WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secure Banking with Error Recovery Process in Cloud Computing

[1]Mrs. R. C. Dyana Priyatharsini, [2]P. Ajay Kumar Reddy, [3]P. Anil Babu, [4]P. Surya Pavan

[1,2,3,4] Bharath institute of higher education and research, Chennai

ABSTRACT:

Cloud computing has grown to become an integral part of present as well as future information technologies. This technology has been designed to be used with internet by providing features such as information storage, remote access, etc. Cloud computing has been proved as an effective tool for all the provided services but it also comes with various types of threats. Over the years of its development, different fire attacks and data theft has been reported as a crucial factor since the data stored in the cloud by an organization or an individual user is basically confidential and sensitive. These data are illegally accessed by many hackers and further it will be used to fire attack the user. This paper mainly aims to highlight such attacks and provide suggestions for sorting the data breaching issues. ary of your work in paper .

Keywords: Cloud computing, security Challenges, Vulnerabilities in cloud computing, cyber attacks.

Introduction:

****Data Storage and Cloud****

Data storage has always been a place for useful information shortage, innit? Even with large scale storage devices, the space ain't be enough to contain the massive amount of information out there, you know? Cloud computing is like an internet-centric open standard model, which is pretty cool and stuff. This model is full of different types of services, both hardware and software, which the service providers don't need no high management efforts for providing and maintaining them. The term "cloud computing" aims to make high power computing systems more awesome, you know? It also aims to reduce the price by making it more efficient and stuff. Though the benefits and facilities provided are very much effective and stuff, the available technical barriers might stop cloud computing from being a thing that's everywhere. One of the main constituents of cloud computing is security, which is like a really big deal and remains as the most significant concern of the system and stuff, ya know? It usually suffers from various types of security concerns and attacks like malicious codes and stuff. In addition, various new concerns like storage and moving of data through the cloud is a big problem for the user, ya know? The possibility of locating in a different place with different regulations adds a lot to this problem, which is like a pretty big deal too. It is also very important for a cloud service provider to confirm the usability and availability of their services, ya know? There are various reasons that could affect the availability and accessibility of the computing resources, like service denial or natural/unnatural disasters and stuff. Data privacy is one of the prime concerns associated with the security of cloud computing as the data must be protected from any third party, which is frequently reported by the users and stuff. Since cloud computing is used for sharing data, data theft is remaining as very common and big risk, which is available for both users and service providers, inniters.

****Cloud Computing and Virtualization Challenges****

Cloud computing has various ways to meet consumer requirements, and one of these ways is virtualization. Even though virtualization is brought in to benefit the consumer, it has its own disadvantages, like issues related to the isolation of data and communication among the viral machines. Through cloud computing, cyberattacks are more likely to happen. Lot of these cyber-crime belong to the most common, as well as potential encounters, which has taken place in the wider internet, like malicious insider, DDOS attack, nefarious use and abuse of cloud computing, programming interface of insecure application, etc. It is important for the service providers who deal in the field of cloud computing to enhance their cyber security and access control system to their resources in order to keep a record of who dealt with them. This paper presents the list of the problems related to challenges which falls over the security of the information. This paper also presents the three different categories which are threats, attacks, and other challenges over the security.

Currently, the data shows the involvement of cloud computing in approximately everyone's life. It is because of the little or no cost services delivery for the storage spaces and the application. Most of the users uses these services on a regular basis. It can be easily explained with the example of email system which is used for exchanging information in forms of text, images videos, etc.; on demand subscription services; various social networking sites and collaboration tools for working along with the people in real time and over same document.

****Impact of Cloud Computing****

The involvement of services of cloud computing does not end here as it is also brought in application within the various types of businesses and it also provides these services on rent to prevent a one-time investment of the companies. Undoubtedly, these services have changed our lives on a great e xtent but the issues of security which comes along with it makes the user vulnerable to many types of available cyber-crimes that can be heard and seen on daily basis.

There are many techniques and methods used by the hackers for accessing cloud without being legally authorized and these criminals also create disruption the services associated with the cloud for attaining their targeted objectives. There is possibility that the services of cloud computing gets tricked by the hackers as they make their unauthorized entrance to the data as a valid entrance and thus gains control over access of the data stored in the cloud.

Overall, the impact of cloud computing on individuals and businesses continues to evolve, bringing both benefits and security challenges that must be ad dressed to ensure safe and efficient use of these services.

