IJDCST @Oct, Issue- V-2, I-7, SW-06
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Security Evaluation Using Shamir's Algorithm in Multi Cloud Data Storage

[1] ASHA PRIYA DARSHINI. MANDA, [2] N. JAGAJEEVAN

[1]Mtech, CHALAPATHI INSTITUE OF ENGINEERING AND TECHNOLOGY, CHALAPATHI NAGAR, LAM, GUNTUR, AP, INDIA.
[2]Assistant Professor, CHALAPATHI INSTITUE OF ENGINEERING AND TECHNOLOGY, CHALAPATHI NAGAR, LAM, GUNTUR, AP, INDIA.

Abstract: Guaranteeing the security of distributed computing is a main consideration in the distributed computing environment which has numerous profits as far as minimal effort and availability of information, as clients frequently store delicate data with distributed storage suppliers, uninformed that these suppliers may be traded off. Managing "single cloud" suppliers is anticipated to wind up less prominent with clients because of dangers of administration accessibility disappointment and the likelihood of noxious insiders in the single cloud. A development towards "multi-mists" or at the end of the day, "entomb mists "or" billow of-mists has risen as of late and a framework that utilizes Byzantine convention for mystery offering has been developed. We expect to prepare Depsky system to supply a protected cloud database that will certification to avert security dangers confronting the distributed computing group. In connection to information interruption and information trustworthiness, in the same way as depsky we convey the information and metadata into diverse cloud suppliers, and we apply the mystery offering calculation on the put away information in the cloud supplier. As opposed to utilizing plain mystery offering utilizing open key figures we utilize Shamir's mystery imparting calculation. Henceforth, reproducing information into multi-mists by utilizing a multi-offer method may diminish the danger of information interruption and build information uprightness. This work intends to advertise the utilization of multi-mists because of its capability to diminish security hazards that influence the distributed computing client.

Key Words: Cloud computing, single cloud, multi-clouds, dep sky architecture, Shamir's secret sharing algorithm.

I. INTRODUCTION

Distributed computing will be figuring that incorporates an extensive number of machines related through a correspondence system, for example, the Internet, like utility processing [4]. In science, distributed computing is an equivalent word for disseminated processing over a system, and means the capacity to run a project or application on numerous joined workstations in the meantime. System based administrations, which have all the earmarks of being conveyed by true server fittings and are indeed served up by virtual equipment mimicked by programming running on one or all the more genuine machines, is regularly called distributed computing. Such recreated servers don't

physically exist and can thusly be migrated around and scaled up or down on the fly without exasperating the end client, to some degree like a cloud getting to be bigger or more diminutive without being a physical item [3].

In as something to be shared use, the expression "the cloud" is in a broad sense a representation for the Internet [5]. Advertisers have further made famous the expression "in the cloud" to allude to programming, stages and framework that are sold "as an administration", i.e. remotely through the Internet. Regularly, the dealer has genuine vitality devouring servers which have items and administrations from a remote area, so end-clients don't need to; they can essentially log on to the system without introducing anything. The real models of distributed computing administration are referred to as programming as an administration, stage as an administration, and foundation as a service[3]. Distributed computing depends on imparting of assets to attain lucidness and economies of scale, like an utility (like the power network) over a network[6]. At the establishment of distributed computing is the more extensive idea of joined base and imparted administrations. The cloud likewise concentrates on amplifying the adequacy of the imparted assets. Cloud assets are typically imparted by different clients as well as progressively reallocated for every interest. This can work for apportioning assets to clients.

Security in distributed computing:

As distributed computing is attaining expanded prominence, concerns are continuously voiced about the security issues presented through selection of this new model.[4][7] The adequacy and proficiency of customary assurance systems are, no doubt rethought as the attributes of this creative arrangement model can contrast generally from those of conventional architectures.[8] An option viewpoint on the subject of cloud security is that this is however an alternate, in spite of the fact that truly wide, instance of "connected security" and that comparable security standards that apply in imparted multi-client centralized computer security models apply with cloud security[9].

