Integration of Multiple Approaches with DIDS for Cloud Security

Punam D. Mate
Computer Engineering, YTCEM, Mumbai, India.

Madhumita Chatterjee
Computer Engineering, PCE, Navi Mumbai, India.

Gaurav Sharma
Computer Engineering, PCE, Navi Mumbai, India.

Abstract – Cloud framework supports end users to easily access powerful and shared resources, software and information stored on specific server. While accessing resources on a Cloud, user needs to deal with security provided by Cloud Service Providers. To achieve the goal of security while storing data on Cloud Servers multiple methods have been proposed but each has limitations of their own. In this Paper we propose a system to solve key challenges of Cloud Storage Servers by integrating Encryption, distributed storage up a file (Split-up) and OTP. The proposed system also provides way to counter DOS and DDOS attacks by incorporating Distributed IDS (DIDS) along with the storage achieving a higher level of security.

Index Terms– Cloud Computing, Intrusion Detection, OTP, DOS, DDOS.

1. INTRODUCTION

Cloud Computing is a computing paradigm where scalable and flexible IT functionalities are delivered as a service to all cloud customers through various internet technologies. With these new computing and communications techniques arise new data security challenges. Anyone with a suitable internet connection and standard browser can access a cloud application. Cryptography alone cannot provide security, demanded by cloud computer services. DDOS is considered one of the most dangerous security threats. As use of internet is growing day by day, user needs to process data, to store data and to develop application but they are unable to do the same their own machine as configuration of that machine does not match the required configuration, To fulfill this requirements Cloud helps user to develop, access and store data and applications over Cloud, but security of data on Cloud becomes a fundamental issue.

Many mechanisms are present to achieve Cloud Data Security such as Encryption, Intrusion Detection System (IDS), and Distributed Intrusion Detection System (DIDS). But, Encryption alone cannot achieve data security completely. IDS and DIDS may counter the attacks like Denial of Service (DOS) or Distributed Denial of Service (DDOS). But if attacker hacks IDS and gets successful to access data, there is no solution to secure data.

Data theft attacks are modified if an attacker is a malicious insider. Cloud Security Alliance has considered it as one of the top threats to cloud computing [1]. All the top threats such as Abuse and Nefarious use of Cloud Computing[9], Data Loss or Leakage Account or Service, Insecure Interfaces and APIs, Malicious Insiders, Shared Technology Issues, Hijacking Unknown Risk Profile to Cloud computing are explained by Cloud Security Alliance and this document is updated every year when new threats comes into the area of Cloud Computing.

In [2], *Dijk et al.* have shown the limitations of cryptography alone in meeting the challenges of cloud privacy, i.e., fully homomorphic encryption is not a sufficient data protection mechanism when used alone.

In [5], *Rocha et al.,* has outlined how easy passwords may be stolen by a malicious insider of the Cloud Service Provider The authors also demonstrated how Cloud customers' private keys might be stolen, and how their confidential data might be fetched from the computer or machine.

Shaikh et al., in [6], have identified that security is the biggest hurdle in wide acceptance of cloud computing. Users of Cloud services fear loss of data and privacy. Their study identifies top security concerns, viz., user's authentication, data loss, attacks by malicious users, leakage of data, trust management, hijacking of sessions while accessing data and so on.

Claycomb et al., in [8], presented cloud related insider risks viz. insider who exploits a cloud-related vulnerability to steal information from a cloud system, and the insider who uses cloud systems to carry out an attack on an employer's local

resources. They also characterize a hierarchy of administrators within cloud service provider and showed that how of cloud systems architectures enables attacks to succeed. Thus, the aim of the proposed method is to achieve higher level of data security for cloud by integrating DIDS and encryption with multiple approaches for cloud security.

2. LITERATURE REVIEW

Cloud computing framework gives access to share distributed resources and services that belong to different organizations or sites. Cloud computing allows to share distributed resources via the network. Thus, cloud computing requires additional security mechanisms to be implemented.

In [3], *Lee et al.* has explained Multilevel Intrusion Detection System. They propose a system which enables Cloud Computing System to achieve effectiveness of system resource and strength of security services without trade-off between them. Proposed Method also provides how to decrease rule-set size of IDS and also manages User logs. They have classified IDS into three levels, viz., Low, High and Medium, and also specified levels of anomalies based on risk factor and according to level of anomaly it assigns work to those specific IDS.

In [4], *Lo et al.* presents a cooperative intrusion detection system for cloud computing network to reduce the impact of DOS attack. The cloud computing regions, when encounter a DOS or DDOS attack, send alert messages to each other using the framework of cooperative intrusion detection. Each IDS in a region has a cooperative agent that computes and check whether to accept or deny the alert sent from other IDS.

