ISSN: 2456 - 4664
International Journal of Advanced Trends in Engineering and Technology
Impact Factor 5.965, Special Issue, February 2018 – Conference Proceedings
National Conference on Recent Trends in Management Studies & Computer Applications
(KRUPACON 2017) On 21st & 22nd September 2017 Organized By
Krupanidhi Group of Institutions, Bangalore, Karnataka

CLOUD COMPUTING SECURITY: A REVIEW

Vijayamala S Yakri* & Anuradha N**
* Krupanidhi Group of Institutions, Bangalore, Karnataka
** Krupanidhi Degree College, Bangalore, Karnataka

Cite This Article: Vijayamala S Yakri & Anuradha N, "Cloud Computing Security: A Review", International Journal of Advanced Trends in Engineering and Technology, Special Issue, February, Page Number 5-8, 2018.

Abstract:

A system that uses a community instead of a local or personal computer to store, process, and process facts in remote storage maintained on the Internet. Equipment can be dynamically captured and managed through cloud infrastructure. It provides an online repository with a lot of facts and skills for your package. You only need an internet connection to access different types of sources and resources on the internet. This document includes an analysis of the virtually hardened cloud security components that digital hardware and applications provide to customers. In this study, we will talk about the confidentiality of documents. Cloud service providers (CSPs) can provide a degree of integrity and security to cloud service customers through cryptographic encryption algorithms. Anyone can access the data on the cloud server by decrypting it according to the application.

Key Words: Cloud Computing, Security, Cloud Storage, Service provider

Introduction:

Cloud refers to any type of network in a remote location (public or private). Almost all types of services (email, video conferencing, athletics, etc.) work in the cloud. Cloud computing [1] allows you to view all kinds of statistics at any time. The cloud infrastructure provides users with specialized resources called the front end, and the cloud itself is known as the backbone of providing these services to customers [2].

Figure 1: Shows the cloud infrastructure

Cloud computing offers users several functions. Some of the popular features offered by cloud computing are shown in Figure 2 below. Some web-based email services such as Gmail and Hotmail offer cloud carriers. If someone wants to access their email, they need an internet connection and an ISP, regardless of the hardware installed on a particular device. Compared to storing directly on the recipient's laptop, emails are hosted on Google and Microsoft servers. Now other offers like Skype Twitter, Media Sales (YouTube, Voting) and many other offers that could be examples of cloud service providers are coming on the same day. Create and save packages dynamically at any time.

Users do not want to bring special software packages to access cloud software. The easiest way for users is to connect to the internet and authenticate on a dedicated cloud. Anyone with login rights can access programs provided by the cloud. The cloud ecosystem provides the creation of online applications and software using the Internet as a service model [3].On all types of gateways, users have access to available cloud resources over the network. It can also be concluded that the cloud infrastructure has unbiased platform access to cloud functions. The cost of cloud services is not very high. Cloud storage provides green load balancing to ensure users receive secure and fast service on all cloud servers. In addition to the special features provided by the cloud, there are some drawbacks to using cloud storage. [18] Identify some common pitfalls related to cloud computing.

Security and Protection of User Data:

The biggest problem with the cloud is that you can use consumer data to celebrate your third birthday. More care is needed when storing important data in the cloud [21].

Portability Issues (Fixed):

Cloud Service Providers (PDCs) offer low portability features, so customers connect and rely on PDCs in all types of products [18].

Delete Only Custom Data or Events:

If a client deletes a cloud record, the stats may not be destroyed as the cloud may already have a copy of the data.

From the above conversation, we can see that one of the most important difficult situations surrounding cloud computing are some real customer security facts. This paper describes the various security measures used to protect garage cloud items [18].

Literature Review:

In the past, there have been several separate attempts to protect cloud data. A literature review of several of these works follows.

Mohammed Abdelhamid [4] introduced several strategies based on the RSA algorithm in 2009 to improve consumer privacy. “The main reason for the author is to give clients access to remotely stored facts.” So you can trust all the evidence. Subashini and Kavita [5] introduced a variety of defense systems through their own strategies and strategies that provided their own security style in different departments. Ahmed et al. [6] Various client-related security issues and accuracy of cloud sources. Their main goal is the comfort of cloud services and consumer information that should be on cloud servers.

