ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 1-5 (2016)

Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

A Comparative Analysis on Cloud Security Issues

T. Satya Nagamani, Asst.Professor
Department of Information Technology
Sir C R Reddy College of Engineering
Eluru, AP, India.
happysatyasai@gmail.com

G. Krishna Veni, Asst.Professor
Department of Information Technology
Sir C R Reddy College of Engineering
Eluru, AP, India.
veni.garlapati@gmail.com

ABSTRACT

Cloud computing in essence an Internet-based network made up of large numbers of servers - mostly based on open standards, modular and low-priced. Clouds contain enormous amounts of information and provide a variety of services to large numbers of people. In cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and financial savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes conventional data utilization.

This paper proposes various protection mechanisms like secure document service mechanism, Claim Based Security (CBS), and Intrusion Detection System and finally their comparative investigation is given in brief.

KEYWORDS

Encryption, Decryption, Networks Security, Privacy, Claim, Security Token service, Identity Providers, Federation Provider, Intrusion Detection.

INTRODUCTION

Cloud computing is the long dreamed vision of computing as a efficacy. Cloud computing builds upon advance of research in virtualization, distributed computing, grid computing and utility computing [11]. Cloud computing is a collection of all sources to enable resource sharing in terms of scalable infrastructures, middleware and application development platforms, and value-added business applications [11]. A major concern is about data security, that is, how to protect data from unlawful users and leakage. In order to reduce action costs on client leakage. In order to reduce action costs on client end and boost the efficiency of alliance, the cloud undertook the majority of jobs.

Cloud computing is subscription-based service where you can gain networked storage space and computer resources. Security is main issue when we are executing many jobs. As can be seen, for both individual user and large-scale enterprises, it is an important issue to protect key data within cloud pattern [12]. In Fig[1] we have an architecture of cloud with different set of users

Consider the potentially large number of on-demand data users and huge quantity of outsourced data documents in the cloud, this problem is particularly tricky as it is awfully difficult to meet also the requirements of performance, system usability and scalability. To retrieve the data from the cloud user has to approach different application interfaces as shown in Fig [1].On the one hand, to meet the effectual data retrieval need, the large amount of documents demand the cloud server to perform result relevance grade, instead of returning undifferentiated results. Whereas the cloud platform will be divided into Data visualization layer, distributed visualization layer and workload distribution system as given in the Fig [1]. Ranked search can also elegantly purge unnecessary network traffic by sending back only the most pertinent data, which is highly desirable in the “pay-as-you use” cloud archetype.

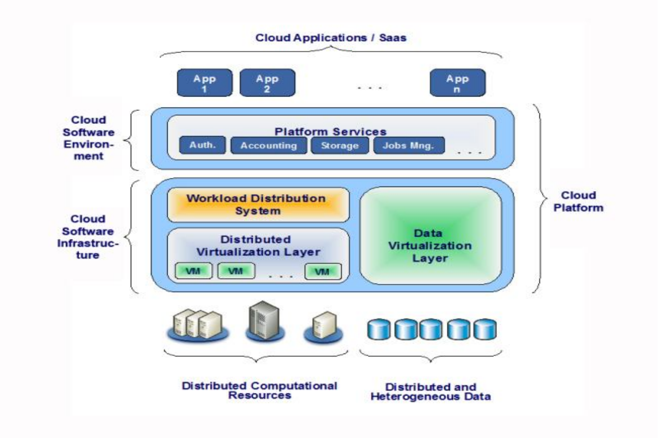
Cloud Applications / Saas
App 1
App 2
. . .
App n
Cloud Software Environ-ment
Platform Services
Auth.
Accounting
Storage
Jobs Mng.
. . .
Cloud Software Infrastruc-ture
Workload Distribution System
Distributed Virtualization Layer
VM
VM
. . .
VM
Data Virtualization Layer
Cloud Platform
Distributed Computational Resources
Distributed and Heterogeneous Data

Fig 1: Cloud computing architecture.

SECURE DOCUMENT SERVICE MECHANISM

Guaranteed privacy of user’s document was vital concept for security document service. For ideal distributed document service based on cloud computing, document handling and storing were not executed by local system in client-end but by remote cloud server that provide document service. There is a novel mechanism to preserve the privacy of user’s document, which correspond with cloud computing. We identify documents with content-format combinations. In reality, most of private information was not stored in format but content.

