International Journal for Modern Trends in Science and Technology, 6(8S): 223-228, 2020

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTSTCIET42
Available online at: http://www.ijmtst.com/ncracse2020.html

A Review on Security Issue Solving Methods in Public and Private Cloud Computing

Swathi Priyadarshini[1],S Ramachandram[2]

[1]Research scholar, Department of computer science, Engineering college, Osmania University,
[2]Professor, Department of computer science engineering, Engineering college, Osmania university

To Cite this Article
Swathi Priyadarshini and S Ramachandram, "A Review on Security Issue Solving Methods in Public and Private Cloud Computing", *International Journal for Modern Trends in Science and Technology*, 6(8S): 223-228, 2020.

Article Info
Received on 16-July-2020, Revised on 15-August-2020, Accepted on 25-August-2020, Published on 30-August-2020.

ABSTRACT

The theory of cloud computing has been around for a long time, but it has recently become one of the most popular technologies. Using this service, customers may conduct computer tasks and from any location as long as they have an internet connection. Public, private, community and hybrid cloud deployment strategies exist. Large-scale computer platforms are now serving a significant number of people and companies due to cloud computing services. Encouraging enterprises to outsource their processing demands progressively by allowing access to massive volumes of low-cost compute resources Customers can access public cloud computing infrastructure over the internet. There is no longer any control over clients' data. This concept, however, has spawned many security problems. Public cloud computing security problems are discussed in this study to help businesses make better judgments about shifting to the cloud, more damaging security risks are presented.

Key words: *- cloud computing; security issues;cloud security; privacy*

INTRODUCTION

Cloud computing introduces a new generation of internet-based computing that is highly scalable, distributed, and provides computer resources as a service. Cloud computing has evolved from its early conceptions to its most advanced forms. Information and Communications Technology (ICT) has lately seen the "Next-Best-Thing" develop as cloud computing [1]. Cloud computing has emerged as a utility paradigm that is gaining traction in both industry and academic research. Because it incorporates more modern ideas, it is currently considered the next evolution in distributed computing [2]. It is the primary goal of every firm to operate in today's competitive marketplace, reduce expenses, and increase profits. The vast majority of today's companies and organizations are heavily reliant on computer systems. Investments in servers, computers, and other equipment must be made to purchase them and maintain them. These devices need IT personnel and experience and their initial purchase and ongoing use and maintenance [3]. The majority of firms now prefer to outsource their computing needs to public cloud providers. As an example, an enormous volume of storage space is needed by a variety of businesses, including insurance firms, data banks, and hospitals, to store and preserve their data. Enterprises will get the computer resources they need at a lower cost thanks to cloud service providers who provide big storage capacity to fit their needs [4]. Organizations will save money by outsourcing computational needs because they won't have to purchase and maintain the software and hardware used to store and process data, as well as IT staff to manage them, space allocation to keep the equipment's, payment for electricity, and other energies, and

payment for maintaining and repairing the equipment.

SECURITY OF CLOUD COMPUTING: Security is an issue because of the cloud's significance in the social infrastructure. Building a secure environment for the deployment, business software, web administration, and email service supplied by cloud computing is the primary problem [5]. It has enormous potential for a dependable, accessible, and adaptive infrastructure in autonomous, distributed, and grid computing settings [6]. The cloud's advantages and prospects excite and worry users, who are equally concerned about the security risks of implementing it. Security concerns in the cloud have become a competitive advantage for cloud computing (CC) companies. To increase the service provider's performance, it is necessary to use a security system and platform to boost cloud security and storage. Protecting data and making its services available to the customer with excellent performance is the main objective of a secure cloud. Also, it may detect and block assaults on the data and services that are being accessed.

LITERATURE REVIEW

Ge Y, Wei G [7] A load balancing task scheduler based on the GA algorithm was presented. Tasks are planned using a sliding window approach in which the window size is specified, and the job that arrives in the sliding window is scheduled. If you want to know how long each job will take to complete, you can utilize Kernel canonical Correlation Analysis (KCCA). As a result, the GA is implemented constantly, updating the system's status to assign the job to a virtual machine (VM). Ying Changtian, Yu Jiong [8] An energy-aware Genetic Algorithm has been devised to schedule appointments based on make span and energy. To reduce energy usage, they used Dynamic Voltage Scaling (DVS) and proposed two algorithms.

