INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 2123 - 2128
RECEIVED : 28-03-17. PUBLISHED: 22-04-17.

April 22, 2017

MOBILE BASED REMOTE MONITORING SYSTEM AND DISASTER SENSING USING MALWARE ATTACKS

[1]Akhila Aniyath, [2]V.Yathavaraj,

[1]PG Scholar, Department of Computer Science, Maharaja Engineering College, Coimbatore.

[2]Assistant Professor, Department of Computer Science, Maharaja Engineering College, Coimbatore.

Abstract

The main objective of this project is to enhance the data storage security during disaster. So that IaaS (Infrastructure as a Service) methodology will be implemented here. This is to provide prior security for the storage devices during malware attacks and also during disaster. The remote monitoring system is growing very rapidly due to the growth of supporting technologies as well. And also problem that may occur in remote monitoring such as the number of objects to be monitored and how fast, how much data to be transmitted to the data centre to be processed properly. This study proposes using a cloud computing infrastructure as processing centre in the remote sensing data. This study focuses on the situation for sensing on the environment condition and disaster early detection. Where those two things, it has become an important issue, especially in big cities big cities that have many residents. This study proposes to build the conceptual and also prototype model in a comprehensive manner from the remote terminal unit until development method for data retrieval. We also propose using DCN method to guarantee the delivery from remote client to server. In added with the remote monitoring system will keep on tracking the database architecture for the data transfer. Whenever destruction occur the data base architecture will transfer the database to the concern location assigned from the admin. So that data base can be saving exactly with the last fine transaction. Here data loss will not occur at any cost. This method is based on IP conflict procedure. So that roll backing process can also be possible. Using the same procedure of IP conflict method and this method will shows the data up to last minute transaction. Enhanced DCN has been used for encrypt the data during the time of data transaction. When a database has been encrypted using a DCN means, the DB could not access by third party.

Keywords: Disaster analysis, local optimization, remote monitoring, software engineering, Data processing

1. INTRODUCTION

As per survey most of the banking server and data centres are placed in metropolitan cities, most of the metropolitan cities are in sea shore. For example in India: Chennai, Mumbai and etc. Even in USA New York city is in sea shore only. For last 10 years tsunami destroyed the cities 3 times. In some case data centres may get destroyed due to earth quake or in flood. In our project we are finding out a solution to safe hand the data centres and banking servers. Basically massive computation power and storage capacity of cloud computing systems allow scientists to deploy computation and data intensive applications without infrastructure investment, where large application data sets can be

stored in the cloud. However, they are either insufficiently cost-effective for the storage or impractical to be used at runtime. In this paper, toward achieving the minimum cost benchmark, we propose a novel highly cost-effective and practical storage strategy that can automatically decide whether a generated data set should be stored or not at runtime in the cloud. The main focus of this strategy is the local-optimization for the trade off between computation and storage, while secondarily also taking users' (optional) preferences on storage into consideration. Both theoretical analysis and simulations conducted on general (random) data sets as well as specific real world applications with Amazon's cost model show that the cost-effectiveness of our strategy is close to or even the same as the minimum cost benchmark, and the efficiency is very high for practical runtime utilization in the cloud.

2. RELATED WORKS

Our ID management algorithm is the rest to enjoy all of the following properties: (a) both arrivals and departures of hosts are handled, (b) departure of a host causes at most one existing host to change its ID, (c) the ratio of the largest to the smallest partition is at most 4, with high probability, and (d) the expected cost per arrival / departure is (R + log n) messages, where n denotes the current number of participants, and R denotes the cost of routing one message in the DHT. In fact, our algorithm is independent of the topology of the overlay network used for routing[1]. This paper presents the design and evaluation of Pastry, a scalable, distributed object location and routing substrate for wide-area peer-to-peer applications. Pastry performs application-level routing and object location in a potentially very large overlay network of nodes connected via the Internet. It can be used to support a variety of peer-to-peer applications, including global data storage, data sharing, group communication and naming[2]. We consider the problem of horizontally partitioning a dynamic relation across a large number of disks/nodes by the use of range partitioning. Such partitioning is often desirable in large-scale parallel databases, as well as in peer-to-peer (P2P) systems. As tuples are inserted and deleted, the partitions may need to be adjusted, and data moved, in order to achieve storage balance across the partici-pant disks/nodes. We propose efficient, asymptotically optimal algorithms that ensure storage balance at all times, even against an adversarial in-section and deletion of tuples[3].

