ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Efficiently Sharing the Report by Combining Cloud

A.Srikanth Kumar
B.V.Raju Institute of Technology.

ABSTRACT:

Advancements in cloud computing are resulting in a promising future for collaborative cloud computing (CCC), wherever globally-scattered distributed cloud resources happiness to completely different organizations or people (i.e., entities) are jointly utilized in a collaborative manner to produce services. Attributable to the autonomous options of entities in 300, the problems of resource management and name management should be together addressed so as to make sure the triple-crown readying of 300. However, these 2 problems have usually been addressed severally in previous analysis efforts, and easily combining the 2 systems generates double overhead. Also, previous resource and name management strategies don\'t seem to be sufficiently economical or effective.

By providing one name price for every node, the strategies cannot replicate the name of a node in providing individual varieties of resources. By invariably choosing the highest-reputed nodes, the strategies fail to take advantage of node name in resource choice to totally and fairly utilize resources within the system and to satisfy users' various QoS demands. We tend to propose a 300 platform, referred to as Harmony that integrates resource management and name management in a very harmonious manner. Harmony incorporates 3 key innovations: integrated multi-faceted resource/reputation management, multi-QoS-oriented resource choice, and price-assisted resource/reputation management.

The trace knowledge we tend to collected from an internet commerce platform implies the importance of multi-faceted name and therefore the drawbacks of highest-reputed node choice. Simulations and trace-driven experiments on the real-world Planet research lab workplace show that Harmony outperforms existing resource management and name management systems in terms of QoS, potency and effectiveness.

KEYWORDS: *CCC, QoS*

INTRODUCTION:

Advancements in cloud computing are resulting in a promising future for collaborative cloud computing (CCC), wherever globally-scattered distributed cloud resources happiness to completely different organizations or people (i.e., entities) are jointly utilized in a collaborative manner to produce services. Attributable to the autonomous options of entities in 300, the problems of resource management and name management should be together addressed so as to make sure the triple-crown readying of 300. However, these 2 problems have usually been addressed severally in previous analysis efforts, and easily combining the 2 systems generates double overhead. Also, previous resource and name management strategies don't seem to be sufficiently economical or effective. By providing one name price for every node, the strategies cannot replicate the name of a node in providing individual varieties of resources.

By invariably choosing the highest-reputed nodes, the strategies fail to take advantage of node name in resource choice to totally and fairly utilize resources within the system and to satisfy users' various QoS demands. We tend to propose a 300 platform, referred to as Harmony, that integrates resource management and name management in a very harmonious manner. Harmony incorporates 3 key innovations: integrated multi-faceted resource reputation management, multi-QoS-oriented resource choice, and price-assisted resource reputation management. The trace knowledge we tend to collected from an internet commerce platform implies the importance of multi-faceted name and therefore the drawbacks of highest-reputed node choice. Simulations and trace-driven experiments on the real-world Planet research lab workplace show that Harmony outperforms existing resource management and name management systems in terms of QoS, potency and effectiveness. Cloud resource orchestration (i.e., resource provision, configuration, utilization and recall across a distributed set of physical resources in clouds) has been studied in recent years; these 2 problems have usually been addressed severally. Merely building and mixing individual resMgt and repMgt systems in three hundred can generate doubled, prohibitively high aloft. Moreover, most previous resMgt and repMgt approaches don\'t seem to be sufficiently economical or effective within the large-scale and dynamic atmosphere of three hundred.

Previous repMgt systems neglect resource heterogeneousness by assignment every node one name price for providing all of its resources. In existing system claim that node name is multi-faceted and will be differentiated across multiple resources (e.g., CPU, bandwidth, and memory). As an example, an individual trusts a doctor for giving recommendation on medical problems however not on money problems. Similarly, a node that performs well for computing services doesn't essentially perform well for storage services. Thus, previous repMgt systems don't seem to be effective enough to supply correct steerage for trustworthy individual resource choice. Due to the problems of resMgt and repMgt, this can be not economical and trustworthy. Single-QoS-demand assumption. In this paper, we tend to propose AN integrated resource reputation management platform, known as Harmony, for collaborative cloud computing (CCC). we tend to introduce Harmony, a cardinal platform with harmoniously integrated resource management and name management.