METHODOLOGY

Software **Existing System**

Large-scale problems in the physical and life sciences are being revolutionized by Internet computing technologies, like grid computing, that make possible the massive cooperative sharing of computational power, bandwidth, storage, and data. A weak computational device, once to such a grid, is no longer limited its slow speed, small amounts of local storage, and limited bandwidth: It can avail itself of the abundance of these resources that are available elsewhere on the network. Without revealing to the remote agents whose computational power is being used, either one's data or the outcome of the computation on the data. Large-scale problems in the physical and life sciences are being revolutionized by Internet computing technologies, like grid computing, that makes possible the massive cooperative sharing of computational power, bandwidth, storage, and data. A weak computational device, once connected to such a grid, is no longer limited by its slow speed, small amounts of local storage, and limited bandwidth: It can avail itself of the abundance of these resources that are available elsewhere on the network. Without revealing to the remote agents whose computational power is being used, either one's data or the outcome of the computation on the data.

Disadvantages

* Secure outsourcing for widely applicable sequence comparison problems as well as other unrelated issues

* Risk of Leak of Secret Information.

Proposed System

We propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.Our scheme can achieve fine-grained access control, with the help of theGroup user list, any user in the group can use the source in the cloud and revokedUsers cannot access the cloud again after they are revoked.We propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspirewith the untrusted cloud.

Advantages of Proposed System

•Power Means of Persuasion and control and More Reliable.

• It's more secure and efficient.

• Data confidentiality.

Result

****COUNTER MEASURES****

The infrastructure of the cloud computing comprises of a provider of the services which is being responsible for providing resources for computing for the end user. All we have to do for assuring the best possible services is important for the service providers to ensure the users regarding the security safety of the cloud. Through applying methods of advanced security as well as defining stringent security policies, this may be done.

1. DevSecOps processes — DevSecOps and DevOps are continuously been observed in order to decrease the options of vulnerability and exploitations', enhance the quality of the codes, deployment of features, and hiking the application's speed. Including security procedures, advancement, and QA in the units of the business/applications team rather than depending upon a single security verification team is important for the operations as per the demands of the today's businesses.

2. Automated application deployment and management tools — Hike in the speed and amount of security threats in combination with the insufficient skills in relations to the security leads to the fact that even the professional with highest experience of security cannot keep up. With the help of automation, ordinary tasks can be removed and it also supplement the human work benefits with that of machines which a basic element of advanced operations ofIT.

Below Are the Top 5 cloud security issues experienced private cloud:

i. Cons spanning of control in relation to the security is lacking in the virtualized and traditional server private cloud infrastructure!!!

ii. Hike in the infrastructure's complexity results in more effort/time of maintenance and implementation?!

iii. Skilled staff is available as per the requirement for managing the software defined data centre's security?

iv. Visibility is not complete over the software defined data centre's security?!

v. Newly developed advance level attacks and threats!!!!

A force which act from outside through which the nodes which existed in one state gets transferred to another is termed as a threat. The data is stored in the node and this node provides the user with a platform for using the application in services form. Significant numbers of intrusions or attacks are available occurring within the applications of the cloud.The 3 service models of the cloud "rovi'es various services to the user and also discloses data's issue of security as well as risks which are available within the systems of cloud.

1.SQL injection protection:-

This is a virtual attack on computers, usually containing SaaS. These types of attacks cause the most damage to SaaS due to poor application performance. It also uses an unsecured connection to complete the execution of SQL (unauthorized) commands. These types of attacks are programmed to gain access to unauthorized information that is protected and not allowed to be publicly accessible.

2. Abuse and malicious use of cloud computing:-

Hackers exploit vulnerabilities in the actual recording process of the cloud. They also provide SaaS, PaaS and IaaS services. Hackers can do this through suspicious activities such as phishing and/or spamming. These threats exist at all 3 levels.

3. Network Sniffer:-

This is also a SaaS-related threat. With these types of threats, hackers can gain access through the application. This allows them to capture packets flowing over the network as well as data sent via unencrypted packets. In such a case, the file will be publicly available.

4. Session Hijacking:-

In network protection, this is an attack on the security of the user session. When a user logs into the site a new session will start on this server. The new session contains all the data and user information on the server, so there is no need for a password every time the user accesses the novel page. Having all the necessary knowledge, a hacker can break into a work session and successfully insert the session code via HTTP. Session identifier is used by the server to identify the user for a particular session. Hackers use this type of session hijacking to gain control of the session identifier, which allows them to gain illegal control over user information. Cross-site scripting, session manipulation, session side hijacking, and session prediction are the most common session hijacking attacks.

5. Man-in-the-Middle Attack :-

MITM attack is another type of speech hijacking in which the hacker uses a sniffer to intercept communication between devices. Therefore, collect information from these devices and proceed with Hacking attacks on the information sent. The hacker creates an independent connection to the user's device, and the user trusts that the connection is direct and private. But in reality, the hacker has full control of the session. This is a major threat to the SaaS model.