Distributed computing offers numerous profits, yet is helpless against dangers. As distributed computing utilization expand, it is likely that more crooks find better approaches to endeavor framework vulnerabilities. Numerous underlying difficulties and dangers in distributed computing expand the danger of information trade off. To moderate the risk, distributed computing stakeholders ought to put intensely in danger appraisal to guarantee that the framework encodes to ensure information, secures trusted establishment to secure the stage and foundation, and incorporates higher affirmation with inspecting to fortify consistence. Security concerns must be tended to keep up trust in distributed computing engineering.

II. RELATED WORK

H. Abu-Libdeh [11] stated that The increasing popularity of cloud storage is leading organizations to consider moving data out of their own data centers and into the cloud. As it became very expensive to switch storage providers a case for applying RAID-like techniques used by disks and file systems, but at the cloud storage level reduce the cost

of switching providers, and better tolerate provider outages or failures. So we introduce RACS, to overcome the drawbacks in the existing system.

G. Ateniese[10] stated that introducing a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data And there will be a drastic change in I/O costs So, they presented two provably-secure PDP schemes that are more efficient than previous solutions.

H. Abu-Libdeh stated that by introducing HAIL a distributed cryptographic system that permits a set of servers to prove to a client that a stored file is intact and retrievable. So, author introduced a strong, formal adversarial model for HAIL, and rigorous analysis and parameter choices to overcome the drawbacks in the esisting system.

C. Cachin in his paper stated that there is a problem of efficient distributed storage of information in a message-passing environment where both less than one third of the servers, So to overcome these problem author introduced first implementation of non-skipping timestamps which provides optimal resilience and withstands Byzantine clients; it is based on threshold cryptography.

KuiRen Stated in his paper cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. So to overcome the drawbacks author used a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data.

III. EXISTING SYSTEM

Multi-Clouds: Preliminary

The term “multi-clouds” is similar to the terms “inter clouds” or “cloud-of-clouds”. These terms suggest that cloud computing should not end with a single cloud. Using their illustration, a cloudy sky incorporates different colors and shapes of clouds which lead to different implementations and administrative domains. Recent research has focused on the multi-cloud environment which control several clouds and avoids dependency on any one individual cloud. Identify two layers in the multi-cloud environment: the bottom layer is the inner-cloud, while the second layer is the inter-cloud. In the inter cloud, the Byzantine fault tolerance finds its place. We will first summarize the previous Byzantine protocols over the last three decades.

Byzantine Protocols

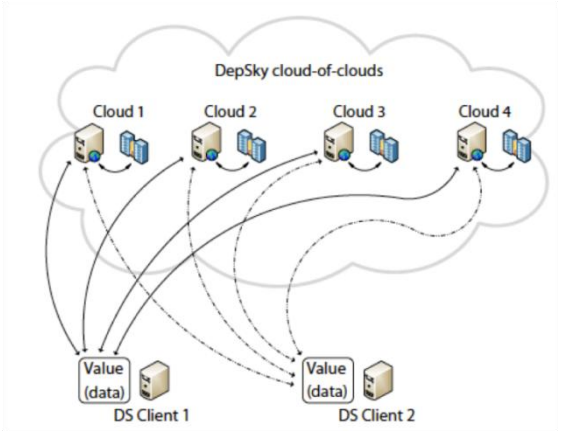
In cloud computing, any faults in software or hardware are known as Byzantine faults that usually relate to inappropriate behavior and intrusion tolerance. In addition, it also includes arbitrary and crash faults. Much research has been dedicated to Byzantine fault tolerance (BFT) since its first introduction. Although BFT research has received a great deal of attention, it still suffers from the limitations of practical adoption and remains peripheral in distributed systems **Multi-Clouds Model**

This will explain the recent work that has been done in the area of multi-clouds. Present a virtual storage cloud system called DepSky which consists of a combination of different clouds to build

a cloud-of-clouds. The DepSky system addresses the availability and the confidentiality of data in their storage system by using multi-cloud providers, combining Byzantine quorum system protocols, cryptographic secret sharing and erasure codes.

DepSky Architecture

The DepSky architecture consists of four clouds and each cloud uses its own particular interface. The DepSky algorithm exists in the clients' machines as a software library to communicate with each cloud. These four clouds are storage clouds, so there are no codes to be executed. The DepSky library permits reading and writing operations with the storage clouds.