In [7], *Li et al.* proved that the traditionally available DIDS could not detect the sophisticated intrusion attacks. The authors have proposed a distributed intrusion detection model based on cloud theory which is composed of Intrusion Detection Agent subsystem and Data Aggregation subsystem to improve detection of intrusion behavior and detection ability of complicated intrusion attacks.

In [10], *Alqahtani et al.* have presented an Intelligent Intrusion Detection System for Cloud Computing (SIDSCC) service which results illustrate that IDS Server possesses an effective mechanism against ICMP packets that comes over SaaS Cloud. It highlights the major vulnerabilities of SaaS Cloud network, which is the rate of packets lost. They also gives an overview of different intrusions in cloud and analysis of some existing cloud based intrusion detection systems (IDS) with respect to their type, positioning, detection time, detection technique, data source and attacks they can detect. They also emphasize the deployment of IDS that uses multiple detection methods to cope with security challenges in cloud.

In [11], *Nikolai et al.* shows that the proposed hypervisor-based cloud intrusion detection where virtual machines requires no additional software to be installed and has many advantages compared to host-based and network based intrusion detection systems which adds benefits to traditional approaches to intrusion detection by presenting Hypervisor-based Cloud Intrusion Detection System. They showed that hypervisor system does not require additional software to be installed in virtual machines.

3. PROPOSED WORK

As Cloud Security is major concern of Cloud Customers, Security Aspect is measured while selecting a Cloud Service Provider. As previously proposed system had few limitations, the proposed work implements "Integration of DIDS System with Split-Up approach Encryption and OTP mechanism for security of the Cloud". Fig. 3.1 shows System Architecture with following modules.

- Registration Module
- Upload Module
- Download Module
- Attack Handling Module
- File Sharing Module

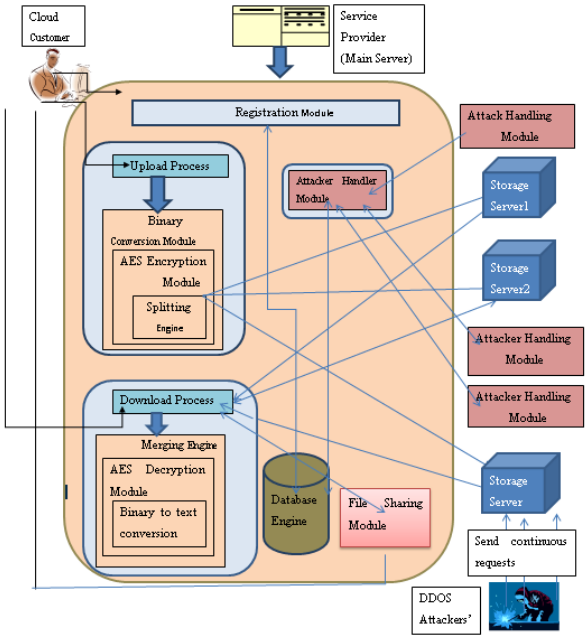

Fig. 3.1 System Architecture

3.1 Registration Module:

For using all the services provided by the System Client needs to register an account. For Registrations process, Client needs to follow Profile Generation and Account Activation.

3.2 Upload Module

This module is responsible for uploading file on storage servers. After successful activation of an Account, Client is ready to upload file. Client can choose a file to upload. When Client chooses and uploads file, three processes of Upload Module start their work.

1. Binary Conversion
2. Split-up Engine
3. AES Encryption

Algorithm for Byte conversion and Split

1. Read File in a variable F
2. Begin
3. Store File Size to variable SIZE(F)
4. Define the number of parts Pn (in our case, 3)
5. Calculate part size, P[(n-1)] = SIZE(F) / (Pn-1)
6. The size of remaining part P[n] = (SIZE(F)) – (SUM(P[i<(n-1)]))
7. Read file streams Byte[] FB=Byte(F)
8. Read data from original file bytes at (start+i) and write to part data at i.
9. Check if any bytes remains if(P[n]>0)
10. Then copy remaining bytes from original file bytes to last part COPY{ FB(P(n-1)*2) -> P[n] }
11. Close File in F
12. Delete ORG File
13. End

3.3 Download Module

Download Module is responsible for file download process. When client clicks on "select file" to download, Email is sent to him with encryption keys related to that file and One Time Password (OTP). When Client enters those encryption keys and valid OTP, file is mailed to him. Download process consists of following AES Decryption, Merge Engine and Conversion from binary to original format.