Making secure content handling was crucial for guaranteeing document privacy. We separated content from document and then content ought to be encrypted before been propagated and stored in remote server.

a) Document Partition

Usually, document handling often did not cover the whole content and format but a part of them. It is not required to re-store the whole document, but just its partition that were handled. It is believed that partitioning the document prior to handling and only updating the modified partition could reduce the overhead of document service and the possibility of the whole document being damaged and hacked.

b) Document Authorization

Data authorization can be implemented by public-key cryptography in traditional network environment.

General Authorization Method (Method 1).

In common practice, the document owner had charge of authorizing other users for accessing documents. We denoted the public and private key of OwnerI as BI , PI and the public and private key of UserJ as BJ , PJ , respectively. BI (c) depicted that content c was encrypted with OwnerI's public key and the procedure of decryption could be written as PI (BI (c)). If OwnerI wanted to authorize UserJ for accessing document, OwnerI required to encrypt the content by UserJ 's public key, namely BJ (PI (c)).

Document owners overhead of encrypting content, on the contrary, would be in conformity with the users who were authorized.

Optimized Authorization Method (Method 2)

(a) Construct two encryption functions f(x), g(x), both of them have the following properties:

i) It is hard to find inverse functions for both functions.

ii) For any M, when f(M) = N, there must be g(N) = M. Also, for any M, when g(M) = N, there must be f(N) = M. As summarize, g(f(M)) = f(g(M)) = M.

iii) It is hard to find inverse function for f(g(x)) and to decompose f(g(x)) as the combination of f(x) and g(x). Denote f(g(x)) as H(x).

iv)It is hard to find inverse function for f(g(g(x))) and to decompose f(g(g(x))) as the combination of f(x) and g(x). Denote f(g(g(x))) as I(x).

v) For any M, when f(M) = N, there is H(N) = f(M).

vi) For any M, when f(M) = N, there is I(N) = f(g(M)).

(b) Suppose H(x) existed and encrypted document BI (c) stored in cloud server, when OwnerI authorized UserJ for access to BI (c) H(x) would be submitted to cloud server. Cloud server would then automatically compute H(BI (c)) and send it to UserJ . H(BI (c)) could be generated as BJ (c) by UserJ . It is easy for UserJ to decrypted BJ (c) by using PJ .(c) Suppose I(x) existed,when UserJ obtained encrypted contentBJ (PI (c)),content c could be generated by computing BI (PJ ((BJ (PI (c))))).

SECURE USING INTRUSION DETECTION SYSTEM

Problems

As shown in Fig[2] Suppose that two users, Client1 and Client2 use the "conventional client- server" system and both are concurrently sending multiple requests to the same server. If the acknowledgment time is escalating, perhaps data. The second problem is, multiple users are requesting the same in parallel. The third problem is, there is no security mechanism.

The main cloud server is connected to all the proxy servers and it maintains the index of the data information by all the proxy servers. At first, the user sends the request to the main cloud server. Then the main cloud server will forward the request to the exact proxy. The proxy server gives backside the information to the main cloud server. Finally, the proxy server will send the file to the user as in Fig[2]. The network administrator cannot monitor all the clients, so it will depend on the IDS which gives the alerts to the remaining "cloud server". So for preventing data from hackers.

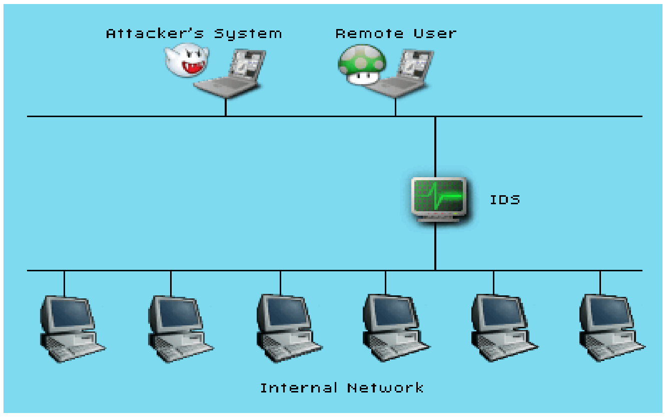

Fig 2: Intrusion Detection System

IDSs are auditing engines, so models of auditing system can illustrate their architecture. When an intrusion occurs some response is appropriate. If the intrusion attempt is detected before the attack is successful, the system can take the action to prevent the attack from succeeding. An IDS inspects all inbound and outbound network activities and identifies suspicious patterns that may indicate a network or system attacks from someone attempting to split into or compromise a system.