3. ANALYSIS

The rapid growth of communication technology has led to many data-intensive applications that produce huge volumes of data. Most of those applications are relying on data centre networks (DCNs) to store and process their huge data. Mean while, DCNs are vulnerable to potential disasters. Some recent natural disasters like 2012 Sandy Hurricane, 2011 Japan Tsunami, 2008 China Wenchuan earthquake, etc., which cause failures of a set of network components and Break downs of some DCNs. For example, China Wenchuan Earthquake in 2008 leads to the damages of over 60 enterprise DCNs and Japan Tsunami and earthquake causes the devastations often of DCNs. Thus, in order to improve the survivability of data in DCNs, the data should be backed up among geo-distributed DCNs . The disasters can be roughly classified into three categories, i.e., predictable disasters, unpredictable disasters, and human Made attacks, in which predictable disasters (e.g. hurricane, flood, and tsunami) can be forecasted before hand by atmospheric and environmental conditions. For a predictable disaster, we can obtain a nearly warning time for DCNs that will be affected by such disaster.

Therefore, considering the newly-generated data that fails to be protected by regular backup in those DCN sunder risk during the early warning time, it is highly desirable that such data can be backed up in the other safe DCNs with in the early warning time such that the data loss is minimized under disaster.

DCN Disaster Analysis

Due to global warming our earth may face many types of disasters like earthquake, tsunami, storm, flood and etc. This disaster can be analysed through cloud remote monitoring. This research main function to capture data from sensor both in digital or analog input. Package of specific sensors with Remote Terminal Unit will be placed in some places or objects prone to disasters. Cloud computing could be proposed as central of data processing to run service like service listener. It has function to capture and store information sent from the remote client. Otherwise, it could be used for the central data storage and application server to display the processed results to the user.

Data preservation using cloud service provider

CSP deals with the software architecture of the cloud service provider, which is inter related with the remote disaster tool, so that when ever disaster will occur the cloud service provider will trigger out the malware process. This process may execute through Intranet, Internet and also through GPS. So that global communication will be possible here. This architecture should be assigned during the server configuration. The Cloud service provider will the triggering function with the TPA(Third Party Auditing). This method will take cares the database migration process. So that when ever disaster will occur the CSP will trigger through the IP conflict and the data base will be restored in the concern location assigned by the admin. Admin can customize the database by providing priority to the table sets. The transfer will works according to the assigned priority with the DCN Node. This saves the database from data loss. The nest process will execute after the disaster and CSP trigger out process. The roll back process too needs IP conflict procedure for analysing the failure calculation as the location of the database. According to the admin request original database can be transfer to the default location and also transfer of duplicate database also possible.

Algorithm

1: At each beacon interval and data ensure

2: if p>t1ands6¼Uthen calculate tables

3: s U data partition

4: PutþID to a beacon message.

5:end if

6:ifp t1ands¼Uthen

7: s NU lime slot in the schedule

8: PutID to a beacon message.

9:end if not scheduled data

10: Upon receiving a beacon message onVi

11:foreach ID in the received beacon messagedo

12: ifID >0then

13: ID ID S fIDg:

14: else

15: ID IDnfIDg:

16: end if

17:end for

18:if ID fg jj>t2then

19: NotifyVdelandV delinitiate topology discovery

21:end if

22:Add the ID inV 0 i sbeacon message.

The objective function minimizes integer variable Y, which is the largest number of tasks on one node. W i j is a decision variable similar to W i j defined previously. The first constraint ensures that the schedule cannot consume more energy that the E min calculated previously. The second constraint schedules each task exactly once. The third constraint for c es Y to be the largest number of tasks on one node. The last constraint is a binary requirement for decision matrix W. Once tasks are scheduled, we then rearrange tasks—tasks are moved to earlier time slots as long as there is free time slot and no same task is executed on other node simultaneously. Algorithm 1 depicts the procedure. Note that k-out-of-n data processing ensures that k or more functional processing nodes complete all tasks of a job with probability1.Ingeneral, it may be possible that a subset of processing nodes, of size less thank, complete all tasks.

