International Journal of Advanced Computational Engineering and Networking, ISSN(p): 2320-2106, ISSN(e): 2321-2063
Volume-7, Issue-6, Jun.-2019, http://iraj.in

MITIGATING CLOUD SECURITY THREATS USING CLOUD ACCESS SECURITY BROKERS

[1]SHABNAM KAUR, [2]RAJANDRA GUPTA

[1,2]KMS College of IT & Management, India
E-mail: kmscollegedasuya@gmail.com

Abstract - The importance of Network cloud is increasing and it is accepting a developing attention in the scientific and industrial communities. Cloud Computing has already started to revolutionize the method we store and access data. Security issues in Network cloud computing are some of the biggest concerns surrounding the technology. To promote cloud computing in a wide range of apps, security issues required to be resolved. Data breaches of cloud services are increasing every year due to hackers, who is always trying to exploit the security vulnerabilities of the architecture of cloud. Cloud Access Security Brokers (CASBs) are one of the fastest growing security technologies, today because they provide cloud service visibility, data security, threat protection, and compliance. CASBs are an effective and easy way to mitigate the top cloud security threats and security practitioners look to trusted CASB suppliers as key accomplices to help exhort on key cloud security decisions. The research is to implement information dispersal algorithms to prevent Data Breaches using Cloud Access Security Brokers.

Keywords - Network cloud, Security Issues, Cloud Access Security Brokers (CASBs), Information Dispersal Algorithm, Data Breaches.

I. INTRODUCTION

We are rapidly moving towards a Cloud majority world. Be that as it may, Cloud adoption has likewise presented another set of risks, both inner and external. The cloud access security broker can provide stronger cloud protection at a lower cost than traditional security processes and tools. Multiple types of security policy enforcements required:

- Authenticated access
- Single sign-on
- Data loss prevention
- IP restriction
- Device restriction and device profiling
- Geographical restriction
- Time zone restriction
- Early Malware detection and prevention

A **CASB** can be used to prevent data breaches. A CASB behaves as a guard, permitting the organisation to extend the reach of their security policies beyond their own infrastructure. A cloud access security broker is on-premises or cloud based programming that sits between cloud service clients and cloud applications, and screens all action and authorizes security policies. A CASB can offer an assortment of services, including however not constrained to monitoring user action, warning administrators about possible risky actions, upholding security policy consistence, and naturally preventing malware. According to Gartner, by 2020, 85% of large enterprises will use a cloud access security broker solution for their cloud services, which is up from less than 5% in 2015.There are many different implementations and types of Cloud Access Security Brokers (CASBs). Enterprises require sophisticated capabilities to secure their cloud footprint. A CASB should:

- Protect your entire cloud footprint, including IaaS, SaaS, and PaaS
- Provide optimal performance with no user impact
- Integrate with your existing security investments through a simple deployment

II. CASBs ARE MANDATORY FOR CLOUD

The rise of SaaS - pervasive According to Cisco Global Cloud Index reports, 58% of all cloud remaining tasks at hand will be SaaS. Indeed, even the financial services sector—since quite a while ago considered a laggard in SaaS appropriation—now utilizes SaaS for 42% of its applications. Numerous SaaS applications have constrained visibility and control choices. SaaS reception is getting to be unavoidable in enterprises, which compounds the dissatisfaction of security teams searching for visibility and control. As a primary concern the SaaS Security Gaps, this paper depict, at a high-level state, four mainstays of expected CASB usefulness: visibility, consistence, information security and threat protection

Adoption of IaaS is growing rapidly IaaS is considered the fastest-growing cloud services market. Many enterprises are moving their entire infrastructure to the cloud.

Erode in Manual Approaches The people-centric approaches won't work. In practical terms, accomplishment with this methodology is about inconceivable as a result of the time and cost related to manual forensics and the lack of skilled labor. Instead a CASB does it for you—saving time and eliminating human error. A CASB uses machine

learning and automation to provide a secure and compliant use of cloud services across multiple providers and technologies. For example, a CASB should include integration with your existing enterprise security solutions such as security information and event management (SIEM), identity as a service (IDaaS), and next generation firewalls (NGFW).

