IJIRMET

ISSN (Online): 2456-0448

International Journal of Innovative Research in Management, Engineering and Technology

Vol. 3, Issue 3, March 2018

Providing Restrictions Against Attack And Congestion Control In Public Infrastructure Clouds

[1] S.Gayathrri ,M.E, [2] Dr.N.Saravanan, M.E,Ph.D,

[1] [2]Department Of CSE MNM Jain Engineering College, Chennai.

Abstract: ***Cloud computing is an environment that plays an vital role in business or in an IT sector for the data storage. Now- a-days petabytes of data is being stored for their future use in order to retrieve the data. This paper proposes a Secure Cloud Computing Adoption framework for automatic intrusion detection, Identity management of users and service provider and key seed mechanism. Multicloud Service provider is held to provide authentication for the users, in order to provide prevention of the attackers or an hackers. we describe a framework for data and operation security in IaaS, consisting of protocols for a trusted launch of virtual machines and domain- based storage protection. Thus once the user is authenticated they will be launched in virtual machines where they initiate the upload process into the cloud. Keywords- virtual machines, domain-based storage protection,, Multicloud service provider, Attribute Based Encryption, Automatic Intrusion Detection, Key seed mechanism.***

Keywords: ***virtual machines, domain-based storage protection,, Multicloud service provider, Attribute Based Encryption, Automatic Intrusion Detection, Key seed mechanism.***

I. INTRODUCTION

Cloud computing is an massive environment which has been developed for open secure data storage for storing the petabytes of data or files. These environment acts as the authorized and authenticated only to the registered users. once the user is being registered in this data storage environment, that particular user alone can logon to store the data or files and they can upload each files or data of the logon users. Here the public cloud is being licensed with the users permittable state and the privacy will be acting as a major role for the authorized users.

II. RELATED METHODS

In Ciphertext Policy Attribute based Encryption scheme, the encryptor can fix the policy, whocan decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the ciphertext. We propose a method in which the access policy need not be sent along with the ciphertext, by which we are able to preserve the privacy of the encryptor.

Cloud computing offers great potential to improve productivity and reduce costs, but at the same time it possesses many new security risks. In this paper we identify the possible
security attacks on clouds including: Wrapping attacks, Malware-Injection attacks, Flooding attacks, Browser attacks, and also Accountability checking problems. We identify the root causes of these attacks and propose specific solutions.

Anomaly based Intrusion Detection Systems (IDSs) are known to achieve high accuracy and detection rate. However, a significant computational overhead is incurred in training and deploying them. In this paper, we aim to address this issue by proposing a simple Artificial Neural Network (ANN) based IDS model. The proposed IDS model uses the feed forward and the back propagation algorithms along with various other optimization techniques to minimize the overall computational overhead, while at the same time maintain a high performance level. Experimental results on the benchmark NSL-KDD data set shows that the performance (accuracy and detection rate) of the proposed ANN based IDS model is at par and in some cases even better than other IDS models. Owing to its high performance and low computational overhead, the proposed ANN based IDS model is a suitable candidate for real time deployment and intrusion detection analysis.

Attribute based encryption (ABE) determines decryption ability based on a user’s attributes. In a multi-authority ABE scheme, multiple attributeauthorities monitor different sets of attributes and issue corresponding decryption keys to users, and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase gave a multi-authority ABE scheme using the concepts of a trusted central authority(CA) and global identifiers (GID). However, the CA in that construction has the power to decrypt every ciphertext, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted authorities. Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user’s attributes, which unnecessarily compromises the privacy of the user. In this paper, we propose a solution which removes the trusted central authority, and protects the users’ privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice.

Cloud computing changed the world around us. Now people are moving their data to the cloud since data is getting bigger and needs to be accessible from many devices. Therefore ,storing the data on the cloud becomes a norm.
However, there are many issues that counter data stored in the cloud starting from virtual machine which is the mean to share resources in cloud and ending on cloud storage itself issues. In this paper, we present those issues that are preventing people from adopting the cloud and give a survey on solutions that have been done to minimize risks of these issues. For example, the data stored in the cloud needs to be confidential, preserving integrity and available .Moreover, sharing the data stored in the cloud among many users is still an issue since the cloud service provider is untrust worthy to manage authentication and authorization. In this paper, we list issues related to data stored in cloud storage and solutions to those issues which differ from other papers which focus on cloud as general.