The structure of the individual levels of cloud protection is described by Krishna Reddy and Reddy [7]. Their main goal was to make the cloud tools and customer information provided by the cloud server easier to use. It also analyzes various types of cloud server systems, including Software as a Service (SaaS), Application as a Service (PaaS), and Technology as a Service (IaaS). Sayam Kumar and Subramanian [8] proposed an elliptic curve cloud and Sobel product line to protect customer information and cloud assets. There are a few guidelines that are used to ensure security in this way and avoid honesty called data consistency. Compared to powerful pirates, it has some defense that can damage our stats.

Abbas Amini [9] proposed a practical cloud-based storage machine. In addition to the security decoration, we use several rules to protect the quality of the parts of the paper. To do this, they used the RSA algorithm. And another set of rules they used was the AES algorithm that hides information about garage owners. Sajjad Hashemi [10] proposed special security measures for processing cloud data. "It also demonstrates various principles within cloud computing to promote data security." Use a set of instructions to troubleshoot or troubleshoot security issues. For example, AES, DES. For the 2014 employer statistics, Svarnalat Bollavarapu and Bharat Gupta [11] proposed cloud processing stability for garage information devices. "Along with RSA, RC4 and ECC, the system uses a variety of algorithms for encryption and decryption strategies."

Velumadhava Rao and Selvamani [12] recognized various data protection problems and solutions for cloud processing. The main reason for these sensitive investigations is to improve the security and maintain the integrity of records. Salim Ali Abbas, Amal Abdul Baqi Mariusz [13] 2015 is an efficient, scalable and simple way to provide encryption and cloud services for customer information. It also provides some guidance on the consistency and security of information in elliptic curve encryption.AL-Museelem Waleed, Li Chunlin [14] evaluated the impact of lack of protection on client cloud statistics and services. UEC (Ubuntu Enterprise Cloud) is used to solve the problem of authenticity. The algorithms they used include encryption and decryption of documents to ensure the accuracy and security of the cloud [24-28].

Problem Statement:

Cloud computing is not necessarily peaceful because of the many complex situations of statistical security. Statistical privacy is provided for documents stored in the "garage cloud" using several encryption methods. However, there is a backlash that truth can be found for accuracy as it moves from the garage cloud to the car cloud for processing. Therefore, in this research phase, we will provide statistics to make cloud computing a more reliable technology for our customers. There may be a problem when an unwanted user tries to access the cloud from the original time cloud, and they may ignore the command, but ignore is always the case in many cases. So we have to look for customers or orders coming over and over and it's still illegal. To do this, you may encounter other issues that say your IP or Mac address can handle and block this computer. You can use AES, DES and RSA for the isomorphic side of this motif.

Risk and Security Concern:

The security goal chosen is to ensure that customers have lost their data from any kind of risk. Sometimes computers use this well-known purpose to protect certain information or services from unwanted objects or hackers [15]. In addition, companies must apply security measures at multiple layers to protect their sites, equipment and user information to achieve the required level of security. The exceptional safety standards an organization must have, according to Whitman [15], are listed below [19].

- Employee Security: The company specifies the legal nature of its employees or its association with employee confidentiality in order to access and disseminate all company resources and information. [18]
- Listening: Unauthorized parties may visit the team's website to access information, which may result in loss of personal information. Headphones secretly focus on other personal language interactions. Additionally, this attack can be carried out via email, on-site text messages, etc. [19]
- Information Security: Organizations must protect and protect confidentiality, integrity (integrity) and ownership facts for processing and storage through statistical security [19].
- Physical Protection: This protection allows companies to protect their physical property and many important residential buildings from unnecessary entry and abuse.
- Network level security: The company protects network components and communicates with group security. It also includes business materials transmitted over the network.
- Process Security: Employers keep records of all regularly conducted transactions and operations with organizational security.
- Communication security: Employers protect communications to protect various technologies, contact media, and their content from unwanted access.

Principles of Cloud Security:

Security guidelines for cloud data are defined in terms of cloud integrity. Here are six ideas for cloud services described by Ramgovind, Eloff, and Smith [16].