It can do increased and joint management of resources and name across distributed resources in cardinal. we tend to propose a comprehensive answer for storing and maintaining log records during a server in operation during a cloud-based atmosphere. we tend to address security and integrity problems not scarcely throughout the log generation section, however conjointly throughout different stages within the log management method, as well as log assortment, transmission, storage, and retrieval. the key contributions of this paper areas follows. we tend to propose design for the assorted parts of the system and develop crypto graphical protocols to deal with integrity and confidentiality problems with accumulating, controlling, and querying log records at the honest however curious cloud supplier and in transit. This provides terribly economical, effectively and trustworthy resource sharing among clouds. Choosing resources from the situated choice

RELATED WORK

Recent Trust Models In Grid

A grid could be a framework providing services to access and manage distributed hardware and computer code resources. A radical authentication is needed before any requested access or operation is allowed on any resource of the grid

Reliable Delivery and Filtering for Sys log

First Published: November 17, 2006 Last Updated: November 14, 2008 The Reliable Delivery and Filtering for Sys log feature permits a tool to be custom-made for receipt of sys log messages. This feature contributes reliable and secure delivery for sys log messages mistreatment Blocks protractible Exchange Protocol (BEEP). to boot, it permits multiple sessions to one work host, freelance of the underlying transport methodology, and provides a filtering mechanism referred to as a message mortal. This module describes the functions of the Reliable Delivery and Filtering for Sys log feature and the way to put together them in a very network.

Consistent Hashing and Random Trees: Distributed Caching Protocols for Relieving Hot Spots on the World Wide Web

We illustrate a family of caching protocols for distributed networks that may be accustomed decrease or eliminate the prevalence of hot spots within the network.

Explorative Visualization of Log Data to support Forensic Analysis and Signature Development

Sebastian Schmerl, Michael Vogel, René Rietz, and Hartmut König Computer Networks and Communication Systems Group, Brandenburg University of Technology, Cottbus, Germany In this paper, we tend to propose associate approach for log resp. audit information illustration that aims at simplifying the analysis method for the protection officer. For this purpose audit information and existing relations between audit events square measure delineated diagrammatically in an exceedingly 3 dimensional area. We tend to describe a general approach for analyzing and exploring audit or log information within the context of this presentation paradigm. Further, we tend to introduce our tool, that implements this approach and demonstrate the strengths and edges of this presentation and exploration type.

On the Security of Public Key Protocols

DANNY DOLEV AND ANDREW c. YAO, MEMBER, IEEE the Use of public key cryptography to produce secure network communication has received appreciable attention. Such public key systems are sometimes terribly effective against a “passive” snoop, namely, one WHO simply faucets the communication line and tries to decipher the intercepted message.

However, as observed in Needham Associate in Nursing Schroeder Associate in nursing improperly designed protocol can be prone to an “active” saboteur, one WHO could impersonate another user and will alter or replay the message. As a protocol could be compromised in an exceedingly advanced means, informal arguments that assert the protection for a protocol square measure susceptible to errors.

Architecture of an Open Object-Oriented Database Management System

David L. Wells, Jose A. Blakeley, and Craig W. Thompson Texas Instruments An open, incrementally extensible object oriented database management system lets developers tailor database functionality for applications. It can also serve as a platform for research. This article describes the architecture of the Open OODB system. First we discuss its requirements, then its computational model. which builds database functionality as an extensible collection of transparent extensions to existing programming languages. We also describe how Open OODB's system architecture is decomposed into a kernel meta-architecture and a collection of modules implementing specific behavioural extensions. Finally, we discuss risks of the approach and report on the project’s status.

Concurrency Control in Distributed Object-Oriented Database Systems

Kjetil Nørv°ag, Olav Sandst°a, and Kjell Bratbergsengen In this paper we've given results from simulations with 2 completely different computer hardware ways. any work for the DBsim machine includes extensions that would build it additional appropriate for simulation of algorithms for object-oriented databases. Obviously, rather more will be through with each the simulation model and therefore the machine. This includes adding new schedulers to the system, e.g., alternative versions of the two-phase lockup computer hardware, like wound-wait and wait-die. during a real system, replication is employed for inflated dependableness and performance. this might even be integrated into this framework.

EXISTING SYSTEM

Cloud resource orchestration (i.e., resource provision, configuration, utilization and recall across a distributed set of physical resources in clouds) has been studied in recent years; these 2 problems have usually been addressed severally. Merely building and mixing individual resMgt and repMgt systems in three hundred can generate doubled, prohibitively high aloft. Moreover, most previous resMgt and repMgt approaches don\'t seem to be sufficiently economical or effective within the large-scale and dynamic atmosphere of three hundred. Previous repMgt systems neglect resource heterogeneousness by assignment every node one name price for providing all of its resources. In existing system claim that node name is multi-faceted and will be differentiated across multiple resources (e.g., CPU, bandwidth, and memory). as an example, an individual trusts a doctor for giving recommendation on medical problems however not on money problems. Similarly, a node that performs well for computing services doesn\'t essentially perform well for storage services. Thus, previous repMgt systems don't seem to be effective enough to supply correct steerage for trustworthy individual resource choice.

