Security Issues in Cloud Computing

Mahalakshmi. D[1], Mrs. T. Sathiyabama[2]
[1]IIIMCA, [2]Assistant Professor
Department of Computer Applications, Dr. Sns Rajalakshmi College of Arts & Science,
Coimbatore, Tamil Nadu, India

ABSTRACT

Using a set of presented package and properties through the internet is called cloud computing. Data hubs located everywhere the world offer the cloud services. As this field of machinery seen a express growth in current times, security has been the foremost distress. Security is the main issues for all technology both it was from past or newly modernized. The information might be own or executive data stored in the cloud is facing probable dangers from hackers and there is a need to categorize the possible security holes that can be made more secure and tough. One work in this field will enable security thinkers and researches to know the dynamic threats that users or service providers are disturbed and do enquiry about the different security implements and models suggested.

Keyword: Cloud Computing, Cloud Security, Security Threats, Security Techniques, Cloud Security Principles.

INTRODUCTION

Cloud computing is a expression that has be approximately for a while but it can be a adding issue to many specialized vendors. Cloud computing is packing and contact or recovery of software and data over community and remote networks. This differs from outdated computing where data and software are stored on a limited firm effort. Anywhere there is no actual "cloud", as in a weather-event, the saying is generally used to represent the internet as a means of admission to lists and files. Skill account experts will memory early charts of grid structures represented as clouds with lines strained into and out of cloud, suggesting networks from network attached procedures like processors and waiters.

SECURITY ISSUES FOR CLOUDS:

➢ Security have frequent issues that involve many technologies with network ,database, operating system, virtualization ,resource arranging, transaction management ,load balancing, concurrency control and memory management.

➢ Data mining techniques may be applicable to malware uncovering in clouds.

➢ Cross cutting services have design layer, cloud monitoring layer, reliability layer and risk analysis layer.

SECURE QUERY PROCESSING WITH HADOOP:
Overview of Hadoop:

➢ Major part of our system HDF is which distributed java based file system with volume to handle a large no of nodes stored petabytes of data. Ideally a file size is multiple of 64MB.

Inadequacies of Hadoop:

1. **No ability to handle encrypted sensitive data:**
   Sensitive data reaching from medical registers to credit card transactions need to be kept using encryption techniques for added security.

2. **Semantic Web Data Management**:
   There is a need for possible solutions to improve the performance and scalability of queries against semantic web data such as RDF (Resource Description Framework).

3. **No fine-grained access control:**
   HDFS does not afford fine-grained access control.

4. **No strong authentication:**
   A user who can connect to the JobTracker can submit any job with the rights of the account used to set up the HDFS.

TECHNIQUES TO SECURE DATA IN CLOUD:
Authentication and Identity:
➢ Validation of users takes place in various methods like in the system of keywords that is known separately, in the form of a safety mark, or in the form a determinate amount like pattern.

Data Encryption:
➢ If you want to store complex files we use facts encryption systems such as keywords and firewalls when numbers is converted we should have the underground core for reading the data.

Information Integrity and Privacy:
➢ Cloud computing provides information and belongings to valid users. Resources can be recovered through web browsers and can also be accessed by malicious attackers

Availability of Information (SLA):
➢ Service Level arrangement is used to provide the information about whether the network resources are current for users or not.
➢ The way to provide user-friendliness of properties is to have a backup idea for local resources as well as for most essential information.

THE BENEFITS AND DISADVANTAGES OF CLOUD COMPUTING
The Benefits of Computing Cloud:
➢ Cloud computing offers the chance of ranging the information system of a creativity at the request the future use.
➢ Services provided in the cloud are broad.

The Disadvantages of Cloud Computing:
➢ Cloud computing looks to talent a great coming.
➢ Many group or business is against this idea, as the famous Richard Stallman .
➢ Cloud Computing leads to the loss of device over the development of applications.

PROBLEMS OF SECURITY IN CLOUD
➢ It has four categories of security, data security, logical security, physical security and administrative security

Problems of Data Security:
➢ There are several studies that display the dangers which exposed the safety of the data stored in the cloud
➢ That safety plays a very main role in cloud computing.

➢ The various security challenges in cloud computing.
➢ The position and Socket Layer).program of data which is secured by using IPSec (IP Security), SSL (Secure

Problems of Logic Security:
➢ They considered that virtualization is one of the main components of a cloud.
➢ The other issue is the control of administrator on host and guest operating systems.
➢ It have focused their work on the risk of intrusion that threatens the cloud.

Problems of Administrative Security:
➢ Administrative problems all cases that affect the type of worker and the type of deal
➢ There may be a case that some cloud workers are not the legalworker.
➢ They may be copying of a Web page that now exists in order to fake and induce users into giving private or financial particulars or their passwords.