The cloud computing uses the internet as the communication media. The Cloud computing system can be easily threatened by various attacks.

Due to their scattered nature, cloud computing environment are easy targets for intruders looking for potential vulnerabilities to exploit. Cloud computing have two approaches i.e. Knowledge-based IDS and Behavior-Based IDS to detect intrusions in cloud computing.

Behavior-based intrusion detection techniques presume that an intrusion can be detected by observing a divergence from normal or predictable behavior of the system or the users. The model of normal or valid behavior is extracted from reference information collected by various means. The intrusion detection system later on compares this model with the present activity. When a deviation is observed, an alarm is generated. Anything that does not correspond to a previously learned behavior is considered intrusive. Therefore, the intrusion detection system might be complete (i.e. all attacks should be caught), but its accuracy is a complex issue (i.e. you get a lot of false alarms).

Knowledge-based intrusion detection techniques apply the knowledge accumulated about specific attacks and system vulnerabilities. The intrusion detection system contains information about these vulnerabilities and looks for attempts to exploit these vulnerabilities.

Knowledge-based approach uses signatures (evidences of attacks and behavior-base approach)uses a set of regular activities to check abnormality, providing a security mechanism called IDS.

An IDS is positioned in the proxy server.

Intrusion Detection System Architecture

The elements that are participating in the architecture are nodes, service, event auditor and storage devices. A node has resources which are accessed homogeneously through middleware. The middleware sets the access-control policies and supports a service-oriented environment.

In the architecture shown in the below Fig[3], the event auditor plays an important role in the system. Initially, it captures the information from different sources such as the log system, nodes and services. After capturing the data the IDS service analyzes the data based on the intrusion detection techniques such as knowledge based and behavior based. If an intrusion is detected in the system then the IDS service uses middleware communication mechanisms for sending alerts to the other nodes. The middleware synchronizes the knowledge based and behavior based databases.

The storage service holds data that should be analyzed by the IDS service as shown in Fig[3]. Because all nodes have to access the same data in the environment. So, the middleware must transparently create a virtualization in the homogenous environment. The client sends a request to the server for getting a service. In the "conventional client server" system, the client communicates with the end server directly, due to which traffic congestion or

data loss etc might take place. So to overcome this issue we have implemented a proxy server, which extends the functionality of the main cloud server and is the mediator between your web browsers and the end server. Initially, your web browser sends a request to the proxy server, after which the proxy server forwards the request to the end server. The end server then gives acknowledgment to the proxy server.

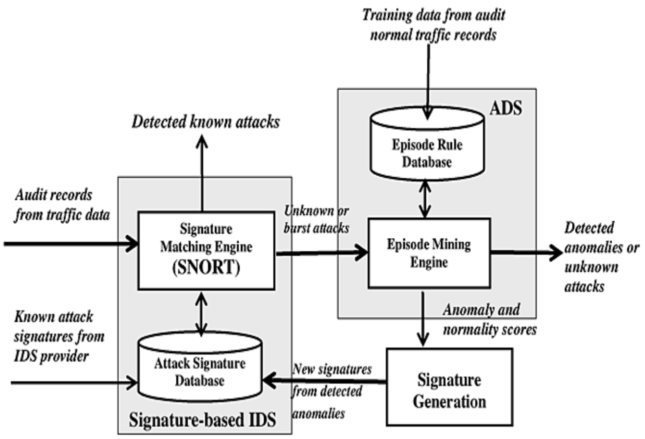
Training data from audit normal traffic records
ADS
Episode Rule Database
Detected known attacks
Audit records from traffic data
Signature Matching Engine (SNORT)
Unknown or burst attacks
Episode Mining Engine
Detected anomalies or unknown attacks
Anomaly and normality scores
Known attack signatures from IDS provider
Attack Signature Database
New signatures from detected anomalies
Signature Generation
Signature-based IDS

Fig 3: Work flow of Intrusion Detection System

Finally, the proxy server replies to the browser So, HTTP request is originated from the intermediate proxy server. As a result the client computer's IP address will be in hidden state and illegitimate users cannot access the client computer's IP address. This type of proxy server is also known as anonymous proxy server.