- Approval: In the cloud system, authentication maintains reference accuracy. Thanks to this law, the most influential legal entities protect access to cloud services. For cloud services and infrastructure, all unauthorized objects are denied [18] [25].
- Integrity: Integrity makes the data stored in cloud storage stable. This represents an acidic artifact (atomic, purity, separation and shelf life) that maintains the reliability of the cloud record [10] [26].
- Secrets: Confidentiality is important if you want to manage statistics from different organizations in different databases. Even if you're working in the public cloud, confidentiality is important and there are opportunities to jeopardize the facts. With a focus on protecting and protecting information and user profiles at all levels, you can implement your unique information security requirements in the cloud [27-32].
- Don't Deny: This concept guarantees the confidentiality of cloud data through multiple authentication protocols and provides a token that sends cloud server statistics to the client and vice versa. Unique ideas are used to prevent rejection, along with digital signatures, verification verification, etc.
- Accessibility: Cloud provider accessibility is another security concept. You should choose a cloud provider from public, private or hybrid cloud providers depending on the features and protection you need for your results. Choose an operator that currently doesn't need a new cloud provider or has full security for sponsored data and sources.
- Identity Verification and Verification: We must pay attention to our customers' needs and access rights to this security concept. If the buyer does not have a specified company, the supplier is rejected. We also tested client protection with username and password before accessing the cloud provider. Identifying and validating all types of clouds is the main theory of defense.

Conclusion:

Cloud refers to all types of networks far away. There is almost any type of application: email, video conferencing, athletics and more. Does it in the cloud? Cloud computing provides the ability to view certain statistics at any time. Cloud storage offers its customers a unique offer called a front-end stop, and the cloud itself matches the backpacks that customers offer these offers. One of the hardest things about cloud storage is storing data for more than one user. In this paper, we analyzed several security variables when dealing with cloud statistics. This study provides a description or definition of issues that may arise in cloud computing with some security issues.

Acknowledgement:

The authors express gratitude towards the assistance provided by The Management, Krupanidhi Group of Institutions (KGI) and Krupanidhi Research Incubation Centre, KGI in completing the research. We also thank our Research Mentors who guided us throughout the research and helped us in achieving the desired results.

References:

1. Anthony T.Velte, Toby J.Velte, Robert Elsenpeter, “Cloud Computing, A Practical approach”
2. B. Hayes, “Cloud Computing,” Commun. ACM, vol. 51, no. 7, pp. 9–11, Jul. 2008.
3. Shankar Nayak Bhukya, Dr. Suresh Pabboju, Dr. K Venkatesh Sharma, “Data Security in Cloud Computing and Outsourced Databases", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 2016 IEEE.
4. Mohamed Abdelhamid, PhD thesis, “Privacy-preserving Personal Information Management”, School of Computer Science, McGill University, Montreal, August 2009.
5. S Subashini, V Kavitha, “A survey on security issues in service delivery models of cloud computing”, Network and Computer Applications, Elsevier, Vol. 34, pp. 1-11, 2010.
6. Mahbub Ahmed, Yang Xiang, Shawkat Ali, “Above the Trust and Security in Cloud Computing: A Notion towards Innovation”, 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp.723-730, 2010.
7. V. Krishna Reddy, Dr. L. S. S. Reddy, “Security Architecture of Cloud Computing”, International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.
8. Syam Kumar P and Subramanian R, “An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.
9. Abbas Amini, MSc thesis, “Secure Storage in Cloud Computing”, Department of Informatics and Mathematical Modelling (IMM), the Technical University of Denmark, May 2012.
10. Sajjad Hashemi, “Data Storage Security Challenges in Cloud Computing”, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol 2, No 4, August 2013.
11. Swarnalata Bollavarapu and Bharat Gupta, “Data Security in Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014.
12. Dr. Salim Ali Abbas, Amal Abdul Baqi Maryoosh, “Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography”, Journal of Computer Engineering, Volume 17, Issue 4, Ver. I (July – Aug. 2015), PP 48-53.
13. Dr. Salim Ali Abbas, Amal Abdul Baqi Maryoosh, “Improving Data Storage Security in Cloud Computing Using Elliptic Curve Cryptography”, Journal of Computer Engineering, Volume 17, Issue 4, Ver. I (July – Aug. 2015), PP 48-53.
14. AL-Museelem Waleed, Li Chunlin, “User Privacy and Security in Cloud Computing”, International Journal of Security and Its Applications Vol. 10, No. 2 (2016), pp.341-352.