Figure(1). DepSky Architecture

DepSky Data model: As the DepSky system deals with different cloud providers, the DepSky library deals with different cloud interface providers and consequently, the data format is accepted by each cloud. The DepSky data model consists of three abstraction levels: the conceptual data unit, a generic data unit, and the data unit implementation.

DepSKy System model: The DepSky system model contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client's tasks. Explain the difference between readers and writers for cloud storage. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behavior) whereas, writers only fail by crashing.

Cloud storage providers in the DepSky system model: The Byzantine protocols involve a set of storage clouds (n) where n = 3 f +1, and f is maximum number of clouds which could be faulty. In addition, any subset of (n – f) storage cloud creates byzantine quorum protocols.

IV. PROPOSED SYSTEM

Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of them are needed in order to reconstruct the secret.

Counting on all participants to combine together the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret.

Mathematical definition:

The goal is to divide secret S (e.g., a safe combination) into n pieces of data $D_1,\ldots\ldots,D_n$ in such a way that:

1. Knowledge of any k or more D_i pieces makes S easily computable.

2. Knowledge of any k-1 or fewer D_i pieces leaves S completely undetermined (in the sense that all its possible values are equally likely).

This scheme is called \left(k,n\right) threshold scheme. If k=n then all participants are required to reconstruct the secret.

Shamir's secret-sharing scheme:

The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes k\,\! points to define a polynomial of degree k-1.

Suppose we want to use a (k,n) threshold scheme to share our secret Swithout loss of generality assumed to be an element in a finite field F of size P where $0 < k \leq n < P$; S<P and P is a prime number.

Choose at random $k-1$ positive integers $a_1, \cdots, a_{k-1}$ with $a_i < P$, and let $a_0 = S$. Build the polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}$. Let us construct any n points out of it, for instance set $i = 1, \cdots, n$ to retrieve $(i, f(i))$. Every participant is given a point (an integer input to the polynomial, and the corresponding integer output). Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term a_0.

One Time Password:

One Time Password (OTP) authentication is a method to reduce the potential for compromised user credentials. The concept behind OTP is that every session initiated by a user generates a unique user credential that is only valid for that session or for a very short period of time. Even if an attacker is capable of obtaining this user credential, it may either no longer be valid or be prohibited from additional use[12].

Security of one-time-password protocols:

The main security property that protocols employing one-time passwords should achieve is: strong mutual authentication based on knowledge of one-time passwords. Our work will address one-time passwords in the context of PAKE protocols, which provide an additional property: secure key exchange.

The motivation for using one-time passwords is that the compromise of one password should not affect the security of sessions involving another password. The one-time password serves to mutually authenticate the client and the server; there are no other long-term values like public keys or certificates. Authentication is based on knowledge of the shared password. Informally, a protocol will provide secure mutual authentication if no honest party A^ accepts a session as being with party B^ unless B^ participated in the protocol, and vice versa. We want a one-time-password protocol to give secure mutual authentication for the current session even if other one-time passwords have been revealed [12].

In addition to mutually authenticating two parties to each other, we want a protocol that will also output a session key that can be used to encrypt

and protect the integrity of future communications between those two parties. This is a common feature required of many secure communication protocols. The traditional use of one-time passwords – sending the password over an SSL connection – is not compatible with our approach. Using SSL to establish an authentic channel requires that the user can obtain and properly use an authentic public key for the server. In other words, it requires a public key infrastructure, whereas one-time-PAKE only needs shared passwords.

V. EXPERIMENTAL SETUP

We describe above features of Shamir secret sharing schema for accessing services in individual modularity. In this achievement accessing services from other user present in network process environment data event generation. For doing this work efficiently in this paper we propose to develop an efficient application like software project management development in real time application using some specified technical languages present in the real time process management event generation. In this cross of cloud application, this is the event management process between each client present in the real time application of all the data sharing network process management applications. Due to this achievement in cloud computing information sharing is the main aspect in commercial event management reorganization in data event management applications. To address this achievement in each client in software application development process for real time application development every client must satisfy the following conditions in commercial event management. In that we are maintain three different aspects for sharing data from one to client other client clients in network application environment.

As discussed in the earlier version of semantic data representation. We have to develop Software Project management application for processing efficient services with different infrastructures. In this requirement specification we have to provide efficient service in real time application process between cloud storage system applications with other features present in the relative data assessment technique feature environment specification. These features are accessed relative data event management for accessing services in real time application development.

