ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 2; Issue 6; Page No. 55-59

Analysis of Cloud Data Mining & Emergence of Self-Destructing Technique to Archive Data

Varugu Ramesh Babu, V.Rama Krishna

Associate Professor, Ananamacharya Institute of science & Technology.

Associate Professor, Ananamacharya Institute of science & Technology.

ABSTRACT

Cloud database Storage is a model of networked enterprise storage where data is stored in virtualized pools of storage which are generally hosted by vendors it may contains large data centers. The information like education notes and business deals documents that could be misused by hacker's unauthorized users. These data copied and archived by cloud storage service often with users and control using self-destructing. Self-destructing protecting the user data in secure way all the data and their copies become destructed or unreadable after a user specified time without any user intervention. This works presents the self-destructing survey interact with cryptography technique with active storage meets the privacy concerns. The functionality compares the earlier self-destructing with our proposed analysis shamir secret sharing algorithmis efficient not used in any earlier data mechanism.

Keywords: Destructing, Cloud Service Provider, Storage device, Cloud databases.

INTRODUCTION:

Database management systems are an integral and indispensable component in most computing organizations today with the advent of hosted cloud computing and storage. Cloud computing is the evolution of internet based computing provided a common infrastructure for applications static web pages began to add interactivity hosted applications like Hotmail more user configuration renamed software as a service. With a growing number of companies looking to get on the software as a service opportunity Amazon released web services that enable companies to operate their own software as a service applications. Cloud database usage patterns are evolving and business adoption of these technologies accelerates that evolution cloud databases serviced consumer applications these early applications put a priority on read access because the ratio of reads to writes was very high. Consumer centric cloud database applications have been evolving with the adoption of web 2.0 technologies user generated content particularly in the form of social networking for example consumer centric cosmetics website if the user does a search for a certain shade of makeup powder it is important that the results be delivered instantaneously to keep the user engaged so she does not click on another cosmetics site. If the site said that the chosen makeup powder is in inventory and completed the sale it would not be the end of the world to later find out that a result of inconsistent data that makeup powder was not really in inventory.Cloud database is a database that consists of cloud computing like Google Microsoft Salesforce Rackspace Amazon etc, cloud database management system are designed to satisfy applications such as availability of a service Data confidentiality flexible query interface. Cloud architecture consists of layers Manageability layer deals with managing various users keeps the record of the time a particular user uses the cloud database.

Security layer provides user authentication mechanism with the help of users' id and passwords should be accepted as being legal one.

Transparency provides transparences to the users of cloud database where it means that the physical of data is not known to the users various types of real time applications easier.

Conceptual is heterogeneity among different databases like SQL DB2 Oracle a logical structure of the entire database deals with the internal processing on data as cloud deals with various types of data here users need to combine the traditional data with the data that are placed on the cloud so various types of systems are required for cloud database that provides all functions.

Interoperability means operate irrespective of their underlying databases for example if customer A wants to share data with another customer with B they are able to share the data irrespective of their underlying different databases of different vendors with the help of this layer.

Cloud computing as a utility that has recently attracted significant features people used terminals to connect to powerful mainframes shared by many users, the standalone personal computers became powerful enough to satisfy users daily work and computer networks allowed multiple computers to connect to each other, the cloud computing allows the exploitation of all available resources on the internet in a scalable way.

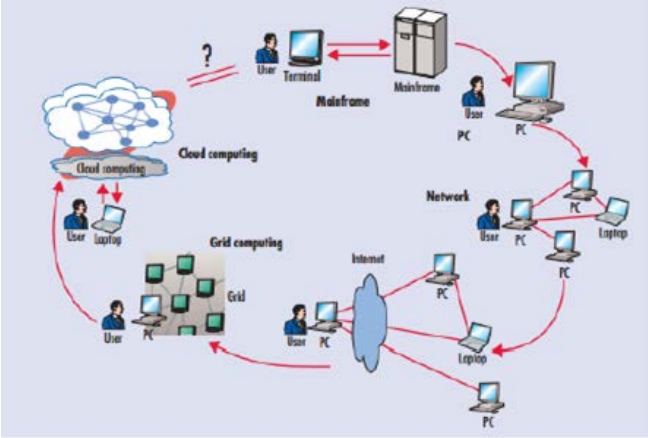

Figure 1: shows the Cloud Storage Environment

Cloud computing is amodel for enabling ubiquitous convenient on demand network access to shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or serive provider interaction. Data mining represents finding useful patterns or trends through large amounts of data defined as atype of database useful patterns or relationships in a group of data uses advanced statistical methods such as cluster analysis and sometimes employs artificial intelligence or neural networks. Data miningthe extraction of hidden predictive information from large databases is a powerful with great potential to help companies focus on the most important information in their datawarehouse. Cloud computing denotes the new trend in internet services that rely on clouds of servers to handledtasks.