Conclusion

This article aims to show the problems that cloud computing users face in security reporting, and also to show the biggest impact that deserves to be rewarded. There are many issues and issues related to cloud computing security. These issues are considered to have a serious impact on user privacy and trust. With good performance and good solutions, understanding all the security risks as well as privacy risks are difficult tasks.More, trust, honesty and privacy are the factors that make security important in applications. As cloud computing continues to evolve, its security will have risks and threats in the future. Service providers and users must be aware of security risks and prepare solutions for these problems to prevent their information from being blocked from any Attacks. This article also offers suggestions and important open questions for understanding climate. This article also aims to provide new directions for this research and help researchers find solutions to these threats and risks.

References:

Research Papers:

1.M. Jensen, M. Schwenk, J. Grushka, N. Iacono, "On Technical SafetyIssues in the Cloud" IEEE World Conference on Cloud Computing,Page 109 - Sixteen, 2009.

2.Mather, T., Kumaraswamy, S., and Latif, S., Cloud Security and Privacy.The Big Apple: O'Reilly, 2009.

3.B. Reddy, R. Paturi, "Cloud Protection Issues", IEEE International Conference on Services Computing, 2009.

4.J. Viega, "Cloud computing and not the common man", IEEEC ComputSociety, Volume forty-two, no. 8, pp. 106-108, 2009.

5 A.Singh, M. Sharivastava, "A Review of Attacks on the Cloud Computing", International Journal of Engineering and Innovation Yuga (IJEIT), Volume 1, Number 4, 2012.

6.G. Kulkarni, J. Gambhir Amrita, "Security in Cloud Computing"International Journal of PC Engineering and Age (IJCET), Vol3, no.1, pp 258 – 265, 2012.

7.Habib, S. M., Hauke, S., Ries, S., & Mühlhäuser, M, "Considering as a Facilitators in Cloud Computing: A Survey", Magazine of Cloud Computing, Volume 1, Number 1, Pages 1-18,2012.

8.Zisis, D., and Lekkas, D,. "Addressing Cloud Computing Security Issues". Destiny Era Computer Structures, Volume 28, Number 3, pp 583-592, 2012.

9.A cloud computing environment against DDoS attacks", IEEE, , pp. 1 –Bansidhar Joshi, A. Santhana Vijayan, Bineet Kumar Joshi, "Securing 5,2011.

10.Hyong LV and Yin Hu, "Evaluation and research about the cloud Computing Safety Protect Policy", IEEE, pp. 214-216, 2011.11

11. M. Rajendraprasad, R. Laxman Naik, V. Bapuji," Cloud Computing:Studies Issues and Implications", Global Journal of Cloud Computing and Service Technology (IJ-Near) Vol.2, no.2, pp. 134-140, 2013.

12.Mladen A. Vouch, "Cloud Computing Issues, Research &Implementation", Journal of Computing and Information Yuga, Vol. Char, pp. 235–246, 2008.

13.Devki Gaurav Pal, Ravi Krishna, Prashant Srivastava, Sushil Kumar,Monark Bag, Vrijendra Singh, A New Open Security Framework for Cloud Computing, International Journal of Cloud Computing And Services Science (IJ-CLOSER) Vol.1, no.2, pp.45-52, 2012.

14.Ashish Kumar, World of Cloud Computing and Security International Journal of Cloud Computing and Services Science (IJCLOSER) Volume I, No. 2, p. 53-58, 2012.

15.Hemraj Saini, T. C. Panda, Minaketan Panda, "Estimation Malware in Computer Networks and Security", International Journal of System Security and its Applications (IJNSA), Vol.3, No.6,pp. 161-171, 2011.

16.C. Modi, D. Patel, B. Borisania, A. Patel, M. Rajaajan, "A.Research on security issues and solutions in different cloud layers Computing", Journal of Supercomputing, Vol. 63, no. 2, page 561-592 in 2013.

17.L. Vaquero, L. Rodero-Merino, D. Moran, "Locking the sky:A survey of IaaS cloud security ", Computing, Vol. 91, no. 1, 93 p. –118 in 2011.

18 .Pankaj Patidar and Arpit Bhardwaj, "Overcoming Network Security SSL in Cloud Computing Environment", International Journal Computing and Information Technology, Volume I. 2, 6, 2011.

19. Insider Threats Related to Cloud Computing, CERT, July 2012.http://www.cert.org/.

20 P. P. Ramgonda and R. R. Mudholkar, "CloudMarket Cogitation And SQL Injection Prevention Techniques for University Clouds"International Journal of Computer Technology and Applications, Vol.3, no. 3, 2012, pages 1217-1224.