LIMITATIONS:

- Due to the problems of resMgt and repMgt, this can be not economical and trustworthy.
- single-QoS-demand assumption

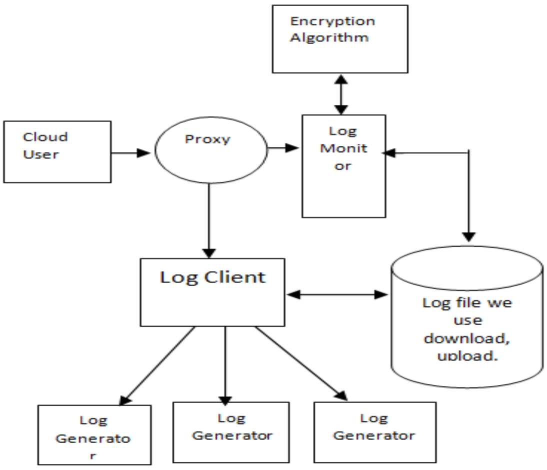
PROPOSED SYSTEM

In this paper, we tend to propose AN integrated resource reputation management platform, known as Harmony, for collaborative cloud computing (CCC). we tend to introduce Harmony, a cardinal platform with harmoniously integrated resource management and name management. It can do increased and joint management of resources and name across distributed resources in cardinal. We tend to propose a comprehensive answer for storing and maintaining log records during a server in operation during a cloud-based atmosphere. We tend to address security and integrity problems scarcely throughout the log generation section, however conjointly throughout different stages within the log management method, as well as log assortment, transmission, storage, and retrieval. The key contributions of these paper areas follow. we tend to propose design for the assorted parts of the system and develop cryptographical protocols to deal with integrity and confidentiality problems with accumulating, controlling, and querying log records at the honest however curious cloud supplier and in transit.

ADVANTAGES:

- This provides terribly economical, effectively and trustworthy resource sharing among clouds.
- Choosing resources from the situated choice

SYSTEM ARCHITECTURE

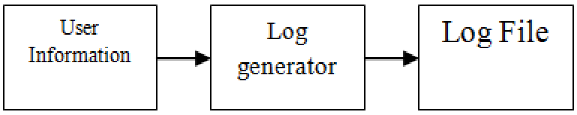


MODULES:

- ➢ Log Generators
- ➢ Logging Client or Logging Relay
- ➢ Logging Cloud
- ➢ Log Monitor

Log Generators

These are the computing devices that generate log data. Each organization hat adopts the cloud-based log management service has a number of log generators. Each of these generators is up to with logging capability. The log files generated by these hosts are not stored locally except temporarily till such time as they are pushed to the logging client.

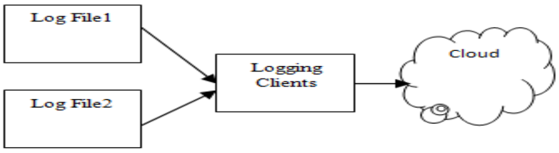


Logging Client or Logging Relay

The logging client is a collector that receives groups of log records generated by one or more log generators, and prepares the log data so that it can be pushed to the cloud for long term storage. The log data is transferred from the generators to the client in batches, either on a

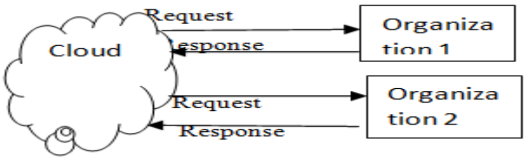
ISSN No: 2348-4845
International Journal & Magazine of Engineering,
Technology, Management and Research
A Peer Reviewed Open Access International Journal

schedule, or sand when needed depending on the amount of log data waiting to be transferred. The logging client incorporates security protection on batches of accumulated log data and pushes each batch to the logging cloud. When the logging client pushes log data to the cloud it acts as a logging relay. We use the terms logging client and logging relay interchangeably. The logging client or relay can be implemented as a group of collaborating hosts. For simplicity however, we assume that there is a single logging client.



