ISSN:2348-2079

Volume-7 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Techniques for securing the data in cloud computing

Dr.P.Thirumoorthy[1], R.Gowsalya[2], P.Sabarishamalathi[3]

[1] Associate Professor, CSE, Nandha Engineering College

[2-3]PG Scholar CSE, Nandha Engineering College

ABSTRACT

Cloud computing is envisioned because the next generation technology. it's an online primarily based technology wherever quality services are provided to users together with information and code, on remote servers .Cloud computing is additionally referred to as information outsourcing as a 3rd party provides storage services to user. this is often a lot of price effective for the user as there's no want of buying valuable hardware and code for information storage. Before information out sourcing will become potential, the info supplier has to guarantee that the data is secure, be able to build transactions, and therefore the transactions should even be secure and not visible to the info supplier. during this paper, we are going to discuss current techniques for securing client's information on remote cloud server.

Keywords: Data Security, Cloud, Integrity, Confidentiality, Outsourcing.

INTRODUCTION

Cloud computing denotes a serious modification in however we tend to store data and run applications. Currently rather than running programs and information on a personal microcomputer, everything is hosted within the "cloud"—a shared pool of computers and servers accessed via the web. Cloud computing provides the ability to access all the documents and application from anyplace within the world and permits multiple cluster members to collaborate from totally different locations. one amongst the most important feature of cloud computing that is wide used is information storage capability. many free and reliable on-line storage services offered to the users are Microsoft SkyDrive, Apple iCloud ,Google Drive, Amazon S3, Dropbox and Gspace. As we tend to get to understand numerous blessings of cloud computing however everything has some execs ANd cons each and cloud computing isn't an exception. There are some doubts in users mind before moving towards cloud computing.

As the use of cloud computing becomes widespread, security of the outsourced user information becomes a crucial analysis topic.

The parameters that are taken into thought for information security are Confidentiality, Integrity, and accessibility. the matter of outsourcing information faces the subsequent obstacles:

Confidentiality:- will we tend to trust some third party and share our personal information with them? will our data stay subject to the local rules and regulations. Some of the countries allowed the seller to access the user's knowledge in step with their rules and Regulation. below such circumstances it becomes crucial for the user to confirm the protection of their data before swing the info over cloud.

Availability:-Does the info that we've got hold on on cloud would be on the market whenever we have a tendency to needed it i.e. handiness of information. once user is absolutely relied on knowledge hold on at cloud storage, it becomes essential that it might be simply accessed.

Integrity:- the info outsourcing party should offer guarantee to the user that the data that they

Author for correspondence:
CSE, Nandha Engineering College

need hold on on cloud wouldn't be changed or altered by any unauthorized user.

These are some doubts that are available the mind of each user or organization United Nations agency desires to modify to cloud computing. during this paper, we'll discuss some techniques used for providing security of information storage in cloud computing.

LITERATURE REVIEW

Many of the researches are done until to this point within which totally different security techniques have been mentioned.

In [1], a knowledge protection model was planned wherever data is encrypted mistreatment Advanced cryptography commonplace (AES) before launching within the cloud, that ensured information security. encoding is historically wont to give confidentiality whereas outsourcing information to cloud service supplier. Hacigumus et al. [2] discusses a technique for capital punishment queries over encrypted information, at the cloud service provider's website and suggests cacophonic a question into 2 components, particularly the server question and consumer query. The server question is dead over the encrypted information at the service supplier aspect and therefore the different half over the results of server query, at the consumer aspect.

Hore et al. [3] describes techniques for building privacy conserving indices on sensitive attributes of a relative table, ANd provides an economical resolution for information bucketization.

Agrawal et al.[4] highlights the advantages of mistreatment the order conserving cryptography scheme(OPES) for querying numeric information. Agrawal et al.[4] highlights the advantages of exploitation the order protective cryptography scheme(OPES) for querying numeric information.

Private info Retrieval (PIR) was initial mentioned in [5]. PIR protocol hides the queries performed by the user on a public information, keep on a group of servers. The PIR protocol provides the privacy of user queries that tends to cover the user's intensions from the service supplier.

After that a brand new protocol parallel personal info Retrieval (SPIR) has been developed. Its main concern was the privacy of user information.

One of the foremost wide used techniques for information outsourcing is Secret Sharing techniques. Shamir's Secret sharing [6] technique and Rabin's info dispersion [7] algorithmic rule (IDA).III.

DISCUSSIONS

Problem statement

Two main challenges of cloud computing are security and dependability. purchasers wants guarantee that their information that is keep on cloud won't be accessed by alternative clients. To attain security on cloud there are such a big amount of techniques and algorithmic rule offered. a number of these techniques are:

Encryption: during this technique advanced algorithmic rule are wont to hide the initial data with the assistance of encoding key. the info is reborn into undecipherable type referred to as cipher text then keep on remote server storage.