. Features

- Highly virtualization and standardized infrastructures
- Massive scalability
- Fault tolerant & high reliable
- Intra and inter cloud load balance
- Instant application deployment

CLAIM BASED SECURITY FOR CLOUD

Cloud computing provides a cloud infrastructure that is used to provide cloud services to their cloud users. During the access time, consumers provide sensitive data such as name, SSN number credit card information for accessing the online services of a cloud service provider. Privacy of the information totally depends on the cloud service security as well as value of the information. As the result, a username/ password security token is used by the most service provider to authenticate [, which may result in the phishing/password guessing attacks to consumer.

There is a need for a solution to address the above problem in form of an Identity Management (IDM) solution. For a developer working with identity management traditionally hasn't been much fun. First a developer decides which identity technology is used in which application, that is accessed in an organization or across an organization via the internet. Each application uses different identity technology to find and keep track of identity of users in different applications. The application gets some information from those users and might get other access from the directory services or some other identity provider.

Rather than using multiple identities, using this single approach user access to the cloud services gives the better result.

Claim-based identity management system is used to address the above problem. This approach provides a single identity that is used to access the cloud services within an organization or outside an organization in the form of digital identity via the internet. Claim-based identity management systems store user's information in the form of digital identity that is used to authenticate and get the role of the user in an application.

Claims-Based Architecture

In this architecture as shown in Fig[4], common assumption is that every participating entity has an identity, which is stored in some other central active directory and every entity follows a consistent identity management technology. In this system they create centralize identity server which is trust server which can be chosen by the user and cloud service provider in cooperation. The identity server provides following facilities

- Registration
- Selection of cloud service
- Implementation of cloud mechanism

user will be providing all its details to the identity server only and cloud will receive the authentic session id from the identity server. For any usage of any service user must be logged in and must have got an authenticated session-id to be presented to the cloud. If a user is using two different services then he will only require to login once and provide service claim id to get the authenticated session id from the identity server.It works smoothly and gives utmost accuracy.

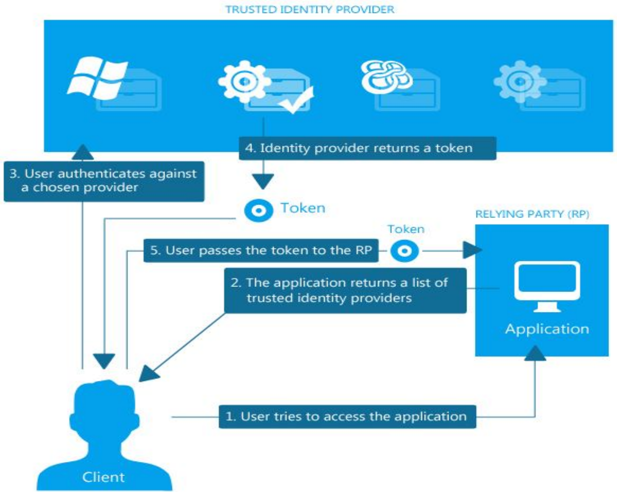
TRUSTED IDENTITY PROVIDER
4. Identity provider returns a token
3. User authenticates against a chosen provider
Token
RELYING PARTY (RP)
Token
5. User passes the token to the RP
2. The application returns a list of trusted identity providers
Application
1. User tries to access the application
Client

Fig 4: Claim based security architecture.

The double authentication process being applied. The first authentication is explicit where user provides the login details to the identity server. After verification by the identity server, user accesses the cloud with key and session id provided by identity server. These key and session ids are again verified by the cloud from identity server in second authentication process which is hidden from users as shown in Fig [4].

