IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

Issues and Challenges In Reducing Data Breaches in Cloud Architecture

Savrabh Kumar Sharma[1*] and Rajneesh Singh[2]

[1] Department of computer science, IEC College of Engineering and Technology, Greater Noida (U.P.) India
[2] Department of computer science, IEC College of Engineering and Technology, Greater Noida (U.P.) India

[*]*Corresponding Author: saurabh416817@gmail.com, Tel.: +011 9711958209*

Available online at: www.ijcseonline.org

Accepted: 10/Jun/2018, Published: 30/Jun/2018

Abstract -Cloud computing has increased awesome consideration from industry yet there are numerous issues that are in their primitive stage which is hampering the development of Cloud. One of these issues is security of information put away in the servers of data centres of Cloud specialist organizations. Numerous plans have been produced till date for guaranteeing security of information in Distributed Systems. Many strategies have been contemplated; dissected and new technique has been proposed which infix the parameters of security like confidentiality of data, recovery of data and uprightness of information to such an extent that it guarantees security of information put away in the servers of Cloud frameworks. This paper examines the imperative research and troubles that presents data breach in Cloud computing and gives best practices to specialist organizations and moreover attempts intend to impact cloud servers to upgrade their fundamental problems in this genuine monetary situation.

Keywords— Cloud Computing, Data Breach, Distributes System, Data Security

I. INTRODUCTION

The Data Beach is a situation in which delicate, classified or generally ensured data has been gotten to and used in an unapproved form. It is an occurrence of stealing, viewing, copying and transmitting the confidential, protected and sensitive data by gaining unauthorized access to the system [1, 2]. This paper is relating to Cloud computing, distinctive cloud models and essential security dangers and information break issues that are at the present time investigating in the cloud computing structure. The proposed work is based on two strategies – Information Dispersal Algorithm and Fingerprinting to reduce data breaches in cloud architecture. Information dispersal algorithm helps in keeping up confidentiality and security of information and Fingerprinting helps in recovery of data the original data. The property of proposed algorithm that makes it not the same as existing data storage schemes is that security is ensure. This property may help in picking up trust of clients.

II. RELATED WORK

Reducing Security Breaches In Cloud Computing Networks

The Cloud security must be a part of any organization's general security procedure. Decreasing security breaches in cloud computing systems requires arranging and technique to be effective. Organizations need to dedicate the same amount of vitality toward securing their cloud as they do securing their server farm, structures, individuals, and data.

Security dangers, dangers, and breaches can come in such a large number of structures and from such a significant number of spots that numerous organizations adopt a far reaching strategy to security administration. Numerous organizations will centre around the expansive scope of potential vulnerabilities to its server farm and additionally approaches to shield touchy corporate, client, and accomplice data, incorporating utilizing worked in applications and information level securities. Indeed, even with all that, it's not generally enough.

When all is said in done, take after these means to lessen the danger of affliction security breaches:

1. Authenticate all individuals getting to the system.
2. Frame all entrance authorizations so clients approach just to the applications and information that they've been conceded particular consent to get to.
3. Authenticate all product running on any PC — and all progressions to such programming. This incorporates programming or administrations running in the cloud. Your cloud supplier needs to mechanize and confirm programming patches and design changes, and additionally oversee security fixes proactively. All things considered, numerous administration blackouts originate from setup botches.

4. Formalize the way toward asking for authorization to get to information or applications. This applies to your own particular inward frameworks and the administrations that expect you to put your information into the cloud.
5. Monitor all system movement and log all bizarre action. Send interloper discovery innovation. Regardless of whether your cloud administrations supplier empowers you to screen exercises on its condition, you ought to have a free view. Notwithstanding when cloud administrators have great security (physical, organize, OS, application foundation), it is your organization's obligation to ensure and secure your applications and data.
6. Log all client movement and program action and examine it for unforeseen conduct. Almost 70 percent of security breaks are caused by insiders (or by individuals getting assistance from insiders). Insiders once in a while get captured.
7. Encrypt, up to the point of utilization, every profitable datum that necessities additional insurance.

Regularly check the system for vulnerabilities in all product presented to the Internet or any outside clients.

DATE STORAGE SECURITY SCHEMES

To Different schemes that ensure security of data stored in servers are explained as follows:

In 1993, CFS was presented which empowers security of information very still in the system. CFS has been accounted for in [3]. Cryptographic document systems is customized toward single-client workstations and depend on client supplied passwords for information encryption [4]. 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 [10,11,12]. Hence this strategy is not recommended.