III. DATA STORAGE SECURITY SCHEMES

Different schemes that ensure security of data stored in servers are explained as follows:
In 1993, Cloud Framework Security (CFS) was presented which empowers security of information very still in the system. CFS has been accounted for in [1]. Cryptographic document systems are customized toward single-client workstations and depend on client supplied passwords for information encryption [2]. This method is not great for Cloud frameworks as Cloud frameworks include dispersed nature of system of servers where information is to be put away and these servers will be utilized by various clients. Additionally, utilization of passwords for information security is firmly precluded; on the grounds that, most regular assault on such frameworks is beast constrain assault particularly because of clients' propensity of keeping passwords basic and essential [3,4,5]. Hence this strategy is not recommended.

In [6], another scheme for dividing secret into shares and reconstructing the secret back from its shares is explained. In this scheme, additional information is added in the shares of the secret. This additional information is a message and the message is retrieved along with file (secret) on reconstructing the file (secret).
Shamir's algorithm: In 1976, a simple (k, n) threshold scheme was explained and this scheme is reported in. According to this scheme data is divided into n pieces and up to k pieces are required to get data. k-1 pieces will not reveal any information about data (secret). This scheme is based on polynomial interpolation: given k points (x_i, y_i) with distinct x such that for each x, there is one and only one polynomial q(x) of degree k-1 such that $q(x_i) = y_i$ for all i. supposes data D is a number (ASCII value). To divide it into pieces D_i, a random polynomial $a_0 + a_1 x + \ldots\ldots\ldots a_{k-1} x^{k-1}$ of k-1 degree is selected in which $a_0 = D$.

Shortcomings of this scheme are as follows:
a) Size of each piece is approximately equal to the size of data. Hence this method is space inefficient. This method does not solve the problem of vulnerability of integrity in AWS [7].
Rabin's efficient dispersal of information for security, load balancing, and fault tolerance: In [8], another scheme is explained for dividing data into pieces/shares. In this scheme, the way of dividing secret into pieces is different from [9]

Purposes of this arrangement are according to the following:
a) Size of all of the mystery is little space which makes it effective.
b) If any piece of data is adjusted during its keep focused, examination will help in making sense of which piece is changed.

Shortcomings of this arrangement are following:
a) Management and limit of secret keys.
b) Also, affirmation of the key requires learning of the secret key, however, then whoever can read the data can in like manner adjust it without being recognized.

IV. PROPOSED METHOD

To construct the security of data sent away in servers of Cloud organization suppliers and to perform destinations of this investigation, the security is proposed for Cloud Access Security Brokers (CASBs). In the proposed computation, two arrangements have been used and one of them is 'Information Dispersal figuring (IDA)'. For executing proposed work, some data is divided into the inside the shares. The usage of IDA in the proposed plan helps in guaranteeing security of information. A second course of action that has been utilized as a part of the proposed figuring is security key. Keys help in guaranteeing validity of data. This key is created by using RSA cryptography. Both the public and private keys can encode a data, the inverse key from the one used to scramble a message is utilized to decode it. This property is one motivation behind why RSA has turned into the most broadly utilized awry algorithm. The steps followed in the proposed work are as per the following:
Steps:
1. In the initial step, File (secret to be put away) or message is taken from the user.
2. In the second step, the document is divided into shares and after that encryption of the shares is performed in the third step.
3. In the fourth step, every offer of the record and its separate key from the picture is sent to various servers. The ids of the servers and names of documents containing shares of record and its particular key are put away in the Cloud Access Security Broker (CASB).
4. In request to remake the document, the client enters the record name and key from any customer

framework. These subtle elements are looked from the Cloud screen.

5. On getting the shares, 'Recreation of record or message' is executed and the document (secret) or the message is recovered using the information provided by (CASB)

6. A message is sent to client and client checks if the message got is same as the duplicate of message with him.

7. If document or message is right, then the record is conveyed to the customer.

Test Results

For the tests, certain attacks have been generated like the way attacks are performed in Cloud systems. These attacks will confirm that objectives have been achieved by the proposed information dispersal algorithm by Cloud Access Security Broker.

Recovery of Data Even If Some Number Of Servers Are Damaged

The servers attacked by hacker can vary. It can be one server or more than one server. Different attacks have been generated to verify whether the first objective of this research "Recovery of data even if some (within a limit) number of servers is damaged" has been achieved or not. As studied earlier, at least, k servers are required to reconstruct the file from its shores, two tests have been performed

For instance, we have taken sample.txt file having size of 815 bytes. We have divided the files into the shares of 200 characters each. So we get 5 shares. These shares are then encrypted using the keys. All information related to shares is maintained by Cloud Access Security Broker (CASB).

For retrieval of the sample.txt file from the servers, all the shares are concatenated after decryption. The file retrieved has the size 815 bytes. Again for retrieval of the file CASB is responsible for information related to the file.