Authentication methodes: during this process, a login mechanism is employed to verify that the sole echt user is accessing the cloud information. It needs making a user name and secret.

Authorization practices: a listing of approved consumer is employed to spot, WHO will access information keep on cloud system.

However, many of us still worry that information saved on a far off storage system may well be accessed by alternative purchasers and that they can alter it. . Hackers may conjointly try and steal the physical machines on that information are keep. associate worker from cloud service supplier may alter or destroy information mistreatment his or her echt user name and secret. rather than of these risks, purchasers are adopting cloud computing wide. Cloud storage corporations are investment plenty of cash to create positive that their purchasers information would be safe. they're attempting to limit the chance of information thieving or corruption.

We are discussing some techniques here that are serving to the way to get security on cloud storage and for various purchasers by reading the various analysis paper. during this article we

glance at the trustworthy Platform Module (TPM). TPM provides Proof for retrieving written serializability, and freshness in clouds.

A TRUSTED STORAGE SYSTEM FOR THE CLOUD

"A sure Storage System "store the info further because it wants confidential storing also and maintain the integrity of the data. To achieve confidentiality and integrity of the info, cryptanalytic techniques are often wont to cipher information To cipher the client's information at intervals the cloud, Encrypted file systems (EFS) is employed .In EFS user's information is encrypted with the assistance of cryptography key that modified the initial data into cipher text which is undecipherable for different users. It develops the Integrity of the info at intervals the cloud. 5 protocols are developed that make sure that the client's information is hold on solely on sure storage servers, information is traced solely on sure storage servers, and guarantee that the info house owners and different privileged users of that data access the data firmly. The system is predicated on sure computing platform technology [8].

Encrypted File Systems

EFS (Encrypted File System) meant for encrypting keep files. Secret writing procedures occur at the classification system level not at the applying level. Secret writing is clear to the user. Scientific discipline techniques are used for secret writing; thus user doesn't have to manage keys in encryption. Below diagram shows the method of secret writing victimization EFS:

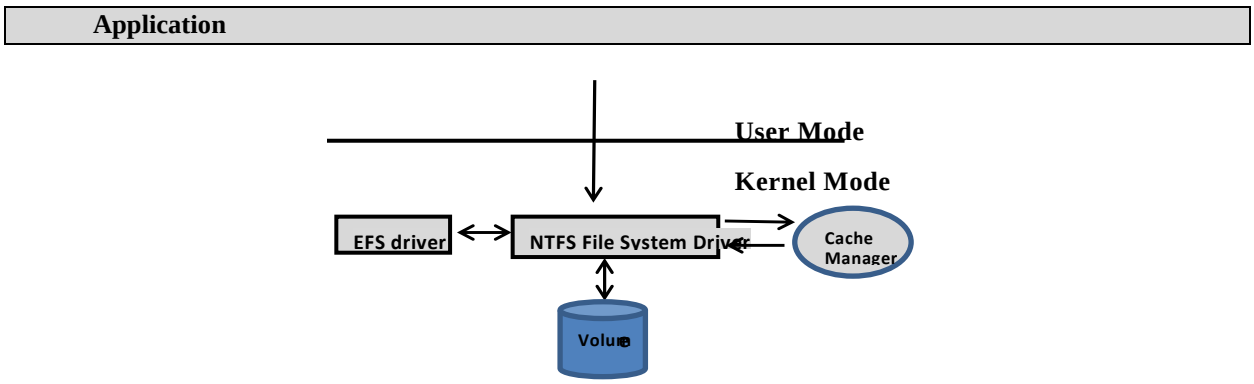

Figure 1: Example of flow of an encryption process in an Encrypting File system

process explanatory steps are as follows.

- Application writes data to an encrypted file
  2. NTFS places data in file system cache.
- Cache manager writes data to disk via NTFS.
- NTFS ask EFS driver to encrypt file contents headed to disk.
- NTFS writes encrypted file contents to disk.

Trusted Platform Module

What is a TPM?

The trusty Platform Module (TPM) could be a laptop microchip or a microcontroller that performs varied task associated with security and cryptography. This technology provides the tools to demonstrate the pc platform. The tools or objects will embody certificates, cryptography keys, passwords, and integrity metrics of a platform. The TPM may be employed in the method of remote attestation of a platform of a machine which is able to be mentioned any later. The chip is put in on the motherboard of a laptop. The TPM communicates with the remainder of the system by employing a hardware bus. The TPM implementation of that specification as a chip. The specification is provided by the trusty Computing cluster Result of trusty Storage system: TPM model offer security for system body level. however there's no resolution for individual users as a result of cloud is maintained by third party on

network. By mistreatment this projected system, administration are able to do confidentiality and integrity of the info hold on solely on trusty storage server

Ensuring data storage security in cloud computing with effect of kerberos

This technology guarantee cloud storage security with the assistance of Kerberos authentication service. that's by implementing the Kerberos; storage security would be achieved for users. Kerberos is outlined for making the price ticket and granting ticket for every user. This technology focuses a lot of on user to supply higher security. [9].