Wang, Liu, Chen, Xu, Xi, and Dai [9] Algorithms for reducing the time it takes to construct a virtual machine and evenly disbursing the workload across virtual machines have been proposed. Two fitness functions are used in the selection procedure, with the population being initialized using a greedy methodology. A task's completion time and inter-load variance are inversely related to both fitness functions. The greater the fitness ratio, the more likely you are to be chosen when it comes to being selected. Instead of using fixed values, they used adaptive probabilities for crossover and mutation. An improved GEP algorithm with double fitness functions (DF-GEP) has been developed by Kun-lun, Jun, Jian, and Qing-yun [10]. (DF-GEP). Map/Reduce programming architecture is used to implement the method.'s Job completion time and operating costs are included in the modified ETCC matrix. In contrast, the conventional matrix simply has task completion times. Double fitness functions are used to improve the encoding and decoding process compared to the GEP algorithm. In comparison to the GEP approach, this strategy lowers the total work completion time and also minimizes the operating costs of operations. Chun-Yan LIU, [11] Ant colony optimization (ACO), and the genetic algorithm (GA) were combined to provide the best solution possible, which takes advantage of both the positive feedback from ACO and the powerful search capabilities of the genetic algorithm. The initial substance is computed using the GA method, and the optimal schedule is determined using ACO. Faster execution can be performed by using this algorithm's efficient search of the resource. Verma, Kaushal [12] The BCHGA proposes scheduling applications to cloud resources that reduce execution costs while fulfilling the results' budget. Priority is allocated to each task in a process based on the importance of the study. These priorities are then used to generate the initial population of BCHGA in order to increase the population's diversity. Singh, Kalra [13] proposed and developed an improved GA for a shorter make time. Instead of using a random technique, the Enhanced Max-Min algorithm generates the initial population (tasks with an average execution time are assigned to the resource with the slowest processing time). Crossover and mutation are used on this original population, and the new offspring/schedule that is produced is added to the population. Select a schedule based on how many people it can support.

SECURITY ISSUES IN CLOUD

Security of data: When cloud computing and web services operate on an open network, they are vulnerable to attack from anyone on the network. In cloud computing, as we all know, users' data is stored and processed in the cloud. When using public cloud services, users have no control over the cloud infrastructure that manages their data, which increases the risk of data loss. These security concerns for users' data are shown below:

Data Breach: Confidentiality and Integrity are the two primary data security attributes addressed. In order to maintain the security of sensitive

information, only those parties or systems that have been granted access to it are permitted to do so. Data integrity is concerned with preventing unauthorized deletions, fabrications, or modifications to data.

Data lock-in: Customers are unable to easily switch from one vendor to another as a result of this. Cloud computing was feared by users because of the risk of losing their data. In the wake of Coghead's collapse, clients were forced to rewrite their applications onto a new platform. Cloud APIs, such as the Go Grid API, should be standardized as a solution.

Data Remanence: As the name suggests, data resonant frequency refers to the residual representation of data that has been eliminated in some way. There are very few security dangers in private cloud, but in public cloud, especially in the IaaS layer, there are many due of the open nature of cloud computing.

Data Recovery: - Users' data can be damaged or lost in the event of a network problem. The data should be backed up in order to prevent this kind of loss from occurring in the future. Those who use the cloud can preserve a local copy of important data.

Data Locality: Data stored in the cloud is not accessible to the consumer; this could be problematic. According to data privacy rules in various European nations, some data cannot be exported from the country. This makes the location of information particularly crucial in many enterprises' architecture plans.

Hence, server security, Database security etc. is necessary considered to assure decent employment of cloud computing

Security at Network Level: Network systems can be divided into shared and non-shared, public and private, restricted and vast area networks. At least a dozen attacks have targeted each of these systems. To ensure network security, one must take into account elements such as the confidentiality and integrity of data in the network, effective data and network access limits and security maintenance methods in the face of third-party threats.