SECTION II

Related Work: When use the system as detection might become complex study of new idea for sharing and protecting privacy system a secret key is divided and stored in a point to point system with distributed hash tables. With joining and exiting of the point to point node the system can maintain secret keys according to characteristics of point to point the distributed has table will refresh every node after every certain hours with secret sharing algorithm when will not get enough parts of a key the person will no decrypt data encrypted with this key means that key is destroyed and the data cannot be recovered some attacks to characteristics of point topoint are challenges of system uncontrolled in how long the key can survive. System used for creating message that automatically self-destruct after certain period of time which integrates cryptographic techniques with global scale point to point distributed hash tables. Distributed hash table have the property to discard data older than a certain age. In this the key permanently lost and the encrypted data is system each message is encrypted with a random key and storing share of the key in a large public distributed hash tables.

Self-destructive system defines two new modules associated with each secret key part and each secret key part has its own survival time parameter. In the self-destructive system can meet the requirements of self-destructing data with controllable survival time while users can use this system as a general object storage system. Apply some load balancing and round trip algorithms an active storage object derives from a user object and has a time to live value property which used to trigger the self-destruct operation. The time to live value of a user object has the property infinite so the user object will not be deleted until a user deletes it manually on the other hand the time to live value of an active storage object is limited so an active object will be deleted when the value of the associated policy object is true. Secure delete sensitive data and reduce the negative impact of performance due to deleting operation the required secure deletion of all the files is not great so if these parts of the file update operation changes.Self-destruction data is implemented by encrypting data with a key and that information is needed to reconstruct the decryption key with many parties local data destruction approach will not work in the cloud storage because the number of backups or archives of the data that is stored in the cloud is unknown and some nodes preserving the backup data have been offline. System creating messages that automatically self-destruct after a period of time it gets integrates cryptographic techniques with global scale peer-to-peer distribution has table.

SECTION III

3.Number of network intrusions have been found till now, each of which utilizes one or more security vulnerabilities in TCP/IP protocol specifications. These intrusions include IP source address spoofing, TCP sequence number prediction as mentioned earlier and other intrusions like SYN flooding, DNS misuse, Ping of Death, or some Java-related attacks. However, based on the intrusion patterns and impacts to the victim systems,

intrusions into two main categories: denial of service and spoofing.The lifeblood of today's world is information. The denial-of-service intrusions attempt to prevent or delay access to the information or the information processing systems. The basic idea behind this type of intrusion is to tie up a service provider with bogus requests in order to render it unreliable or unusable.

Network –based intrusion detection system[NIDS**]**][6] that tries to detect malicious activity such as denial of service attacks, port scan or even attempts to crack into computer by monitoring network traffic. NIDS does this by reading all incoming packets and trying to find number of TCP connection requests to a very large number of different ports is observed, one could assume that there is someone conducting a port scan of some or all of the computers in the network. It mostly tries to detect incoming shell codes in the same manner that an ordinary intrusion detection system does. Often inspecting valuable information about an ongoing intrusion can be learned from outgoing or local traffic and also work with other systems as well, for example update some firewalls blacklist with the IP address of computers used by suspected crackers.

Host-based intrusion detection system [HIDS] [4] monitors parts of the dynamic behavior and the state of computer system, dynamically inspects the network packets. A HIDS could also check that appropriate regions of memory have not been modified, for example- the system-call table comes to mind for Linux and various v table structures in Microsoft windows. For each object in question usually remember its attributes (permissions, size, modifications dates) and create a checksum of some kind (an MD5, SHA1 hash or similar) for the contents, if any, this information gets stored in a secure database for later comparison (checksum-database). At installation time- whenever any of the monitored objects change legitimately- a HIDS must initialize its checksum-database by scanning the relevant objects. Persons in charge of computer security need to control this process tightly in order to prevent intruders making un-authorized changes to the database.