15. M. E. Whitman, Principles of information security, 4th ed. Boston, MA: Course Technology, 2012.
16. S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in Cloud computing," in Information Security for South Africa (ISSA), 2010, 2010, pp. 1–7.
17. Mr. V. Biksham, Dr. D. Vasumathi," Query based computations on encrypted data through homomorphic encryption in cloud computing security", International Conference on Electrical, Electronics, and ptimization Techniques (ICEEOT) - 2016 IEEE
18. Ahmed Albugmi,Madini O, Alassafi Robert Walters, Gary Wills," Data Security in Cloud Computing , 2016 IEEE"
19. R. Charanya1, M.Aramudhan2, K. Mohan3, S. Nithya4"Levels of Security Issues in Cloud Computing" International Journal of Engineering and Technology (IJET), Vol 5 No 2 Apr-May 2013.
20. Mrinal Kanti Sarkar, Sanjay Kumar," A Framework to Ensure Data Storage Security in Cloud Computing",2016 IEEE.
21. https://www.calyptix.com/research-2/top-5-risks-of-cloud-computing/
22. ShankarNayak Bhukya, Dr.Suresh Pabboju, Dr. K Venkatesh Sharma, "Data Security in Cloud computing and Outsourced Databases", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 2016 IEEE.
23. Z. C. Nxumalo, P. Tarwireyi, M.O Adigun "Towards Privacy with Tokenization as a Service", Department of Computer Science, University of Zululand, Empangeni, South Africa -2014 IEEE.
24. Athitya Kumaraguru, M, Viji Vinod & Rajkumar, N 2017, 'A Comparative Study on SVM and RVM in Imbalance Data', Journal of Advanced Research in Dynamical & Control Systems, vol. 10, no.03-Special Issue pp. 1393-1395.
25. Mercy Beulah E, Nirmala Sugirtha Rajini S & Rajkumar N 2016, 'Application of Data Mining in Healthcare: A Survey', Asian Jr. of Microbiol. Biotech. Env. Sc., Vol. 18, No. 4, pp. 999-1001.
26. Viji Vinod, Rajkumar, N, Karthikeyan, S & Subramanian, C 2015, 'Expectation of Rising Customer Intelligence System in Road Service Transport using Cloud Services', International Journal of Applied Environmental Sciences, vol.10, no.1, pp. 135-142.
27. Nirmala Sugirtha Rajini, S, Rajkumar, N & Mercy Beulah, E 2015, 'An Innovative Cloud Computing Infrastructure for e-Tourism', International Journal of Applied Environmental Sciences, vol.10, no.1, pp. 19-22.
28. Gohin, B, Viji Vinod & Rajkumar, N 2012, 'Cloud Computing Architecture for Visual Disabilities on E-Governance', International Journal of Computer Applications, vol. 52, no. 1, pp. 44.48.
29. Abinaya, S, Rajkumar, N, Josephine, MS & Karthikeyan, S 2016, 'A study on Keyword ranked Searching and Encrypted over mobile Cloud Data', Proceedings of the National conference on Smart Information Light fidelity (Li-fi) Internet of things Conferences (Silicon'16), Dr. MGR Educational and Research Institute University, Chennai
30. Gohin, B, Viji Vinod & Rajkumar, N 2013, 'Evaluation of Cloud software service accessibility of E-Governance Websites', International Conference (ICTCST-2013), Bakthavatsalam Memorial College for Women, Chennai, pp. 112-116.
31. Gohin, B, Viji Vinod & Rajkumar, N 2012, 'Usability of Cloud SaaS based E-Governance for people with Disabilities', International Journal of Computer Applications Proceedings on E-Governance and Cloud Computing Services – 2012, vol. 2, no. 2, pp. 23-28.
32. Mercy Beulah E, Nirmala Sugirtha Rajini S & Rajkumar N 2016, 'Application of Data Mining in Healthcare: A Survey', Asian Jr. of Microbiol. Biotech. Env. Sc., Vol. 18, No. 4, pp. 999-1001.