Threats associated with network level security are as:

Domain Name System (DNS): attacks–DNS is a basic building piece of the internet that allows users to access websites and exchange emails. An IP address is generated from a domain name using the Domain Name System (DNS) on the network (Internet). It's far easier to recall a domain name than a company name. When the user's request is sent to a malicious cloud rather than the server they requested, this is a DNS assault. Domain Name System Security Extension undoubtedly reduces domain risks; however, several examples have been recorded in which these protections have shown to be insufficient [14].

Sniffer attacks: network information can be hacked A sniffer is a piece of software that collects information on network traffic. Sniffers are the real-life savers when it comes to network problems. Through a sniffer, an intruder can read the contents of a network packet. [15].

Reusability of IP Addresses: Whenever a user leaves the network, the IP address assigned to that node is redistributed to a new one. It takes some time to change an IP address in the domain name system (DNS). A hacker may be able to gain access to the data during this lag time since the address is still in the DNS cache, which could violate the confidentiality of the prior user. [16].

Border Gateway Protocol (BGP) Prefix Hijacking - When an Autonomous System (AS) IP address is declared incorrectly, hijackers are able to trace the untraceable IP addresses and gain control of them. The BGP model is used by AS to communicate. It is possible that the erroneous IP address was announced by a defective AS, causing the traffic to be sent elsewhere than desired. As a result, sensitive information is exposed and obtained by an unauthorized source. **Security at Application Level:** Software and hardware modifications are necessary for application-level security to ensure that intruders cannot take control of any of the programs. To get access to the system, attackers pose as trusted users, and the system is damaged by this. As a result, it is imperative to implement security measures to reduce the dangers at this level. The threats to application-level security are:

Denial of Service Attacks: Disruptive services (DoS) prevent authorized users from accessing the services they've been assigned. Some cloud resources are unavailable to users because of the high volume and volume of traffic on the server, which leads to congestion. An intrusion detection system (IDS) is applied to protect against DoS attacks [17].

Cookie Poisoning: A cookie can be tampered with in order to get access to a program without the user's permission. A user's personal data is stored in cookies. The cookie's contents can be tampered with as soon as it is made available. In order to avoid this problem, it is possible to wipe up cookies on a regular basis or encode the cookie's data [18].

Invisible Field Manipulation: Using a web page, we may see that some fields are suppressed because they contain information that is only accessible to the page's developers. These fields are susceptible to assault since they can be changed.

Backdoor and Debug Options: The purpose of enabling the debug option is merely to make modifications to the code during development. Unintentionally enabling debugging settings opens a door to code modification by a malicious party. [19].

Distributed Denial of Service Attack: DDoS targets the substantial services active on server. It overloads the server with numerous of packets so that it fails to handle them and obtain the control of information flowing at certain times Prevention treatment suggested against DDoS is to install IDS on all the machines [20].

CAPTCHA Breaking: Anti-spam and anti-botnet abuse have been made easier with the introduction of the Completely Automated Public Turing Test (CAPTCHA). CAPTCHA security has recently been breached by spammers, who take advantage of the audio systems that service providers such as Google and Hotmail use to read CAPTCHA characters for the visually impaired [21].

Risk of Google Hacking: When it comes to searching for information on the internet, Google has emerged as the most reliable resource. When an attacker utilizes the Google search engine to look for personal information about a targeted individual, they are still doing Google hacking. Millions of Gmail users' log-in information was stolen by a Chinese hacking organization in 2010 during a Google hacking case. [22].