VI. PERFORMANCE RESULTS

As discussed in above section V, the overall information gives efficient achievement between developed cloud environment specifications in software development application processing. In this paper we develop a specialized requirement of the all the relative client request. Each client registered with his login credentials like username and password specification with relative data management specification from storage cloud and firm cloud with relative data management for accessing services from relative data management of each client present in the cloud environment specification. Storage cloud provide efficient services for registering with suitable credentials or not. If we register then achieve all the relative services in cloud environment, firm cloud give relative services to each client registered in cloud then take the assessment technique for accessing services in real time application development specifications. All the commercial

cooperation between each data event progression then we provide security to client if all the relative services. Then each client achieves the relative data process between each cloud with suitable credential in event management for accessing services in cloud computing. Data storage cloud operations are accessed services in real time application management for accessing client services from firm cloud and assessment cloud operations with semantic data event management progression in real time cloud application with secret sharing client details in relative data management between client operations using the services of all the services in cloud computing operations between each client.

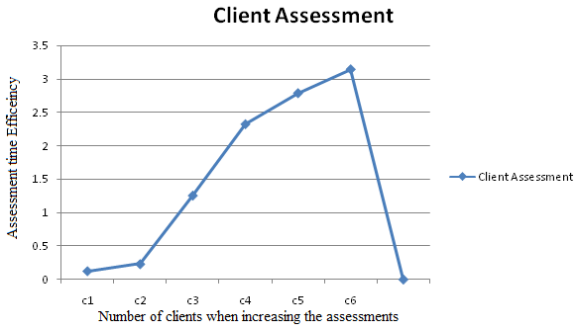


Figure 2: Performance calculation of each client in cloud data sharing.

As discussed in the above section i.e, section V,VI, there is relative data management with cloud sharing operations between cloud data storage and other cloud data storage with firm cloud. In that we are maintaining one time password for each client data processor in cloud computing. Our experimental results show efficient data processing in storage cloud and firm cloud processing with required results.

VII. CONCLUSION

We aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity. In relation to data intrusion and data integrity, like depsky we distribute the data and metadata into different cloud providers, and we apply the secret sharing algorithm on the stored data in the cloud provider. Instead of using plain secret sharing using public key ciphers we employ Shamir's secret sharing algorithm. An intruder needs to retrieve at least three values to be able to find out the real value that we want to hide from the intruder. This depends on Shamir's secret sharing algorithm with a polynomial function technique which claims that even with full knowledge of (k – 1) clouds, the service provider will not have any knowledge of vs (vs is the secret value).

In other words, hackers need to retrieve all the information from the cloud providers to know the real value of the data in the cloud. Therefore, if the attacker hacked one cloud provider's password or even two cloud provider's passwords, they still need to hack the third cloud provider (in the case where k = 3) to know the secret which is the worst case scenario. Hence, replicating data into multi-clouds by using a multi-share technique may reduce the risk of data intrusion and increase data integrity.

VIII. REFERENCES

[1]. Cloud Computing Security: From Single to Multi-Clouds by Mohammed A. AlZain, Eric Pardede , Ben Soh , James A. Thom.

[2].Shamir's secret sharing from Wikipedia.

[3]. Cloud computing from wimkipedia.

[4]. Securing Virtual and Cloud Environments".By I. Ivanov et al..

[5]. Cloud Computing entry".By NetLingo.

[6]. The NIST Definition of Cloud Computing".By National Institute of Standards and Technology.

[7].Secure virtualization: benefits, risks and constraints, by M Carroll, P Kotzé, Alta van der Merwe (2011).

[8] "Addressing cloud computing security issues". By Zissis, Dimitrios; Lekkas (2010).

[9]. Securing the Cloud: Cloud Computer Security Techniques and Tactics by Waltham.

[10]. "Provable datapossession at untrusted stores", by G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson and D. Song.

[11]. "RACS: a case for cloud storagediversity", byH. Abu-Libdeh, L. Princehouse and H.Weatherspoon.

[12]. One Time Password Authentication for Open High Performance Computing Environments by Stephen Chan, Stephen Lau slau, Adrian Wong.