Algorithm for Merge and Get Original File

1. Begin
2. Initiate the number of storage servers i.e. no. of chunks Pn (in our case 3)
3. Get summation of size of each part SIZE(F) = SUM(P[0]+P[1]+P[2]+. . . +P[n])
4. Initiate byte array of size Byte[] FB=new Byte(SIZE[F])
5. Copy bytes from each part to byte array FB
6. For(i<Pn) COPY { P[i] -> FB[] }
7. Write stream byte[] FB to original file type F
8. Save file in F to output
9. Close file in F
10. End

3.4 Attack Handling Module

Cloud security is major concern for client. However, achieving it needs to handle all the attacks encountered by an Attacker. Attacker tries to make DOS (denial of service) or DDOS (distributed denial of service) attack on any Cloud Storage Server. Attack is detected by IDS (Intrusion Detection System) on cloud and informed to the server about IP address of that attacker and blocks that IP Address and informs to all Clouds about the same. Hence, next time when same attacker encounters attack on same or another cloud attacker is blocked.

Algorithm for Attack handling Module:

1. Begin
2. Invoke method on new request from client
3. Read the IP address of client IP[client]
4. Check IP address in database
5. Check_result = Check(IP[client])
6. If Check_result = true then block ip address and jump to step 17
7. If Check_result = false
8. Then count requests from same IP address Tot_Req = count (IP[client])
9. If total requests are equal or more than 10 If Tot_Req > 10
10. Then block ip address BLOCK(IP[client])
11. If total requests are more than 0 but less than 10 0 < Tot_Req < 10
12. Then increment request count by one Tot_Req{IP[client]} +=1
13. If total requests are zero or ip address not present
14. Then save IP address in temp session Temp_Session = IP[client]
15. And initiate Tot_Req = 0
16. Jump to step 2 for check new request
17. End Session

3.5 File Sharing Module

This module handles data sharing responsibility. When a user logs-in he can see the option as "Other User's File". When he clicks on other users file option, he will see the list of all the files uploaded by all the users with all the details. The user can then request for the any of the files by clicking on "request file" button. Owner of the requested file will then get an email with encryption keys and OTP and needs to enter those encryption keys and OTP and click on approve request. As soon as user clicks on approve request, that file will be mailed to Requesting user.

4. RESULTS AND ANALYSIS

Existing System allows file to be uploaded on single Storage Server, hence there are Limitations of an Existing System that

does not provides Distribution of user data on different storage servers, cannot prevent DDOS attack fully. No mechanism to protect user data if hacker gets success to overcome/skip all security gates. But in implemented system if attacker gets access to one part, he cannot have the complete file. Figure 4.1 shows uploaded file's view.

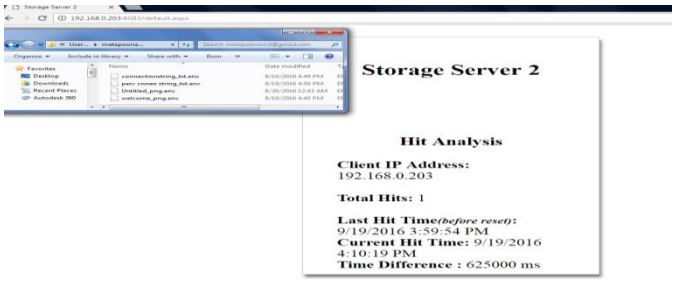

Figure 4.1 Uploaded File's View

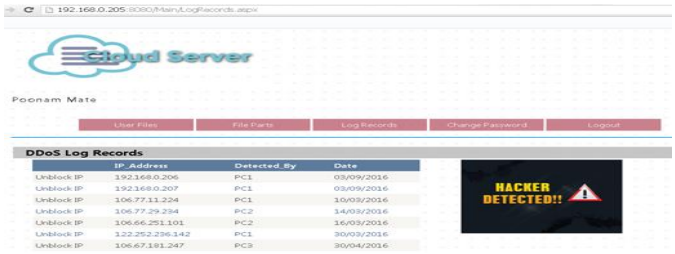

Figure 4.2 Attack Log Record

Existing system is able to provide Encryption, Split-Up approach, and way to secure data even when hacker succeeds to get data. Time required to process data by an existing system is almost same as compared to proposed and implemented System because even if file is Split, Encrypted and then Stored, as all file's all parts are fetched in parallel and parts are small compare to complete file, time required to fetch those small parts is less as compare to fetching complete file. There is trade-off between performance and Security. Security provided is high. Security is major concern as compare to time required for processing. Figure 4.1 shows Performance Analysis graph for Time. Table 4.1 shows Comparison chart between Proposed System and relevant researches.