4.0 EXISTING SECURITY SCHEMES

Table 1 Existing security Schemes for Cloud

Scheme	Suggested Approach	Strengths	Limitations
[1] User Identity	Consider using an active bundle method where sensitive data is encrypted and the bundle enables itself upon arrival at its destination.	Trusted Third Party (TTP) verification is not needed	In order for SP to make use of identifying information, the data must first be decrypted.
[2] Trust Model for interoperability in cross cloud	Users and service providers are separated and trust techniques are proposed for each separately in this domain-based approach.	Secure multi-layered cloud applications	Obtain identification and behavioral verification, but not integrity verification
[3] Reputation-based trust management	Based on overlay networks, the DHT structure is used.	comprehensive usage of virtualization to secure cloud services	The performance must be verified by use of a sample.
[4] Virtualization	Cloud components are audited using shared middleware and logs, as well as the executable file system, using the Advanced Cloud Protection System (ACSP) to secure guest VMs.	Prone to different types of security attacks	System performance marginally degraded
[5] Secure Virtualized network	Organizations should be encouraged to conceal the internal workings of their services in order to reduce the risk of data leakage.	Identifies the attacking party	If attacker gets the address of any other VM, may harm VMs in between
[6] Secure Data Storage	Byzantine failures, unauthorized data alteration, and the addition of homomorphism token with distributed verification of erasure-coded data are all covered by this system.	preventing data loss during dynamic data operations and being resistant to byzantine failures	The location of fine-grained data errors has not been addressed in this study.

Searchable encryption methods in cloud computing:

Access to a centralized pool of resources is made simple and on-demand through cloud computing. For many people, cloud storage is the best option for reducing the burden on local storage. However, storing private information on remote computers creates privacy concerns and is becoming a source of concern for many people. With SE (Searchable Encryption), users' sensitive data is protected while still being searchable on the server. SE enables the

server to inspect encrypted data without disclosing any information contained in encrypted data.
Suggested Enhancements (SE) You may search for keywords in encrypted content using this method. SE systems allow a user to outsource encrypted data to the server while retaining the ability to search for the data. Papers and keywords are secure from a security perspective. SSE and PEKS are SE's two most important sub-divisions. It is a part of the private key primitive. As long as you have the private key, you are allowed to create ciphertexts and set trap doors for search purposes. Unlike with the public key primitive, PEKS is linked to it. Although many people can generate ciphertexts, only the private key user can set up search trapdoors.

Model of searchable encryption:

Three parties are involved in a searchable encryption method: a secure information owner O, a semi-trusted server S, and a limited number of users who are allowed to search. Each party's job is as follows:

Data owner: A data owner would want to outsource a collection of documents D= D1, D2, ... Dn" coupled with specific keywords. So that they may be searched right away, data owners must first encrypt their documents and keywords and then send the ciphertexts to the virtualized environment.

Data user: In order to search for articles containing a given word, an authorized user must provide the server with the trapdoor of this query keyword. Once the documents have been scanned, the server will show the user just those that include the search phrase.

Server: When the server receives a version of a query phrase from a user, it searches through ciphertexts and sends relevant content to the user. We assume that the server is honest, but a little suspicious. This implies that the server will perform the protocol successfully, but it may analyse the data it receives and try to get more information.

CONCLUSION:

Cloud computing security and privacy issues were investigated in this work, as well as the cloud computing environment. Also, we looked into the various architectures and the requirements, applications, and associated issues and concerns associated with each of them. Efforts are being made to solve the issues that cloud adoption presents. The paper's main focus is on the security and privacy issues that must be addressed and controlled in order for this new computing paradigm to perform effectively. Problems with data security and integrity in the cloud need to be explored before implementing cloud services. In addition, regular audits of the cloud are necessary to guarantee that the cloud is working effectively and provides a safe environment for attacks. Each and every component of the cloud must be evaluated, from hardware to cloud services.

In the future, cloud computing's profitability and its actuality should be the subject of more study. As a second track, we'll look at how top management decides whether or not to implement such a strategy in the organization. Organizations' adoption of new technologies can be better understood by using the Innovation Diffusion Theory. We need to conduct a field study to investigate how cloud computing affects the perspectives of enterprises and how they evaluate their experience with cloud computing.Need of data mining can also include to make privacy and segregation of large cloud data.

References

[1] Cheng and Lai (2012). "The Impact of Cloud Computing Technology on Legal Infrastructure within Internet—Focusing on the Protection of Information Privacy." Procedia Engineering 29: 241- 251.

[2] Tripathi and Mishra (2011). Cloud computing security considerations. Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on, IEEE

[3] Patidar, K., Gupta, M. R., Singh, G., Jain, M. M., & Shrivastava, M. P. (2012). Integrating the Trusted Computing Platform into the Security of Cloud Computing System. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2(2), pp. 1-5

[4] Madhavi, K. V., Tamilkodi, R., & Sudha, K. J. (2012). Cloud Computing: Security threats and Counter Measures. International Journal of Research in Computer and Communication technology, IJRCCT, Vol. 1(4), pp. 125-128.