COMPARATIVE SCRUTINY

All the three methods for securing the data at and in cloud has been implemented procedures for their best extent. However there are merits and demerits with each system regarding their implementation and also the result obtained. Here we will see the comparative analysis of the methods in a table [1] with respective advantages and disadvantages.

Table 1: Illustrating the comparison among the three security methods.

S.No	Method	Advantages	Disadvantages
1	Secure Document Service Mechanism	Document will be securely received in a encrypted form	Data assurance will not be there because of the document partition before encryption.
2	Secure using intrusion detection system	IDS will secure the system IPs as well as the data from the intruder attacks.	Middleware proxy server should be a knowledge base of all the behaviors otherwise chance of rising false alarms.
3	Claim Based Security for Cloud	Double authentication procedure gives utmost security to the cloud	Client chosen server may not be a security assured server to cooperate with the cloud server.

As there are some linguistic problems in above explained table [1] existing security methods which are non-imaginable attacks, we propose some alternative solution to be implemented in future which includes the encryption of the user accessing document will be done without partitioning instead of which it will be zipped without losing any contents of it. The same document is given access to the user with the claim based security method adding the middleware server security through the IDS procedure so that there is no chance of insecurity from the unauthorized middleware. We hope this technique will give the secure cloud services if it can be implemented with nativity.

References

[1] H. Debar, M. Dacier, A. Wespi,"Towards a Taxonomy of Intrusion Detection Systems," Int'l J. Computer and Telecommunications Networking, vol. 31, no. 9,1999, pp 805–822.

[2] I. Foster et al.,"A Security Architecture for Computational Grids," Proc. 5th ACM Conf. Computer and Communications Security, ACM Press, 1998, pp. 83–92.

[3] Text book, Could Computing.

[4][Online]Available:http://www.en.wikipedia.org/wiki/ Intrusion_detection_system

[5] Resnick, P., Zeckhauser, R.,"Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system", Advances in Applied Microeconomics: A Research Annual 11, pp. 127–157 (2002)

[6] Krautheim, F.J.,"Private virtual infrastructure for cloud computing", In: HotCloud, USNIX (2009).

[7] Rivest, R., Shamir, A., Adleman, L.,"A method for obtaining digital signatures and public-key cryptosystems.

[8]Biham, E., Shamir, A.,"Differential cryptanalysis of DES-like cryptosystems", Journal of Cryptology 4(1), 3–72 (1991).

[8] Singh, A.; Chatterjee, K.,"Identity Management in Cloud Computing through Claim-Based Solution", Advanced Computing & Communication Technologies (ACCT), 2015. Fifth International Conference on, pp. 524,529, 21-22 Feb.

[9] [Onli ne] Available: msdn.microsoft.com /en-us /library/ hh446535.aspx

[10] Shalini Shrivastava, Aviral Dubey, Efficient Claim Based Security for Cloud , International Journal of Computer Science and Technology Vol 6.4 ver – 1 (Oct – Dec 2015).

[11] National Conference on Recent Trends in Computer Science and Information Technology(NCRRCSIT-2013) IJCST Vol. 4, Issue Spl - 4, Oct - Dec 2013, "Data Protection Analysis in Cloud Computing".

[12] National Conference on Recent Trends in Computer Science and Information Technology(NCRRCSIT-2013) IJCST Vol. 4, Issue Spl - 4, Oct - Dec 2013," A Trusted Mechanism For Providing Security Over Cloud Computing".

ABOUT AUTHORS

T.Satya Nagamani, working as an Asst. Professor, in I.T Department, Sir C. R. Reddy College of Engg, Eluru, A.P., India.
She has received her B.Tech (CSIT) from Lakireddy BaliReddy College of Engineering, Mylavaram,A.P and M.Tech(CSE) from JNTUK,AP.
Her research interests include Cloud Computing, Big Data,Data Mining, Networks and Image Processing.

G. Krishna Veni, working as an Asst. Professor, in I.T Department, Sir C. R. Reddy College of Engg, Eluru, A.P., India.
She has received her B.E (Mech) from S.R.K.R College of Engineering, Bhimavaram, A.P and M.Tech(CSE) from JNTUK,AP.
Her research interests include Cloud Computing, Big Data, Data Mining, Networks and Security.