A Review on Various Approaches for Security of Data on Cloud Environment

Amandeep Kaur
PG Research Scholar, Department of CSE
Punjabi University Regional Centre, Mohali, Punjab

Navpreet Kaur
Assistant Professor, Department of CSE
Punjabi University Regional Centre, Mohali, Punjab

ABSTRACT

Cloud computing has grabbed the spotlight within some time span. The cloud computing trend is increasing rapidly so to implement it into an organization we need to observe the threats of cloud computing. At an unusual pace it has turned the face of government and business and has created some new challenges. However developers have created new vulnerabilities, including security issues whose full impressions are still rising. This paper presents an overview and study of cloud computing, with several security threats, security issues, currently used cloud technologies and security solutions [3].

Keywords:

Cloud Security;Encryption Algorithm; Fully Homomorphic Encryption

1. INTRODUCTION

1.1 Cloud

The term cloud is analogical to internet. The term cloud computing is based on cloud drawings used in past to represent telephone networks. Cloud computing involves deploying groups of remote servers and software networks that allow different kinds of data sources be uploaded for real time processing to generate computing results without the need to store processed data on the cloud. Clouds can be classified as public, private or hybrid. Thus, users can concentrate more on their core business processes rather than spending time and gaining knowledge on resources needed to manage their business processes [5].

1.2 Way to Use The Cloud

The cloud makes it feasible for you to get to your data from anyplace whenever. While a conventional PC setup obliges you to be in the same area as your information stockpiling gadget, the cloud makes away that stride. The cloud evacuates the requirement for you to be in the same physical area as the equipment that stores your information. Your cloud supplier can both own and house the equipment and programming important to maintain your home or business applications. This is particularly useful for organizations that can't manage the cost of the same measure of equipment and storage room as a greater organization. Little organizations can store their data in the cloud, uprooting the expense of acquiring and putting away memory gadgets [6].

1.3 Types of Clouds [8]

There are distinctive sorts of mists that you can subscribe to relying upon your needs. As a home client or little entrepreneur, you will in all probability use open cloud administrations.

1.3.1 Public Cloud - An open cloud can be gotten to by any supporter with a web association and access to the cloud space.

1.3.2. Private Cloud - A private cloud is secured for a particular gathering or association and limits access to simply that gathering**.**

1.3.3. Community Cloud - A group cloud is imparted among two or more associations that have comparative cloud prerequisites.

1.3.4. Hybrid Cloud - A cross breed cloud is basically a blend of no less than two mists, where the mists included are a mixture of open, private, or group.

1.4 Choosing a Cloud Provider

Every supplier serves a particular capacity, giving clients pretty much control over their cloud relying upon the sort. When you pick a supplier, contrast your needs with the cloud administrations accessible. Your cloud needs will shift relying upon how you expect to utilize the space and assets connected with the cloud. On the off chance that you need to utilize it at home then you require an alternate cloud sort [9].

1.4.1Software as a Service - **A** SaaS supplier gives supporters access to both assets and applications. SAAS makes it pointless for you to have a physical duplicate of programming to introduce on your gadgets. SaaS likewise makes it less demanding to have the same programming on the majority of your gadgets on the double by getting to it on the cloud. In a SaaS understanding, you have the minimum control over the cloud.

1.4.2Platform as a Service - A PaaS framework goes a level over the Software as a Service setup. A PaaS supplier gives supporters access to the segments that they require to create and work applications over the web.

1.4.3Infrastructure as a Service - An IaaS understanding, as the name states, bargains principally with computational foundation. In an IaaS understanding, the supporter totally outsources the capacity and assets, for example, equipment and programming that they require. As you go down the rundown from number one to number three, the supporter increases more control over what they can do inside the space of the cloud [11].

1.5 Security

The data housed on the cloud is regularly seen as profitable to people with vindictive expectation. There is a ton of individual data and possibly secure information that individuals store on their PC s, and this data is presently being exchanged to the cloud. This makes it basic for you to comprehend the efforts to establish safety that your cloud supplier has set up, and it is similarly vital to take individual insurances to secure your information. The principal thing you must investigate is the efforts to establish safety that your cloud supplier as of now has set up. These change from supplier to supplier and among the different sorts of mists.

What encryption routines do the suppliers have set up? What strategies for assurance do they have set up for the genuine equipment that your information will be put away on? Will they have reinforcements of my information? Do they have firewalls set up? On the off chance that you have a group cloud, what hindrances are set up to keep your data separate from different organizations? Numerous cloud suppliers have standard terms and conditions that may answer these inquiries; however the home client will likely have little transaction room in their cloud contract [14].

1.6 CHALLENGES

The accompanying are a portion of the striking difficulties connected with distributed computing, and albeit some of these may bring about a lull when conveying more administrations in the cloud, most additionally can give opportunities, if determined with due consideration and consideration in the arranging stages.

1.6.1Security and Privacy — maybe two of the more "hot catch" issues encompassing distributed computing identify with putting away and securing information, and observing the utilization of the cloud by the administration suppliers. These issues are for the most part credited to abating the arrangement of cloud administrations. These difficulties can be tended to, for instance, by putting away the data inward to the association, yet permitting it to be utilized as a part of the cloud [13].

1.6.2Lack of Standards — Clouds have archived interfaces; nonetheless, no norms are connected with these, and accordingly it is improbable that most mists will be interoperable.

1.6.3Continuously Evolving — User prerequisites are persistently developing, similar to the necessities for interfaces, systems administration, and capacity. This implies that a "cloud," particularly an open one, does not stay static and is additionally constantly developing.

1.6.4Compliance Concerns — The Sarbanes-Oxley Act (SOX) in the US and Data Protection orders in the EU are only two among numerous agreeability issues influencing distributed computing, taking into account the sort of information and application for which the cloud is being utilize [17].