Cloud computing provides users with ample computing resources, storage, and bandwidth to meet their computing needs, often at minimal cost. As such services become popular and available to a larger body of users, security mechanisms become an integral part of them. Conventional means for protecting data privacy, such as encryption, can protect communication and stored data from unauthorized access including the service provider itself. Such tools, however, are not sufficient against powerful adversaries who can force users into opening their encrypted content. In this work we introduce the concept of deniable cloud storage that guarantees privacy of data even when one’s communication and storage can be opened by an adversary. We show that existing techniques and systems do not adequately solve this problem. We design the first sender-and-receiver deniable publickey encryption scheme that is both practical and is built from standard tools. Furthermore, we treat practical aspects of user collaboration and provide an implementation of a deniable shared file system, DenFS.

Cloud computing is a new computational paradigm that offers an innovative business model for organizations to adopt IT without upfront investment. Despite the potential gains achieved from the cloud computing, the model security is still questionable which impacts the cloud model adoption. The security problem becomes more complicated under the cloud model as new dimensions have entered into the problem scope related to the model architecture, multi-tenancy, elasticity, and layers dependency stack. In this paper we introduce a detailed analysis of the cloud security problem. We investigated the problem from the cloud architecture perspective, the cloud offered characteristics perspective, the cloud stakeholders perspective, and the cloud service delivery models perspective
.Based on this analysis we derive a detailed specification of the cloud security problem and key features that should be covered by any proposed security solution.

III. PROPOSED SYSTEM

i. IaaS consisting of protocols for a trusted launch of virtual machines and domain-based storage protection.
ii. If the session tokens are not properly protected, an attacker can hijack an active session and assume the identity of a user.
iii. Session management, we have implemented cookie management and idle timeout.

iv. Authentication is a critical aspect of this process, but even solid authentication mechanisms can be undermined by flawed credential management functions.
v. RSA algorithm For data owner file encryption, we use camellia algorithm Finally the files are stored in public cloud named CloudMe.

A. Architecture

In this paper we propose a multi cloud service provider to split up the files and also authentication is been given with attacks and splitting and merging technique for the file uploading and retrieval purpose. Key seed mechanism to generate different keys at each time of files uploading.

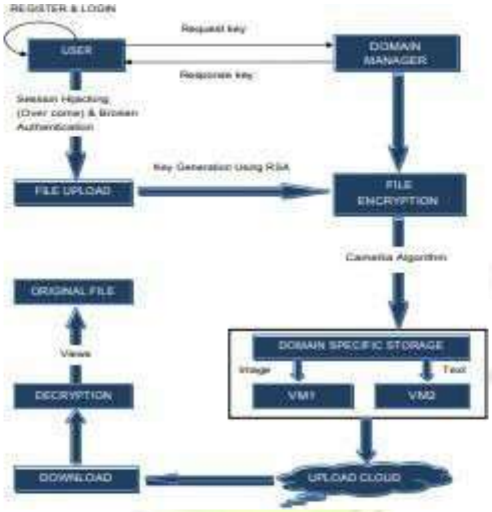

Figure 1

B. *Automatic Intrution Detection*

In this paper we are using the multi cloud concept and the files has been spilled up into four parts and stores a couple of file in each cloud so that authorization is being provided for the users files and the hackers cannot very easily take the files without the users knowledge. The attack has also been implemented for the authorization from the prevention of the attackers. We address the following attacks to prevent the user files such as Brute force attack, SQL Injection and Wrapping attack. In Brute force attack the OTP authentication is being done so that incase of many times trying up of password will automatically block the account and the blocked status will be instantly intimated to the authenticated users knowledge and then the request send from the authenticated original user will be sent so that the blocked account will be unblocked. Due to many times trying password will make much complex for the hackers too. The SQL Injection attack has also been addressed generally for the prevention by using prepared statement and validation has been done, so that if the statement gets false it will prevent the hackers from hacking their files or data. Wrapping attack prevention addresses, when the hacker tries to login the authenticated users account that hacker can only view the design page and the code rather than the web xml and java file of the authenticated user.

C. *Identity Management for User and Service Provider*

In this module, authentication has been done at the user and service provider level. When the registered user is being logon to upload a file at that time too the validation checking is being required by giving the identified user ID and the password at each time for the uploading status.similarly,the service provider will also validate by checking with an required identified password and service providers ID at each time of login the account.

D. *Broken Authentication*

In this paper we propose an attribute based encryption algorithm which has been used for the users file encrypted at each time and that cipher text of the each file will also provide with the private key at the user side by using an key seed mechanism and then the cloud service provider
will send those cipher text files into the two cloud by using the splitting method at the time of sending, the public key will also been generated for each files and the file ID is identified for each files of the authenticated user. Hence
the files have been spillited up into four parts and the cloud service provider will convert those files in an encrypted form with their specified file name.