Kerberos operation erberos uses the technique of robust cryptography methodology and sophisticated price tag granting algorithmic rule [9] so user may be documented on network. During this a session key's used which permit encrypted information stream over AN scientific discipline network for every user. If new user needs to use the cloud then he must build profile on network by providing the data. once registering with Kerberos, the user will get his user ID and arcanum which can additionally store on server info. Each user should follow following steps for mistreatment cloud data:

- go surfing to system by mistreatment user ID and arcanum.
- User can send the request for price ticket granting ticket to the Authentication Server.
- Authentication server verifies user's document in database; produce the price ticket and session key. Results are encrypted mistreatment key derived from user arcanum.
- User can send the request cloud service granting price ticket to price ticket Granting server.
- TGS can send the price ticket and session key to the user.
- digital computer sends price ticket and appraiser to cloud server supplier.
- Server verifies price ticket and appraiser match, if verified, then grant access to service.

ENABLING SECURITY IN CLOUD STORAGE SLAS WITH CLOUD PROOF

One more technique for cloud storage security is predicated on "Enabling Security in Cloud Storage SLAs with Cloud Proof". This presents a secure storage system specifically designed for cloud, named as Cloud proof. In cloud proof customers will find if the integrity of information is profaned, violation of write-serializability, and freshness. They will conjointly prove these violations to a 3rd party [13].

System Overview of cloud proof: Cloud Proof has the subsequent four goals. Goal 1: Customers ought to apprehend if service supplier has desecrated the integrity of knowledge, freshness, and writeserializability. User's information should be confidential from outsiders. It are often achieved by encrypting the info they store on the cloud.

Goal 2: Customers ought to be ready to prove cloud violations whenever they happen.

Goal 3: Cloud Proof ought to offer scan and write access management in a very scalable manner. Since we have a tendency to are handling enterprise sizes, there is also thousands of users, several teams, and terabytes of knowledge. we wish to get rid of data house owners from the info access path the maximum amount as doable for performance reasons. house owners ought to be ready to believe (in a verifiable way) on the cloud for key distribution and access management, that could be a extremely difficult task.

Goal 4: Cloud Proof ought to maintain the performance, quantifiability, and accessibility of cloud services despite adding security.

The overhead ought to be acceptable compared to the cloud service while not security, and concurrency ought to be maintained.

The system ought to scale to massive amounts of knowledge, several users per cluster, since this is often demanded by massive enterprise information homeowners.

CONCLUSION

In this discussion we have a tendency to found varied techniques give the safety for information

keep on cloud. during this paper we have a tendency to demonstrate however we will win confidentiality and integrity security by mistreatment EFS and TPM techniques. Kerberos proofs the authentication of users on network. SLAs with Cloud Proof build confidentiality, integrity, writeserializability and browse freshness (denoted by C, I, W, F). Providing privacy to client and his information on cloud is incredibly advanced and price effective system however it is achieved by completely different technologies we've got mentioned during this paper.

REFERENCES

[1]. Abha Sachdev, Mohit Bhansali "Enhancing cloud computing security using AES Algorithm" International Journal of Computer Applications (0975-8887) 67(9), 2013.

[2]. H. Hacigumus, B.R.Iyer, C.Li and S. Mehrotra, "Executing SQL over encrypted data in the database service provider model," in proc of the ACM SIGMOD Conf., 2002.

[3]. B.Hore, S.Mehrotra, and G.Tsudik," A privacy preserving index for range queries,"in Proc. Of the VLDB Conf., 2004, 720-731.

[4]. R.Agrawal, J.kiernan, R.Srikant, and Y.Xu,"Order preserving index for range queries," in Proc. Of the ACM SIGMOD Conf., 2004, 563-574.

[5]. Chor, B. Goldreich, O., Kushilevitz, E., Sudan, M.:Private information retrieval In: Journal of the ACM, 45(6), 1998, 965-982.

[6]. Shamir,A.: How to share a secret. In: Commun. ACM, 22(11), 1979, 612-613.

[7]. Rabin,M.O.: Efficient dispersal of information for security, load balancing, and fault tolerance. In: journal of the ACM 36(2), 1989, 335-348.

[8]. http://www.tar.hu/wininternals/ch12lev1sec8.html

[9]. Mehdi Hojabri,' Ensuring data storage security in cloud computing with effect of Kerberos', 1(5), 2012, ISSN: 2278- 01 81.

[10]. Raluca Ada Popa, Jacob R.Lorch, David Molnar, Helen.J.Wang,Li .Jhuang :Enabling Security in Cloud Storage SLAs with cloudProof.