V. RESULTS CONCLUDED FROM DIFFERENT ALGORITHMS

Comparison of the proposed algorithm with few talked algorithm

Parameters / Algorithms	Recovery of data	Integrity of data	Confidentiality of data
Shamir's Algorithm [7]	✗	✗	✓
Distributed Fingerprints and Secure Information Dispersal [8]	✓	✓	✓
A Tree Based Recursive Information Hiding Scheme [9]	✗	✓	✓
PROPOSED ALGORITHM	✓	✓	✓

According above results, In Shamir's Algorithm the data recovered is not as per saved on the server, confidentiality is maintained. Using this algorithm the integrity is violated. , In Tree Based Recursive Information Hiding Scheme the data recovered was not as saved on the server, confidentiality and integrity was maintained. In the proposed algorithm, data recovered is same as saved on the server and Integrity and confidentiality is maintained. It is important to maintain confidentiality, integrity and recovery of complete data.

VI. CONCLUSION

The cloud access security broker (CASB) can help to move to the cloud safely. It protects the cloud users, data, and apps. This paper provides a simulation tool to manage the risks in the cloud app ecosystem. It is important to develop a comprehensive information security program and train them to monitor and research anomalous activities. The proposed paper is maintaining the confidentiality, integrity and recovery of data stored in the cloud using CASB cloud service.

REFFERENCES

[1] M. E. Smid and D. K. Branstad, "The data encryption standard: Past and future," Proc. IEEE, vol. 76, no. 5, pp. 550-559, May 1988

[2] Emily Maltby, "Small companies look to Cloud for savings in 2011," http://online.wsj.com/article/SB10001424052970203513204576047972349898048.html, December 29, 2010.

[3] Lenk, M. Klems, J. Nimis, S. Tai, F. Karlsruhe, and T. Sandholm, "What's Inside the Cloud? An Architectural Map of the Cloud Landscape," in Proc. of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, IEEE Computer Society, pp. 23–31, 2009.

[4] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "A View of Cloud computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[5] [John, "Top 10 Enterprises in the Cloud," http://www.johnmwillis.com/other/top-10-entperises-in-the-Cloud/, Jul. 13, 2008.

[6] "Google App Engine," http://en.wikipedia.org/wiki/Google_App_Engine.

[7] Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612-613, 1979.

[8] H. Krawczyk, "Distributed Fingerprints and Secure Information Dispersal," in Proceedings of the 12th annual ACM symposium on Principles of distributed computing, 1993

[9] Parakh, A. and Kak, S. 2010 "A Tree Based Recursive Information Hiding Scheme" proceedings of IEEE ICC 2010 – Communication and Information System Security Symposium (ICC"10 CISS"), May 23-27, Cape Town, South Africa.

[10] Gartner: The Growing Importance of Cloud Access Security Brokers - http://www.computerweekly.com/news/2240223323/Cloud-access-brokers-top-security-technology-says-Gartner

[11] Gartner: Emerging Technology Analysis: Cloud Access Security Brokers - http://www.ciphercloud.com/2014/09/30/public-cloud-security-demands-cloud-access-security-broker-casb/

[12] https://www.netskope.com

[13] Medina, A. Lakhina, I. Matta, and J. Byers, "BRITE: An Approach to Universal Topology Generation," in Proc. of MASCOTS '01, August 2001.
[14] Bitglass: The Definitive Guide to Cloud Access Security Brokers
[15] CipherCloud looks to stay at the head of the cloud security class
[16] Ciphercloud: 10 Minute Guide to Cloud Encryption Gateways
[17] Ciphercloud: Cloud Adoption & Risk Report in North America & Europe – 2014 Trends
[18] NetworkWorld: How the cloud is changing the security game
[19] Adallom: The Case For A Cloud Access Security Broker
[20] Adallom: Cloud Risk Report Nov 2014
[21] Check Point Capsule and Adallom Integration
[22] HP - Adallom: Proven Cloud Access Security Protection Platform
[23] Adallom : to Offer Comprehensive Cloud Security Solution for Businesses With HP
[24] PingOne - Skyhigh: PingOne & Skyhigh Cloud Security Manager
[25] ManagedMethods: Role of Enterprise Cloud Access Security Broker
[26] Standing at the Crossroads: Employee Use of Cloud Storage.
[27] Cloud Computing: Security Threats and Tools
[28] SC Magazine: Most cloud applications in use are not sanctioned

★★★