WORKING PRINCIPLE

STEP 1: User will upload a file.

STEP 2: During upload of each file, they are get encrypted using an ABE algorithm with variant of an user attributes.

STEP 3: Each encrypted file will have different keys generated at each time of their upload.

STEP 4: The key generated was mean to be secret key i.e., private key

STEP 5: After uploading, the encrypted file will be in the decrypted form.

STEP 6: When requested file ID is being sent for the user needed file, the file ID will be verified at first.

STEP 7: After verification, the service provider will match the file ID, secret key along with decrypted key which in turn consider to be the encrypted key.

STEP 8: When the required ID, keys are given the particular file will get download for the user’s use.

E. Key Seedmechanism User Sideprocess

i) Uploading the files or data.

ii) Each file upload will automatically generate different key i.e., private key, with respect to the user and file attributes.

ADMIN SIDE PROCESS

i) Splits the uploaded file into cloud.

ii) Public keywill be generated at that time.

iii) The same key is used for the verification purpose too.

F. Multicloudstorage

Cloudme and Dropbox service providers are the two clouds which are being purchased with their licensed

G. Retrival Offiles

When the user sends the request to the service provider, the file ID,keys of both private and public will be analyzed and it will match with the required file ID of the authenticated user, then it is true. By using the splitting and merging techniques the files is retrieved and then it is decrypted by using an ABE algorithm for the user who has been already authorized to use the file.

IV. CONCLUSION

One of the promising factor in this paper is Multicloud service provider used for authentication of the user files. An Attribute based encryption generally encrypt the user files at each time of uploading to the service provider. During uploading of each file, different keys will be generated automatically by using
the key seed mechanism. The files are also been authorized with the attacks such as Brute force, SQL Injection and an Wrapping attack. We hope that hackers cannot easily hack the files from this authentication method.

V. RESULT AND DISCUSSION

In this paper, session hijacking provides storage and reduces the time consumptions. It implements the Domain storage protection and virtual machine.

Figure 2

Infrastructure as a service maintains the cloud storage. Iaas provider also supplies a range of service to accompany those infrastructure components. It includes clustering, load balancing, security and backup.

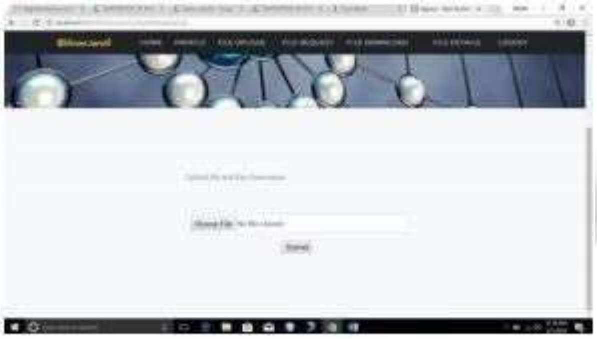

Figure 3

Separate file is chosen from folder and keep the file in privacy mode without admin reference.

References

[1] A.Balu and K.Kuppusamy,“Ciphertext policy Attribute based Encryption with anonymous access policy”in Department of Computer Science & Engg.,Alagappa University.

[2] Kazi Zunnurhain and Susan V. Vrbsky“Security Attacks and Solutions in Clouds”,Department of Computer Science,The University of Alabama,Tuscaloosa, AL 35487- 0290,2010.

[3] Basant Subba , Santosh Biswas, Sushanta Karmakar “A Neural Network Based System for Intrusion Detection and Attack Classification”,Department of Computer Science Engineering Indian institute of technologyGuwahati Assam 2014.

[4] Melissa Chase, Redmond, Sherman S.M Chow “Improving Privacy and Security in Multi-Authority Atrribute-Based Encryption”, Department of Computer science, New York University, NY 10012, USA,pp.515-534,2007.

[5] Melbourne, William Allen and Sultan Aldossary "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions",Department of Computer Sciences and Cypersecurity,Florida Institute of Technology Melbourne, Florida 32901
Vol. 7, No. 4, 2016.

[6] Paolo Gasti, Giuseppe Ateniese and Baltimore, MD Marina Blanton"Deniable Cloud Storage: Sharing Files via Public-key Deniability",University of Genoa, Italy,inWPES,2010

[7] Mohamed Al Morsy, John Grundy and Ingo Müller"An Analysis of The Cloud Computing Security Problem",Computer Science & Software Engineering, APSEC 2010 Cloud Workshop, Faculty of Information & Communication Technologies Swinburne University of Technology, Hawthorn, Victoria, Australia,30th Nov 2010.