. The findings of the authors in terms of the Strong points and Limitations of the proposed work has been presented in a table for easy reference. This extensive survey in QoS paper will be very much helpful for researchers to do research in QoS.

The present article analyzes the main research and technological challenges that should be addressed to unleash the full potential of IaaS clouds and enable the deployment of the future IoS. While we revisit some of the issues addressed by these previous studies, we also present these challenges from a new IoS requirement perspective. Cloud platforms considered in this challenge analysis can range from private on premise cloud infrastructures, large public IaaS providers, or hybrid cloud infrastructures.

4. Conclusion

In this paper, we design a secure data sharing method, for dynamic groups in an un-trusted cloud. A cloud user is able to share data with others in the group without revealing identity privacy to the cloud. In addition, it supports well-organized cloud user revocation and new user joining. In addition, the storage overhead and the encryption computation cost are stable. Extensive study shows that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

References

[1] Cheng-Kang Chu, Sherman S. M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng, “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage” IEEE Transactions on Parallel and Distributed Cloud Computing Systems, Volume: 25, Issue: 2, Issue Date: Feb2014.

[2] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Secure Cloud Storage,” IEEE Trans. Computers, vol. 62, no. 2, pp. 362–375, 2016.

[3] B. Wang, S. S. M. Chow, M. Li, and H. Li, “Storing Shared Data on the Cloud via Security-Mediator,” in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2016.

[4] R. S. Sandhu, “Cryptographic Implementation of a Tree Hierarchy for Access Control,” Information Processing Letters, vol. 27, no. 2, pp. 95–98, 1988.

[5] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," [7] D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proceedings of Advances in Cryptology – CRYPTO '01, ser. LNCS, vol. 2139. Springer, 2015, pp. 213–229.

[7] R. Canetti and S. Hohenberger, "Chosen-Ciphertext Secure Proxy Re-Encryption," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07).

[8] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in ACM Conference on Computer and Communications Security, 2009, pp. 121–130.]

[9] Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," in Proceedings of the 23th IEEE International Conference on Computer Communications.

[10] Jansen, W.A.; (2010), " Cloud Hooks: Security and Privacy Issues in Cloud Computing5719001 IEEE 2015 44th Hawaii International Conference on System Sciences (HICSS), pp1, 4-7 Jan. 2015.

*Corresponding author.
E-mail address: madhumala8887@gmail.com