Research Paper

Computer Science

DATA STORAGE SECURITY AND DATA MANAGEMENT IN CLOUD COMPUTING

Kuldip M. Josh Lecturer in Department Of Computer Science, Shree G.K. & C.K. Bosamia College, Jetpur.

Jignesh M. Joshi Lecturer in Bhavan's Shree H.J. Doshi Information Institute, Jamnagar

ABSTRACT

Cloud Computing has been visualized as the future generation architecture of Information Technology activity. In difference to predictable solutions, Cloud computing moves the application software and databases to the huge information centers. Data security for such a cloud computing includes safe channels, access controls, and encryption. When we think the security of data in a cloud, we must consider: privacy, reliability, and accessibility. The challenge of building dependable, accessible and scalable data management systems able of serve petabytes of data for lots of users has tackled the data security and management research community as well as large internet enterprises. Existing future solutions to scalable data management, driven mainly by common application requirements, limit reliable access to only the granularity of single items, rows, or keys, thus trading off regularity for high scalability and availability.

KEYWORDS : - Security, Management, Cloud Computing, data

INTRODUCTION

Cloud computing is today's most modern research areas due to its capability to reduce costs connected with computing while increasing scalability and flexibility for computing services.

What is Cloud Computing?

Cloud computing is a common expression for anything that engages distributing hosted services more over the Internet. These services are normally separated into three categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). The name cloud computing was inspired from the cloud symbol that's frequently used to stand for the Internet in flowcharts and diagrams. The different types of deployment model are Throughout this paper, we will focus on one of the fundamental resources: throughput and delay. Estimating the outstanding bandwidth at a given time and in a given part of the network is difficult because, in a wireless network, the average is shared between close nodes. In this paper, we present a new method to evaluate the available bandwidth and end to end delay in ad hoc networks based on the IEEE 802.11 MAC layer. This scheme uses the nodes carrier sense capability combined to other techniques such as collision prediction to perform this estimation.

What is Data Management?

Scalable and constant data management is a challenge that has confronted the database research community for more than two decades. Historically, distributed database systems were the first common solution that deals with data not enclosed to the limitations of a single machine while ensuring global serializability. This design was not sustainable further than a few machines due to the crippling effect on act caused by partial failures and synchronization in the clouds. As a result, most of these systems were never widely used in industry. Current years contain therefore seen the coming out of a various class of scalable data management systems such Google's Bigtable, PNUTS from Yahoo! and other related but undocumented systems. All of these systems communicate with petabytes of data, provide online requests with severe latency and availability requirements, accommodate inconsistent workloads, and run on cluster computing architectures; stake claims to the territories used to be engaged by database systems.

SECURITY ISSUES

In a typical situation where an application is hosted in a cloud, two wide security questions that arise are:

– *How secure is the Data?*
– *How secure is the Code?*
Cloud computing environment is normally implicit as a potential cost saver as well as provider of advanced service quality. Security, Accessibility, Dependability, Data Integrity, Privacy, Access power, Validation is the major quality concerns of cloud computing service users.

SECURITY ADVANTAGES IN CLOUD ENVIRONMENTS

Presently cloud service providers manage very large systems. They have multipart processes and specialist personnel for maintaining their systems, which small enterprises may not even have an access to. Due to this, there are numerous security advantages for the cloud computing users. At this time present some of the most important security advantages of a cloud computing environment:

Centralization of Data:

In a cloud atmosphere, the cloud service supplier takes care of storage issues and small businesses need not spend a lot of money on physical peripherals for storage. Also, cloud computing based data storage provides a method to centralization of the data in a quicker and possible mode. This is primarily very useful for small type businesses, which cannot spend extra money on security parameters to secure the data.

Incident Response:

IaaS providers can put up a enthusiastic forensic server that can be used on require basis. As soon as, a security infringement takes place, server can be brought online. In some study cases, even a backup of the environment can be easily made and put onto the cloud without affecting the regular route of business.

Forensic Image Verification Time:

Some cloud storage implementations representation a cryptographic verifies sum or hash. For example, Amazon S3 create MD5 (Message Digest algorithm 5) hash automatically when you store an entity. Therefore in theory, they require to generate time intense MD5 checks using outside tools is eliminated.

PROBLEM STATEMENT

A main hurdle to moving Information Technology systems to the cloud is the lack of trust on the cloud supplier. The cloud supplier, in rotate, also needs to implement strict security policies, which in turn requires further trust in the clients. To get improved the internal trust between consumer and cloud supplier, a good trust foundation needs to be in place. Cloud computing can position for dissimilar things to different people. The privacy and security concerns will surely differ between a customer using a public cloud application, medium-sized enterprise using a modified suite of business applications on a cloud platform, and a management organization with a to cloud systems brings a different types of benefits and risks. What remains steady, though, is the real value that the user seeks to care for. For single task, the value which is at risk can range from loss of social independence to the contents. For a business, the value executes from main deal secrets to stability of business operations and public status. Much of this is quite hard to estimate and interpret into standard metrics of rate. The job in this conversion is to evaluate the opportunities of cloud implementation with the risks associated with the same. If cloud computing is so immense, then why is not everyone working it? Because the cloud acts as a big black box nothing inside the cloud is visible to client and this leads to two main issues that are:

Integrity:
It is level of confidence that the data in the cloud is protected against accidental or intended alteration without permission. Thus it implies that data should be directly stored on the cloud servers and any violation can be detected.

