ISSN 2278-8808 SJIF 2014 = 4.889
An International Peer Reviewed & Referred
SCHOLARLY RESEARCH JOURNAL
FOR INTERDISCIPLINARY STUDIES

INTRUSION DETECTION SYSTEM ON MULTI-CLOUD COMPUTING

Gaurav Katte[1], Mayur Kudale[2], Priyanka Gire[3]& Shantam Padyachi[4]

Dept. Of Computer, NESGOI, Pune, Maharashtra, India

Abstract

Remote data checking is of crucial importance in Multicloud storage. It enables the users to their required data without downloading the whole data. The existing remote data possession integrity checking (ID-DPDP) protocols have been designed in the PKI (public key infrastructure) model. The multi-cloud server has to validate the users' certificates before save the data uploaded by the clients in order to prevent attack. Distributed Denial of Service (DDOS) RTOL and normal attack are the major security issue that poses a great threat to the availability of the multi cloud services. We propose an intrusion detection system with ID-DPDP strategy that help identify the data leakage or attacks .Data Leakage is main problem in our Multicloud server, we can apply data leakage algorithm for data leakage detection and prevention from the intruder ,RSA algorithm for cryptography and Hashing index.

Keywords: *Integrity checking, multicolor computing, ID-DPDP cryptography, network intrusion Data leakage detection.*

Introduction

Data integrity checking basically means protection of data from unauthorized users or hackers and providing high security to prevent data intrusion. In order to improve the security features in multi-cloud storage for data transfers, many techniques have been developed like: provable data possession Cryptography. Cloud computing is a technology of computing as a utility where client or user can remotely store their data and access into the cloud so as to enjoy high quality applications and services from a shared pool of Multi-cloud computing resources. Unauthorized network access to multi-cloud sever. A multi-cloud user needs a client device to access a cloud services over the internet. Normally the user will log into the cloud at a public service provider or private company, such as their employer. The multi-cloud provides server-dependent applications and whole data services to the user, access the client device. The client system's web browser is used to make the services data appear on the client system, but all

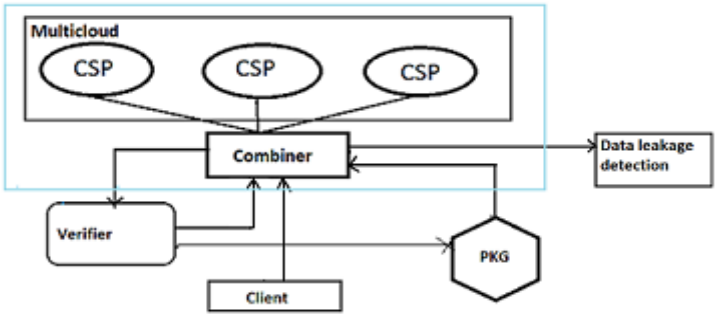
computations and changes are made by the multi cloud- server, and finally including files created or altered are permanently stored on the multi-cloud Servers.

Performance of the cloud application is based on the network access, speed, integrity and reliability as well as performance of the client

Device. Cloud Computing makes brings new and challenging security threats towards user's data on Multicloud server.ID- DPDP is such a technique for a storage provider to prove the integrity of clients' data without downloading whole data.

Problem Statement: Privacy detection or preservation and data integrity are the two main issues faced by single cloud service providers, when client stores or save his whole data on multi-cloud servers, the distributed storage and integrity checking are at risk .Distributed server model of cloud makes it critical and prone to distributed intrusion attacks like Distributed Denial of Service (DDOS), data leakage prevention is a major problem.

Architectural Design:



1) Client: an entity, which has whole amount data to be stored on the multi-cloud for maintenance and computation, can be Individual Corporation.

2) Cloud Server (CS): an entity, which is managed by cloud service provider, has whole amount storage space to maintain the clients' data.

3) Combiner: it is a flow entity which receives the storage request and passed or distributes the block-tag pairs to the corresponding cloud servers. When receiving the request, it distributes the challenge and split them to the different cloud servers. When receiving the request from themuliti- cloud servers, it collect them and sends the combined response to the verifier.

4) Private Key Generator (PKG): it is also an entity, when receiving the data, it outputs the corresponding private key.

Modules:

Modules in the System

1. Data owner
2. Proxy server
3. Receiver
4. Data Storage System

1) Data Owner

In this modules first the new data owner registers and get a valid login credentials. After logged in, the data owner has the authority to upload their data or file into the Cloud Server. The data owner encrypts his data and outside supplier the cipher texts to the proxy servers.