The Topology Monitoring component monitors the network topology continuously and runs in distributed manner on all nodes. Whenever a client node needs to create a file, the Topology Monitoring component provides the client with the most recent topology information immediately. When there is a significant topology change, it notifies the frame-work to update the current solution. We first give several notations. A term refers to a state of a node, which can be either U or NU. The state becomes U when a node finds that its neighbour table has drastically changed; otherwise, a node keeps the state as NU. We let p be the number of entries in the neighbour table that has changed. A set I D contains the node IDs with p greater thant1, a threshold parameter for a significant local topology change

4. PERFORMANCE METRICS

According to the performance metrics, the data will be transferred to a desired three locations for back up. At the time of back up the database will be partitioned and start to splitting up. At that time the speed is depends on the hardware and the receiving point's configuration..The same process will be reversed for back up process. But according to the result back up takes less time then restore. This is because back up is working under a emergency situation, but restoring works on relaxing situation.

Drive	Back up in seconds	Restore in seconds
Loc1	3.87767	17.5281
Loc 2	3.87878	17.5506
Loc 3	3.98989	15.9381

CONCLUSION

In this paper, we propose an effective and flexible distributed scheme with banking application and explicit dynamic data support to ensure the correctness of user's data in the cloud. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphism token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s). It is concluded that the application works well and satisfy the owner and customers. The application is tested very well and errors are properly debugged. The site is simultaneously accessed from more than one system. Simultaneous login from more than one place is tested. The project works according to the restrictions provided in their respective browsers. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one. The speed of the transactions become more enough now.

REFERENCE

[1] Balanced Binary Trees for ID Management and Load Balance in Distributed Hash Tables. G.S. Manku, "Balanced Binary Trees for ID Management and Load Balance in Distributed Hash Tables,"Proc. 23rd ACM Symp. Principles Distributed Computing (PODC '04),pp. 197-205, July 2004.

[2] Pastry: Scalable, Distributed Object Location and Routing for Large-Scale Peer-to-Peer Systems A. Rowstron and P. Druschel, "Pastry: Scalable, Distributed Object Location and Routing for Large-Scale Peer-to-Peer Systems,"Proc. IFIP/ACM Int'l Conf. Distributed Systems Platforms Heidelberg, pp. 161-172, Nov. 2001

[3].Online Balancing of Range-Partitioned Data with Applications to Peer-to-Peer Systems. P. Ganesan, M. Bawa, and H. Garcia-Molina, "Online Balancing of Range-Partitioned Data with Applications to Peer-to-Peer Systems," Proc. 13th Int'l Conf. Very Large Data Bases (VLDB '04), pp. 444-455, Sept. 2004.

[4] Smarter Cities Series: Introducing the IBM City Operations and Management Solution, IBM White Paper, 2011

[5] Yongqiang Zhang, Guozhen Zhao, Yongjian Zhang, "Design of a remote image onitorinmg system based on GPRS", International Conference on Machine Learning and Computing, 2009

[6] B. Durai, Timothy A. Gonsalves and Krishna M. Sivalingam, "Adaptive Push Based Data Collection Method for Online Performance Monitoring"

[7] Stuart Clayman et all, "Monitoring Service Clouds in the Future Internet", IOS Press, 2010

[8] Sinung Suakanto, Suhono Harso Supangkat, Suhardi, "Introduction to Finite Time Response-HTTP: a Simplest Way to Guarantee Quality of Service of Web Application under Best Effort Network", Proceedings International Conference AOTULE 2010

[9] Donald Kossmann, Tim Kraska, Simon Loesing, "An Evaluation of Alternative Architectures for Transaction Processing in the Cloud", SIGMOD'10, June 2010.

[10] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing", Grid Computing and Distributed Systems (GRIDS) Laboratory - University of Melbourne, Australia, 2008.