DATA SECURITY CHALLENGES:
➢ Data loss or Data leakage can have simple effect on business, brand and hope of a group.

Security:
➢ Protection of data is the most significant tasks in cloud computing.
➢ It is important to deliver authentication, authorization and access device for data stored in cloud. The three main areas in data security are

Confidentiality:
➢ Data is safe from any attacks. So security test has to be done to watch data from mean user such as Cross-site Scripting, Access Control devices etc.

Integrity:
➢ Users should not supply their exact data such as passwords so that honesty can be organizations reverse stoppage as a major secure.

Availability:
➢ Availability is the most important problem in several issues. It depends on the procedure between dealer and the client.

Solutions to Data Security Challenges:
➢ Encryption is suggested as a better resolve to secure data.

➢ Before loading data in cloud server it is improving to translate data.

➢ Data Owner can give promise to specific group secondary such that data can be easily saved by them.

➢ Mixed data centric safety is to be used to provide data access control.

CONCLUSION:

Cloud computing is the most popular idea in IT today; even an abstract noise from UC Berkeley says "Cloud Computing is likely to have the same control on software that foundries have had on the hardware trade". They go on to mention that "inventors would be wise to project their next generation of systems to be arranged into Cloud Computing". While many of the expectations may be cloud build-up, I believe the new IT finding model open by cloud computing is here to visit. Whether approval becomes as widespread and bottomless as some guess will depend largely on killing fears of the cloud. Cloud fears mostly stem from the supposed loss of switch of complex data. Modern control methods do not tolerably address cloud computing's third-party files loading and treating needs. In style I present, the writers suggest to extend control processes from the creativity into the cloud through the use of Trusted Computing and applied cryptographic performances. These measures should improve much of today's fear of cloud computing, and, I believe, have the possible to provide obvious business intelligence advantages to cloud sharing. The approach also relates to likely problems and taking advantage ascending from a greater trust on cloud computing, and how to maintain security in the face of such attacks. Namely, the new threats need new structures to maintain and develop security. Among these are tools to regulator and understand privacy outflows, perform verification, and security accessibility in the face of cloud denial-of-service attacks.

REFERENCES:

1. Boldreva A., Chenette N., Lee Y, O'neill A. (2009), "Order-preserving Symmetric encryption", Advances in Cryptology-EURO CRYPT 2009 Springer, Berlin/Heidelberg, pp. 224-241.

2. Boney D., Di G., Ostrovsky R., Persiano G. (2004), "Public key encryption with keyword search", Advances in Cryptology-Euro crypt, Springer, Berlin/Heidelberg, pp 506–522.

3. B. R kandukuri, R. Paturi V, and A. Rakshit, "cloud security issues",2009 IEEE International Conference on Services Computing, sep. 21-25, 2009, Bangalore, India, pp. 517-520.

4. N. Padia and M. Parekh, "Cloud Computing Security Issues, in Enterprise Architecture and Its Solutions," International Journal of Computer Application, vol.2, issue 1, pp. 149-155,December 2011.

5. A. Parakh and S. Kak, "Online data storage using implicit security," Information Sciences, vol.179,pp.3323-3331, 24 May2009.

6. K. Karkouda, N. Harbi, J. Darmont, and G. Gavin, "Confidentialité et disponibilté des donnéesentreposéesdans les nuages," in Proc. 9ème atelier Fouille de données complexes (FDC 12),pp. 1-14,2012.

7. S. O. Kuyoro, F. Ibikunle, and O. Awodele,"Cloud Computing Security Issues and Challenges," International Journal of Computer Networks, vol. 3,issue 5, pp. 247-255,2011.

8. R. Maheshwari and S. Pathak, "A Proposed Secure Framework for Safe Data Transmission, in Private Cloud," International Journal of Recent Technology and Engineering, vol.1, issue 1, pp.78-82, April 2012.

9. N. Padia and M. Parekh, "Cloud Computing Security Issues, in Enterprise Architecture and Its Solutions," International Journal of Computer Application, vol.2, issue 1, pp. 149-155,December 2011.

10. A. Parakh and S. Kak, "Online data storage using implicit security," Information Sciences, vol.179, pp.3323-3331, 24 May2009.

11. K. Karkouda, N. Harbi, J. Darmont, and G. Gavin, "Confidentialité et disponibilté des donnéesentreposéesdans les nuages," in Proc. 9ème atelier Fouille de données complexes (FDC 12),pp. 1-14,2012.

12. A. Talib, "Security Framework of Cloud Data Storage Based on Multi Agent System Architecture: Semantic Literature," Computer and Information Science, Published by Canadian Center of Science and Education, vol. 3, pp.175-186, November 2010.