Privacy:
In this model providers ensured that all critical data example credit card number are masked and only approved users have access for it. In 2009 a major incident in SAAS cloud occurs with Google Docs. Google Docs allocate users to edit document online and share these documents with other users. But once these documents shared with anyone it was available for everybody. Thus in epoch of personal privacy personal data should really protect.

ANALYZING PRESENT SCALABLE SYSTEMS

Abstractly, a distributed system can be modeled as a grouping of two different components. The system state, which is the distributed metadata significant for the proper operation and the strength of the system. This state requires stringent constancy guarantees and fault acceptance to ensure the proper functioning of the system in the available of different types of failures. But scalability is not a main requirement for system state. On the other hand is the application state, which is the application exact information or data which these systems store. The constancy, scalability and accessibility of the application state is dependent purely on the requirements of the type of application that the system aim to support, and different systems provide unreliable tradeoffs between different attributes.

SYSTEM STATE

In a distributed data management system, data is partitioned to achieve scalability and pretend to achieve fault acceptance. The system must have a correct and constant view of the mappings of partitions to nodes, and that of a separation to its replicas. If here is a concept of the master amongst the model, the system have to also be alert of the position of the master at all times. Note that this data is in no way connected to the data hosted by the system; rather it is required for the appropriate operation of the entire system. Since this status is critical for operating the system, a distributed system cannot afford any unpredictability or loss. In a more traditional context, this match to the system state in the logic of operating systems which has a comprehensive view about the state of the machine it is controlling.

APPLICATION STATE

Distributed data management systems are intended to host large amounts of data for the applications which these systems aim to support. Here refer to this application specific data as the application state. The application state is normally at least two to three orders of amount larger than the system state, and the consistency, scalability, and accessibility requirements vary based on the applications.

Data Model and its inference:
The unique feature of the three main systems we consider in this paper is their simple data model. The primary abstraction is a table of items where every item is a key value pair off. The value can either be an uninterrupted string, or can have structure. Atomicity is supported at the granularity of a single item – i.e., atomic read-write and atomic read-modify-write are likely to only individual items and no security is provided across objects.

Single Object Operations and stability: Once processes are limited to a single key, providing single object stability while ensuring scalability is good. If there is no object level duplication, all requests for an object appear at a single node that hosts the object. Even if the entire data set is division across multiple hosts, the single key nature of requests makes them limited to a single node. The system can now provide operations such as atomic reads, atomic writes, and atomic read-modify-write.

Duplication and stability:
Mainly modern systems need to support per object duplication for high availability, and in some cases to get better the performance by distributing the load amongst the copy. This complicates providing stability guarantees, as updates to an object need to be spread to the duplication as well. Different systems use different mechanism to synchronize the duplication thereby providing different levels of stability such as eventual stability, timeline stability and so on.

Accessibility:
Conventional distributed databases considered the entire data as a consistent whole, and hence, non availability of a part of the data was deemed as non availability of the entire systems. But the single object semantics of the modern applications have allowed data to be less interrelated. As a result, modern systems can stand non availability of positive portions of data, while still providing logical service to the rest of the data. It must be noted that in conventional systems, the components were cohesively bound, and non accessibility of a single part of the system resulted in the entire system becoming unavailable. On the other hand, modern systems are insecurely coupled, and the non availability of certain portions of the system might not affect other parts of the system. For example, if a partition is not accessible, then that does not affect the accessibility of the rest of the systems, since all operations are single object. Thus, even though the system accessibility might be high, record level accessibility might be lower in the existence of failures.

CONCLUSION

In this paper, we have provided security to application which is stored on public cloud, by using security techniques such as Message Digest, Encryption, Decryption, Hash function. Thus i have successfully maintained the integrity, privacy and privacy of data stored on public cloud. Among the main reasons for the success of the cloud computing paradigm for usefulness computing are elasticity, pay as you go model of payment, and use of product hardware in a large scale to develop the economies of scale. So, the continued success of the model require the design of a scalable and flexible system that can provide data security and data management as a service in cloud computing.

REFERENCES

[1]. Veerraju Gampala, (2012), Data security in cloud computing with elliptic curve cryptography, International Journal of Soft Computing and Engineering(IJSCE), 2. | [2]. Zhifeng Xiao and Senior Member Yang Xiao, Security and privacy in cloud computing, IEEE Communications Surveys and tutorials, 15. | [3]. Lori M. Kaufman John Harauz. Data security in the world of cloud computing. IEEE Computer and Reliability society. | [4]. Party Auditor Indrajit Rajput. Enhanced data security in cloud computing with third party auditor. International Journal of Advanced Research in Computer Science and Software Engineering, 3. | [5]. O. B. Akan and I. F. Akyildizis,"Event-to-sink consistent transport in wireless sensor networks", IEEE/ACM Trans. Network., vol.13,. 1003-1016, Oct. 2005. | [6]. Jens-Matthias Bohli, (July/August 2013), Security and privacy-enhancing multicloud architectures, IEEE transactions on dependable and secure computing,10. | [7]. Amit Sangroya, (July/August 2010), Towards analyzing data security risks in cloud computing environments. | [8]. Gu Yaqiang Zhang Quan Tang Chaojing Dai Yuefa, (November 21-22, 2009), Data security model for cloud computing