In [5], 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. Suppose 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:

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 [6].

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 [7].

Purposes of this arrangement are according to the following:

a) Size of all of the mystery is little which makes it space 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:

Management and limit of secret keys. 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.

III METHODOLOGY, RESULTS AND DISCUSSION

Organization suppliers and to perform destinations of this investigation, the security is proposed. 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 joined inside the shares of exceptional question. For execution of IDA in the proposed tally, extra data to be consolidated is a message. The usage of IDA in the proposed plan helps in guaranteeing riddle and openness of information. Second course of action that has been utilized as a part of the proposed figuring is key time. Keys help in guaranteeing validity of data. This key is created by using RSA cryptography. Both public and the 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 calculation are as per the following:
Steps

1. In the initial step, File (secret to be put away) or message is taken from user. Duplicate of message is still spared with client.
2. In second step, for guaranteeing information stockpiling security, preparing of information happens. This incorporates part of document into shares and after that unscrambling of shares is performed in third step.
3. In fourth step, every offer of the record and its separate key from 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 Monitor
4. In request to remake the document, 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' calculation is executed and the document (secret) or the message is recovered.
6. Message is sent to client and client checks if message got is same as the duplicate of message with him.
7. If document or message is right, then record is conveyed to customer.

Message is again rechecked to guarantee in the event that it is same as what the client sent.

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 algorithm.

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 first objective of this research "Recovery of data even if some (within a limit) number of servers are damaged" has been achieved or not. As studied earlier, at least, k servers are required to reconstruct the file from its shares, 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.

For retrieval of the map.txt file from the servers, all the shares are concatenated after decryption. The file retrieved has the size 815 bytes.

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 is not as saved on the server, confidentiality and integrity is 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.

IV CONCLUSION AND FUTURE SCOPE

This paper portrays the utilization of data apportioning plan called Information dispersal for actualizing such security. The chunks of data after encryption are put away on the servers. Cloud information stockpiling has numerous focal points.

Cloud data stockpiling however has a few noteworthy downsides, including execution, accessibility, contradictory interfaces and absence of gauges. Be that as it may, this work is giving an interface to secure record stockpiling and additionally recovery from any framework. This image based recursive data storage plan is free of equipment and programming.

In this work, servers are picked in the system and used to store the chunks of encrypted data. Data reproduction obliges access to every server, and the learning of the servers on which the information or data are put away. This plan may likewise be utilized for data security as a part of sensor systems and web voting conventions, in armed force for sending private information's.

REFERENCES

[1] D Zissis, D Lekkas. Addressing cloud computing security issues. Future Generation computer systems. 583-92, 2012.

[2] M Ali, SU Khan, AV Vasilakos. Security in cloud computing: Opportunities and challenges. Information sciences. vol1, no305, pg,357-83, 2015.

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

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

[5] J. Feng, Y. Chen, P. Liu, "Bridging the missing link of Cloud data storage security in AWS," Proc. IEEE 7th Consumer Communications and Networking Conference (CCNC 2010), pp. 1-2, Jan. 2010, doi: 10.1109/CCNC.2010.5421770.

[6] "What is AWS?," *http://aws.amazon.com/what-is-aws/*

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

[8] M. O. Rabin, "Efficient dispersal of information for security, load balancing and fault tolerance," Journal of the ACM, vol. 36, no. 2, pp. 335-348,1989

[9] M. O. Rabin, "Fingerprinting by random polynomials," Report TR-15-81, Center for Research in Computing Technology, Harvard University, 1981.

[10] R. Pletka, C. Cachin, "Cryptographic security for a high-performance distributed file system," IBM Research, Technical report, Sept. 2006.

[11] E. Gheringer, "Choosing passwords: security and human factors," Proc. of IEEE 90, pp. 369–373, 2000.

[12] R. Proctor, M. Lien, K. Vu, G. Salvendy, "Improving computer security for authentication of users: influence of proactive password restrictions, Behavior Research Methods," Instruments and Computers 34, pp.163–169, 200

Authors Profile

Mr Savrabh Kumar Sharma pursed Bachelor of Science from Gauttam Buddha Technical University in 2012. He is currently pursuing M-Tech in Computer Science from IEC College of Engineering and Technology, Greater Noida (U.P.) India

Mr. Rajneesh Shing pursed Bachelor of Science from Guru Gobind Singh University 2 and Master of Technology from Gautam Buddha University in year 2006. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computational Sciences, in IEC College of Engineering and Technology, Greater Noida (U.P.) India.