Logging Cloud:

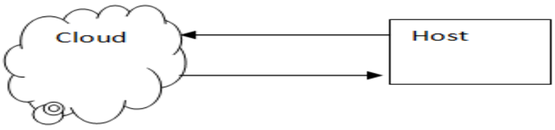
The logging cloud provides long term storage and maintenance service to log data received from different logging clients belonging to different organizations. The logging cloud is maintained by a cloud service provider. Only those organizations that have subscribed to the logging cloud's services can upload data to the cloud. The cloud, on request from an organization can also delete log data and perform log rotation. Before the logging cloud will delete or rotate log data it needs a proof from the requester that the latter is authorized to make such a request.



Log Monitor

These are hosts that are used to monitor and review log data. They can generate queries to retrieve log data from the cloud. Based on the log data retrieved, these monitors will perform further analysis as needed. They can also ask the log cloud to delete log data permanently, or rotate logs.

Queries to Retrieve log Response



ALGORITHM

Definition

The Advanced Encryption Standard (AES) is an encoding algorithmic program for securing sensitive however unclassified material by U.S. Government agencies and, as a possible consequence, might eventually become the factual encoding customary for business transactions within the non-public sector. (Encryption for the U.S. military and alternative classified communications is controlled by separate, secret algorithms.)In Jan of 1997, a method was initiated by the National Institute of Standards and Technology (NIST), a unit of the U.S. Department of Commerce, to seek out a additional sturdy replacement for the info encoding customary (DES) and to a lesser degree Triple DES. The specification demanded a even algorithmic program (same key for encoding and decryption) victimization block encoding (see block cipher) of 128 bits in size, supporting key sizes of 128, 192 and 256 bits, as a minimum.

The algorithmic program was needed to be royalty-free to be used worldwide and supply security of a comfortable level to shield information for ensuing twenty to thirty years. it absolutely was to be simple to implement in hardware and software package, furthermore as in restricted environments (for example, in a very sensible card) and supply sensible defences against numerous attack techniques. The entire choice method was totally hospitable public scrutiny and comment, it being determined that full visibility would make sure the absolute best analysis of the styles. In 1998, the government agency select fifteen candidates for the AES, that were then subject to preliminary analysis by the planet cryptanalytic community, together with the National Security Agency. On the idea of this, in August 1999, government agency elect 5 algorithms for additional intensive analysis. These were:

- MARS, submitted by an outsized team from IBM analysis
- RC6, submitted by RSA Security
- Rijndael, submitted by 2 Belgian cryptographers, Joan Daemen and Vincent Rijmen
- Serpent, submitted by Ross Hans Christian Andersen, Eli Biham and Lars Knudsen
- Two fish, submitted by an outsized team of researchers together with Counterpane\'s revered cryptologist, Bruce Schneier.

Implementations of all of the on top of were tested extensively in ANSI C and Java languages for speed and dependableness in such measures as encoding and decipherment speeds, key and algorithmic program set-up time and resistance to numerous attacks, each in hardware- and software-centric systems. Once again, elaborate analysis was provided by the worldwide cryptanalytic community (including some groups making an attempt to interrupt their own submissions). the top result was that on Oct a pair of, 2000, government agency proclaimed that Rijndael had been elect because the planned customary. On Dec vi, 2001, the Secretary of Commerce formally approved Federal scientific discipline customary (FIPS) 197, that specifies that each one sensitive, unclassified documents can use Rijndael because the Advanced encoding customary. Also see cryptography, information recovery agent (DRA)

RELATED GLOSSARY TERMS:

RSA algorithm (Rivest-Shamir-Adleman), data key, grey net (or gray net), spam cocktail (or anti-spam cocktail), fingers canning (finger print scanning),mugging, insider threat, authentication server, defense in depth, non repudiation

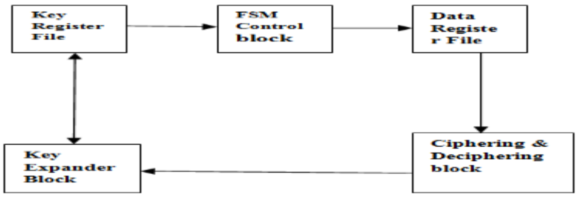
Explanations

AES relies on a style principle called a Substitution permutation network. it's quick in each code and hardware. not like its predecessor, DES, AES doesn't use a Feistel network.AES contains a secured block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael is nominative with block and key sizes in any multiple of thirty two bits, with a minimum of 128 bits. The block size contains a most of 256 bits, Still the key size has no problematic most.AES performs on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a bigger block size have further columns within the state). Most AES calculations square measure worn out a special finite field. The AES cipher is nominative as variety of repetitions of transformation rounds that convert the input plaintext into the ultimate output of cipher text. Every spherical consists of abundant process steps, as well as one that depends on the secret writing key. a collection of reverse rounds unit applied to remodel cipher text back to the initial plaintext exploitation identical secret writing key.