2) Proxy Server

In Proxy servers store the encrypted data which is forward the secret text from the owner to the recipient when they obtain access permission from the owner.

In these proxy servers are accept to be trusted. They authenticate receivers and validate access permissions

3) Receiver

The receiver certify himself to the owner and decrypts the re-encrypted Cipher text to obtain the data.

An end to-end surety is provided by cryptographic protocols which are executed by the file owner to prevent proxy servers and illegal users from reorganize and accessing the sensitive files. These systems can be splits two types: shared file system and non-shared file system.

4) Data Storage System:

The data storage system permits user to save their data to external proxy servers to enhance the access and availability the reduce preserve cost. The data storage scheme are classified into 3 kinds:

1. Network file system
2. Storage base intrusion detection system
3. Cryptographic file system

Result

This section describes the technologies used for developing the system which protect Sqlinjection attack, data leakage detection etc. self-made cloud is used to store data That data get protected from attacker. Our project result is all about the solution which was not solved in previous paper. So following point shows the one by one results.

1. Data leakage detection happens and stop data leakage.

2. Sql injection attack can be detected.
3. No expensive software are needed - It runs entirely on web browser.

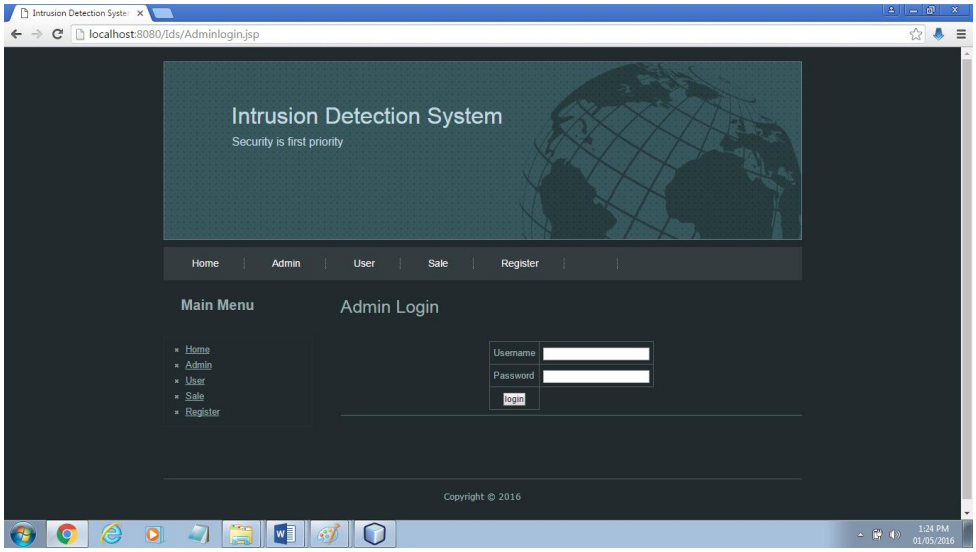


Fig .System Conclusion:

Conclusion

In multi-cloud system design to be copied and safety design to be copied. In addition to of the elimination of statement as authority business managers, our model design can high doing work well. At the same time, the ID-DPDP signed agreement between nations can take note private verification, gave verification and prevention and public verification based on the clients authority

References

Anilkumar.V.BrahmaneAmrutaAmune ,An Efficient Approach for Dynamic Distributed Network Intrusion Detection using Online Adaboost-Based Parameterized MethodsInternational Journal of Computer Applications (0975 – 8887)Volume 117 – No. 18, May 2015

Poovarasi R, Anbumozhi A, Sivasankari K. Distributed intrusion detection based on ensemble of classifier using Gaussian mixture models (GMMs). Indian Journal of Science, 2015, 17(55), 34-38

Chandra SekharGolagana , M.Sreedhar , G.ChinnaBabu ,A Novel Application for Integrity Verification in Multi-Cloud Storage by using Provable data possession ,International Journal of Application or Innovation in Engineering & Management (IJAIEM) November 2013

Kailas S. Elekar , prof M.M.Waghmare , Effective Intrusion Detection System using Combination of Data Mining Techniques ,ourth Post Graduate Conference ,iPGCON-2015

MeghaPatil , Prof. G.R.Rao ,Integrity Verification in Multi-Cloud Storage Using cooperative provable data possesion,(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 982-985