Protocol-based intrusion detection system [PIDS][4] typically installed on a web server, monitor the dynamic behavior and state of the protocol, typically consists of system or agent that would sit at the front end of a server, monitoring the HTTP protocol stream. Because it understands the HTTP protocol relative to the web server/system it is trying to protect it can offer greater protection than less in-depth techniques such as filtering by IP address or port number alone, however this greater protection comes at the cost of increased computing on the web server and analyzing the communication between a connected device and the system it is protecting.

Application protocol based intrusion detection system [APIDS][4] will monitor the dynamic behavior and state of the protocol and typically consists of a system

or agent that would sit between a process, or group of servers, monitoring and analyzing the application protocol between two connected devices.

SECTION IV

4. Problem Definition: Computer networkis a system that we can perform development, software applications, used to transfer data packets,unauthorized attacks intrusion detection became the anomaly, installation of antivirus protection software the system became more complex, to avoid all these detection and protection over the computer applications data packets will not provide secure for our data. Cloud storage service is technique that provides destructing when the application of development is to be done.Use of destructing is information available in the cloud could not miscreant or court law these data is cached copied and archived by cloud service providers often without user's authorization and control. If we retrieve at any time all the data and their copies become destructed or unreadable after a user specified time without any user intervention.

Computer Operating system kernel code as code that to be executing a service method should be implemented in user space with libraries functions is used by code in user specific functions. Tools to develop software system in user space much safe to debug code in user spam than in kernel space. The method process takes long time a complicated task so implementing code of a method in user space have advantage of performance of the system. The system might crash with an error in kernel code but if error occurs in code of user space self-destruct method object is a method with arguments which specifies the device object to be destructed.

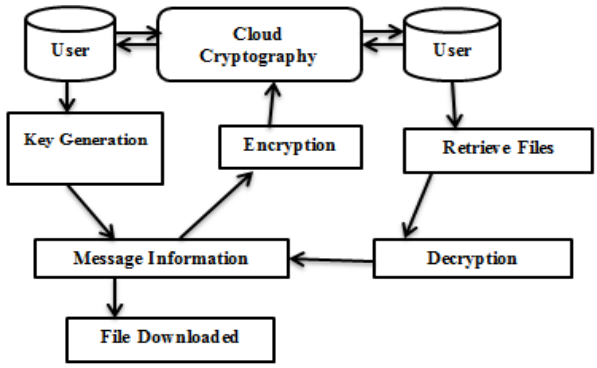

Figure :2 De-structing cloud Storage

SECTION V

5.1. Shamir algorithm: Secret sharing is a method in cryptography for distributing a secret among a group of participants each of which is allocated to share a secret. Secret can only be reconstructed when the shares are combined together or individual share are of use on their own. Sharing a secret gives control and removes single point vulnerability, independent share holder cannot change or access the data.

A goal is divide some of data for example D into n pieces D1, D2….Dn and a knowledge of any k or more D pieces makes D easily computable, knowledge of any k-1 or fewer pieces leaves D completely undetermined is called (k,n) threshold scheme if k=n then all participants are required together reconstruct the secret.

Suppose we want to use (k,n) threshold scheme to share our secret S where k<n at random (k-1) coefficients a1,a2,a3…ak-1 and let S be the a0.

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_{k-1}^{k-1}$$

Construct n points (I,f(i)) where i=1,2,..n

Given any subset of k of these pairs we can find the coefficients of the polynomial by interpolation and then evaluate a0=S, which is the secret.

5.2. Cloud Data Sharing &Storage Analysis: users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

Cloud Service Provider (CSP): a CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

Third Party Auditor (TPA): an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

5.2.1. File Retrieval and Error Recovery

Since our layout of file matrix is systematic, the user can reconstruct the original file by downloading the data vectors from the first m servers, assuming that they return the correct response values. Notice that our verification scheme is based on random spot-checking, so the storage correctness assurance is a probabilistic one. We can guarantee the successful file retrieval with high probability. On the other hand, whenever the data corruption is detected, the comparison of pre-computed tokens and received response values can guarantee the identification of misbehaving server(s).

5.2.2. Third Party Auditing

In case the user does not have the time, feasibility or resources to perform the storage correctness verification, he can optionally delegate this task to an independent third party auditor, making the cloud storage publicly verifiable. However, as pointed out by the recent work, to securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy. Namely, TPA should not learn user's data content through the delegated data auditing.