High-level description of the algorithm

1. Key Expansion— round keys area unit derived from the cipher key spherical keys area unit derived from the cipher key using Rijndael key schedule
2. Initial Round
   - ➢ Add Round Key— each computer memory unit of the state is combined with the spherical key victimization bitwise xor
3. Rounds
   - ➢ Sub Bytes - a non-linear substitution step wherever every computer memory unit is replaced with another in line with lookup table
   - ➢ Shift Rows— a transposition steps wherever every row of the state is shifted cyclically a definite range of steps.
   - ➢ Mix Columns— a combining operation that operates on the columns of the state, combining the four bytes in every column
   - ➢ Add Round Key
4. Final Round (no Mix Columns)
   1. Sub Bytes
   2. Shift Rows
   3. Add Round Key

Diagrams



CONCLUSION

We projected an entire system to firmly source log records to a cloud supplier. We tend to reviewed existing solutions and known issues within the current software system based mostly work services like sys log and sensible difficulties in a number of the present secure work techniques. During this work, mostly log management service. The attackers use below 3 steps to hack. First, the aggressor will intercept any message sent over the net. Second, the aggressor will synthesize, replicate, and replay messages in his possession. And Last The aggressor is a legitimate participant of the network or will attempt to impersonate legitimate hosts. we tend to implement a way to store secure log come in cloud which file we will modification browse, write, delete, transfer and transfer. We will implement AES rule that uses for log monitor and log generator. we tend to then projected a comprehensive theme that addresses security and integrity problems not simply throughout the log generation section, however conjointly throughout different stages within the log management method, together with log assortment transmission, storage and retrieval. One in all the distinctive challenges is that the drawback of log privacy that arises once we outsourced log management to the cloud. Log info during this case mustn't be nonchalantly linkable or traceable to their sources throughout storage, retrieval and deletion. we tend to provided anonymous transfer, retrieve and delete protocols on log records within the cloud victimization the Tor network. The protocols that we tend to developed for this purpose have potential for usage in many various areas together with anonymous publish-subscribe.

REFERENCES

1) An Efficient and Trustworthy Resource Sharing Platform for Collaborative Cloud Computing Haiying Shen, Senior Member, IEEE, and Guoxin Liu, Student Member, IEEE

2) Amazon Elastic Compute Cloud (EC2), http://aws.amazon.com,2013.

3) Drop box, www.dropbox.com, 2013.

4) P. Suresh Kumar, P. Sateesh Kumar, and S. Ramachandram, "Recent Trust Models In Grid,"J. Theoretical and Applied Information Technology, vol. 26, pp. 64-68, 2011.

5) J. Li, B. Li, Z. Du, and L. Meng, "CloudVO: Building a Secure Virtual Organization for Multiple Clouds Collaboration," Proc. 11th
   a. ACIS Int'l Conf. Software Eng. Artificial Intelligence Networking and Parallel Distributed Computing (SNPD), 2010.

6) C. Liu, B.T. Loo, and Y. Mao, "Declarative Automated Cloud Resource Orchestration,
   a. "Proc. Second ACM Symp. Cloud Computing (SOCC '11), 2011.

7) C. Liu, Y. Mao, J.E. Van der Merwe, and M.F. Fernandez, "Cloud Resource Orchestration: A Data Centric Approach , "Proc. Conf.Innovative Data Systems Research (CIDR), 2011.

8) V. Kantere, D. Dash, G. Francois, S. Kyriakopoulou, and A. Ailamaki, "Optimal Service Pricing for a Cloud Cache," IEEE Trans. Knowledge and Data Eng., vol. 23, no. 9, pp. 1345-1358, Sept. 2011

9) M. Cai and K. Hwang, "Distributed Aggregation Algorithms with Load-Balancing for Scalable Grid Resource Monitoring," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2007

10)] S. Di and C. Wang, "Dynamic Optimization of Multi attribute Resource Allocation in Self-Organizing Clouds," IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 3, pp. 464-478, Mar. 2013 Zol, http://www.zol.com.cn/, 2013.

11) D. Qiu and R. Srikant, "Modeling and Performance Analysis of Bittorrent-Like Peer-to-Peer Networks," Proc. ACM SIGCOMM, 200.