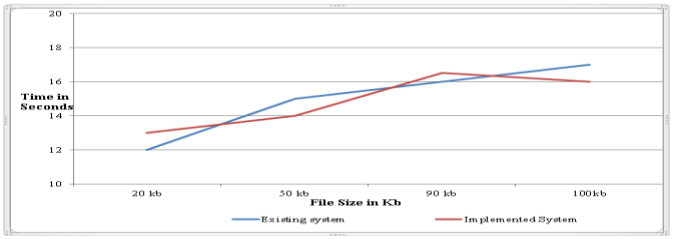

Figure 4.1 Performance Analysis

SYSTEM PARAMETERS	PROPOSED IDS	COOPERATIVE IDS	DISTRIBUTED IDS	COLLABORATIVE IDS	MULTILEVEL IDS	HYPERVISOR BASED
SERVICE BASED	YES	YES	YES	YES	YES	YES
ENCRYPTION PROVIDED	YES	NO	NO	NO	NO	NO
SPLITTING ENGINE USED	YES	NO	NO	NO	NO	NO
ATTACKER CAN DOWNLOAD ENTIRE AES ENCRYPTED FILE	NO	YES	YES	YES	YES	YES
ATTACKS COVERED	DOS/DDOS	DOS/DDOS	DOS/DDOS	DOS/DDOS PORT SCANNING	DOS/DDOS	DOS/DDOS
IDS TECHNIQUE	HIDS	NIDS	HIDS OR NIDS	HYBRID	BASED ON LEVEL OF SECURITY	HYPERVISOR BASED
IF KEY IS COMPROMISED ATTACKER IS ABLE TO GET FILE	NO (OTP is used)	YES	YES	YES	YES	YES

Table 4.1 Comparison with Relevant research

5. CONCLUSION

In the Proposed work Distributed Intrusion Detection System with the Integration of Encryption, parts of data and OTP for Cloud Security, maintains availability of system by blocking, by blocking DOD/DDOS attacks. It also achieves level of confidentiality by using Encryption and Data-Chunk mechanisms while uploading a file. Every Storage Server synchronizes its attack log periodically with Main Server to achieve Integrity. If the attacker tries to download a file from any of the single Storage Server, he is unaware that it is not a complete file and decryption would not work. The System also provides file sharing facility by placing request for any of the file uploaded by any of registered users. Encryption of Data by AES makes data more Secure. Enforcing to enter One Time Password (OTP) and multiple encryption keys sent to Email-ID at the time of file download, increases Data Security one level up.

In Future Work, OTP facility can be send to mobile instead of Email account making it most secure.

REFERENCES

[1] Cloud Security Alliance, "Top Threat to Cloud Computing V1. 0," March 2010. (URL).

[2] Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec'10. Berkeley, CA, USA: USENIX Association.

[3] Jun-Ho Lee, Min-Woo Park, Jung-Ho Eom, and Tai-Myoung Chung "Multi-level Intrusion Detection System and Log Management in Cloud Computing". in Advanced Communication Technology (ICACT), 2011 13th International Conference.

[4] Chi-Chun Lo, Chun-Chieh Huang and Joy Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks" IEEE 2010. DOI 10. 1109/ICPPW. 2010. 46.

[5] F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," in Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops, ser. DSNW '11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 129–134.

[6] Engr: Farhan Bashir Shaikh and Sajjad Haider " Security Threats in Cloud Computing" 6th International Conference on Internet Technology

and Secured Transactions, 11-14 December 2011, Abu Dhabi, UnitedArab Emirates, 978-1-908320-00-1/11/$26. 00 ©2011 IEEE.

[7] Han Li, Qiuxin Wu "A Distributed intrusion detection model based on cloud theory" 978-1-4673-1857-0/12/$31. 00 ©2012 ieee.

[8] William R. Claycomb, Alex Nicoll, "Insider Threats to Cloud Computing: Directions for New Research Challenges", In Computer Software and Applications Conference (COMPSAC), IEEE 36th Annual, 2012, July.

[9] Yasir Ahmed Hamza1, Marwan Dahar Omar1 "Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing" International Journal of Computational Engineering Research, 6,june 2013.

[10] Saeed M. Alqahtani, Maqbool Al Balushi and Robert John "An Intelligent Intrusion Detection System for Cloud Computing (SIDSCC)" 2014 International Conference on Computational Science and Computational Intelligence.

[11] Jason Nikolai and Yong Wang "Hypervisor-based Cloud Intrusion Detection System". Computing, Networking and Communications (ICNC), 2014 International Conference.

[12] Wikipedia the free encyclopedia://en.wikipedia.Org/wiki/Cloud_computing.