[5] Rani, A. M. G., & Marimuthu, A. (2012). A Study on Cloud Security Issues and challenges. Int.J.Computer Technology & Applications, Vol. 3(1), pp. 344-347. [4] Kumar, K., Rao, V., & Rao, S. (2012). Cloud Computing: An Analysis of Its Challenges & Cloud Computing: An Analysis of Its Challenges & Security Issues. International Journal of Computer Science and Network (IJCSN) Vol. 1(5), pp. 1-8.

[6] Chandrahasan, R. K., Priya, S. S., & Arockiam, L., (2012). Research Challenges and Security Issues in Cloud Computing. International Journal of Computational Intelligence and Information Security, Vol. 3(3), pp. 42-48.

[7] Ge Y, Wei G., "GA-based task scheduler for the cloud computing systems", int conf web inf syst min, vol. 2; 2010. p. 181–186.

[8] Ying Changtian, Yu Jiong, "Energy-aware Genetic Algorithms for Task Scheduling in Cloud Computing", in proceeding of Seventh China Grid Annual Conference, 2012.
[9] Wang, Zhaobin Liu, Yi Chen, Yujie Xu, Xiaoming Dai, "Load Balancing Task Scheduling based on Genetic Algorithm in Cloud Computing", in proceeding of IEEE 12th International Conference on Dependable, Autonomic and Secure Computing, pp: 146-152, August 2014.
[10] LI Kun-lun; Wang Jun; Song Jian; Dong Qing-yun, "Improved GEP Algorithm for Task Scheduling in Cloud Computing", in proceeding of Second International Conference on Advanced Cloud and Big Data, pp:93-99, Nov 2014.
[11] Chun-Yan LIU, Cheng-Ming ZOU, Pei WU, "A task scheduling algorithm based on genetic algorithm and ant colony optimization in cloud computing", in proceeding of 13th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, ISBN: 978-1-4799-4168-1, January 2015.
[12] Amandeep Verma, Sakshi Kaushal, "Budget constrained priority based genetic algorithm for workflow scheduling in cloud", in proceedings of Communication and Computing, pp.216-222,2013.
[13] Shekhar Singh, Mala Kalra, "Scheduling of Independent Tasks in Cloud Computing Using Modified Genetic Algorithm", in proceedings of Sixth International Conference on Computational Intelligence and Communication Networks, 2016.
[14] D. E. Eastlake and others, "Domain name system security extensions," 1999.
[15] Z. Trabelsi, H. Rahmani, K. Kaouech, and M. Frikha, "Malicious sniffing systems detection platform," in Applications and the Internet, 2004. Proceedings. 2004 International Symposium on, 2004, pp. 201–207
[16] R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, "A Survey on Security Issues in Cloud Computing," arXiv Prepr. arXiv1109.5388, 2011.
[17] K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusion detection for grid and cloud computing," It Prof., no. 4, pp. 38–43, 2009
[18] D. Gollmann, "Securing Web Applications," Inf. Secur. Tech. Rep., vol. 13, no. 1, pp. 1–9, Jan. 2008.
[19] R. Lua and K. C. Yow, "Mitigating ddos attacks with transparent and intelligent fast-flux swarm network," Network, IEEE, vol. 25, no. 4, pp. 28–33, 2011.
[20] U. Jangid, N. Sharma, and K. Rathi, "A Survey on Secure the Cloud Environment using hypervisor-based virtualization technology," Int. J. Innov. Comput. Sci. Eng., vol. 1, no. 3, pp. 27–29, 2014.
[21] L. M. Joshi, M. Kumar, and R. Bharti, "Understanding Threats in Hypervisor, its Forensics Mechanism and its Research Challenges," Int. J. Comput. Appl., vol. 119, no. 1, 2015.
[22] T. Y. Win, H. Tianfield, and Q. Mair, "Virtualization Security Combining Mandatory Access Control and Virtual Machine Introspection," in Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, 2014, pp. 1004–1009