5.2.3. Cloud Operations

Update Operation

In cloud data storage, sometimes the user may need to modify some data block(s) stored in the cloud, we refer this operation as data update. In other words, for all the unused tokens, the user needs to exclude every occurrence of the old data block and replace it with the new one.

Delete Operation

Sometimes, after being stored in the cloud, certain data blocks may need to be deleted. The delete operation we are considering is a general one, in which user replaces the data block with zero or some special reserved data symbol. From this point of view, the delete operation is actually a special case of the data update operation, where the original data blocks can be replaced with zeros or some predetermined special blocks.

Append Operation

In some cases, the user may want to increase the size of his stored data by adding blocks at the end of the data file, which we refer as data append. We anticipate that the most frequent append operation in cloud data storage is bulk append, in which the user needs to upload a large number of blocks (not a single block) at one time.

SECTION V

6. Comparative Study: Cloud storage services for a user to store data to avoid problem that can raised by the centralized trusted third party of self-destructing is to protect the user key and provide the functions of self-destructing data. The system contains clients and vendor party data storage and self-destructing. The process to store data has no change, cryptography is applied to upload and download data from cloud storage it mainly runs in kernel mode and it can mount a remote file system to local machine. The input full path of file key file and the life time for key parts system encrypts data and uploads encrypted data system prompts creating active object are successful afterwards and that means the uploading file gets completed. Personal data stored in the Cloud may contain account numbers, passwords, notes, and other important information that could be used and

misused by a miscreant, a competitor, or a court of law. These data are cached, copied, and archived by Cloud Service Providers (CSPs), often without users' authorization and control. Self-destructing data mainly aims at protecting the user data's privacy. All the data and their copies become destructed or unreadable after a user-specified time, without any user intervention. Besides, the decryption key is destructed after the user-specified time. These data are cached, copied, and archived by Cloud Service Providers (CSPs), often without users' authorization and control. Self-destructing data mainly aims at protecting the user data's privacy. All the data and their copies become destructed or unreadable after a user-specified time, without any user intervention. Besides, the decryption key is destructed after the user-specified time. we present Self-destructing, a system that meets this challenge through a novel integration of cryptographic techniques with active storage techniques based on T10 OSD standard. We implemented a proof-of-concept Self-destructing prototype. Through functionality and security properties evaluation of the Self-destructing prototype, the results demonstrate that Self-destructing is practical to use and meets all the privacy-preserving goals described above. Compared with the system without self-destructing data mechanism, throughput for uploading and downloading with the proposed Self-destructing acceptably decreases by less than 72%, while latency for upload/download operations with self-destructing data mechanism increases by less than 60%. Compared with the system without self-destructing data mechanism, throughput for uploading and downloading with the proposed Self-destructing acceptably decreases by less than 72%, while latency for upload/download operations with self-destructing data mechanism increases by less than 60%.

CONCLUSION VI

Data security has become increasingly important in the Cloud database. The analysis of paper presents new technique for protecting data privacy from unauthorized users who retroactively obtain, through legal or other means, a user's of cloud storage data and private decryption keys. Comparative study shows the fixed data timeout and large replication factor present challenges for a self-destruction data system.

REFERENCE:

1. Peter Mell, and Timothy Grance, "The NIST Definition of Cloud Computing", The National Institute of Standards and Technology, USA, 2011, Link: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
2. IT Strategists, "Top Cloud Computing Companies and Key Features", Link: http://www.itstrategists.com/Top-Cloud-Computing-Companies.aspx.
3. Merriam-Webster Dictionary, "Definition of data mining", Link: http://www.merriam-webster.com/dictionary/data%20mining.
4. C. Kruegel and G. Vigna, "Anomaly Detection of Web-Based Attacks," Proc. ACM Conf. Computer and Comm. Security, Oct. 2003.

	Ramesh Babu Varugu B.Tech Computer Science Engineering from LakkireddyBalreddy Engineering College M.Tech Information Technology from Gurunank Engineering College. Having eight years of experience in Academic currently working as Asst Prof in Annamacharya Institute of Science & Technology and guided many UG & PG students His research areas include Network Security, Data Mining, Cloud Computing.
	V.Rama Krishna B.Tech Computer Science engineering from Gulberga University M.Tech Computer Science Engineering from VT University Karnataka. Having twelve years of experience in Academic currently working as Assoc Prof in Ananamacharya Institute of science & Technology. He has guided many UG & PG student's interested subjects include Network Security, Data Mining, Cloud Computing.