1.7 BENEFITS

The accompanying are a percentage of the conceivable advantages for the individuals who offer distributed computing based administrations and applications:

1.7.1Cost Savings — Companies can diminish their capital uses and utilization operational consumptions for expanding their processing capacities. This is a lower boundary to passage furthermore requires less in-house IT assets to give framework support.

1.7.2Scalability/Flexibility — Companies can begin with a little sending and develop to a huge arrangement reasonably quickly, and after that scale back if important. Likewise, the adaptability of distributed computing permits organizations to utilize additional assets at crest times, empowering them to fulfill buyer requests.

1.7.3Reliability — Services utilizing different repetitive locales can bolster business coherence and debacle recuperation.

1.7.4Maintenance — Cloud administration suppliers do the framework support, and access is through APIs that don't oblige application establishments onto PCs, subsequently further diminishing upkeep prerequisites.

1.7.5Mobile Accessible — Mobile specialists have expanded benefit because of frameworks open in a base accessible from anyone [16].

2. ENCRYPTION ALGORITHMS

Different types of algorithms are explained as follows:-

2.1 Data Encrytion Algorithm

This is a block cipher symmetric algorithm that uses same key for both encryption and decryption. The basic building block (a substitution followed by a permutation) is called a round and is repeated for 16 times.

The substitutions process depends on the S-Box. S-Box is a matrix of 4 rows and 16 columns. DES has 8 different S-Boxes in each round. S-Box is used to map the input code to another code to the output. The input code specifies the output code position in this S-Box. The first and last bits specify the row number, and the rest bits specify the column number. The permutation tables are used for changing the bit-orders in the packet. For each DES round, a sub-key is derived from the original key using an algorithm called key schedule.

2.2 ADVANCED ENCRYTION STANDARD

AES algorithm is a symmetric block. It is used to encrypt and decrypt the plaintext and cipher text of 128-bits respectively by using cryptographic keys of 128-bits (AES-128), 192-bits (AES-192), or 256-bits (AES-256). The number of rounds in the encryption or decryption processes depends on the key size.

2.3 RC6 ALGORITHM

RC6 is more accurately specified as RC6-w/r/b where the word size is w bits, encryption consists of a nonnegative number of rounds r, and b denotes the length of the encryption key in bytes. Since the AES submission is targeted at w = 32 and r = 20, RC6 shall be used as shorthand to refer to such versions. When any other value of w or r is intended in the text, the parameter values are specified as RC6-w/r. Of particular relevance to the AES effort is the versions of RC6 with 16-, 24-, and 32-byte keys. The complexity of the algorithm and the key size enhance the data security in WLAN, and they increase the difficulty to the attackers to discover the original message.

2.4 HOMOMORPHIC ENCRYPTION

Homomorphic fundamentally means having "same roots" or "same structure". In this idea information can be encoded without offering the mystery key expected to unscramble the information. The significant issue in utilizing the cloud based administrations is security. Cloud clients particularly in government segments are truly extremely frightened of losing their information. On the off chance that you need to impart encryption methods you have to impart decoding key on the cloud also. This causes the security issues. Yet this issue is tackled with the assistance of homomorphic encryption.But since of a few constraints it is not thought to be useful. In the event that a functional, completely homomorphic arrangement can be made, it could be the impetus that separates the security hindrance to far reaching cloud selection. There are two sorts of homomorphic encryption:

1. Fully homomorphic encryption (FHE)

2. Semi homomorphic encryption (SHE).

FHE permits boundless calculations on information to be scrambled. SHE backings predetermined number of operation to be connected on encoded information. One of the blocks in FHE is commotion. Clamor for this situation is twisting in figure content. This issue is overcome utilizing bootstrapping as a part of SHE arrangements. Bootstrapping changes a SHE arrangement so it can homomorphically run its own decoding method by including an encryption of the mystery key to general society key. This is refined by utilizing an inadequate subset-total issue (SSSP) or increasing the general population key with a substantial arrangement of vectors so that a meager subset of the vectors will mean be the mystery key. Bootstrapping procedure includes another layer of encryption utilizing encryption key to open the internal layer of scrambling. This additional layer expands the general computational exertion expected to finish the inquiry. FHE arrangements are premise on perfect cross sections. Perfect grids are essentially helpful in cryptography. Cross sections are utilized on the grounds that they have basic unscrambling calculations which could diminish the computational overhead connected with bootstrapping SHEs. Subsequently, they are secure by the assaults.

3. CONCLUSION

The cloud gives numerous alternatives to the ordinary PC client and additionally expansive and little organizations. It opens up the universe of registering to a more extensive scope of employments and builds the usability by giving access through any web association. In any case, without breaking a sweat additionally come disadvantages. You have less control over who has admittance to your data and practically zero information of where it is put away. You likewise must be mindful of the security dangers of having information put away on the cloud. The cloud is a huge focus for malignant people and may have impediments on the grounds that it can be gotten to through an unsecured web association. In the event that you are considering utilizing the cloud, be sure that you distinguish what data you will be placing out in the cloud, which will have admittance to that data, and what you will need to verify it is ensured. Also, know your choices regarding what kind of cloud will be best for your needs, what sort of supplier will be most helpful to you, and what the notoriety and obligations of the suppliers you are considering are before you sign up. This work can also be done with other encryption schemes.

4. REFERENCES

[1] Sharma, Rajeev, and Bright Keswani. "study& analysis of cloud based erp services." Communication Software and Networks (ICCSN), 2011, PP 468 – 471.

[2] Juneja, Gurpreet K. "Use of Modeling Language to deploy applications in clouds." International workshop on Maintenance and Evolution of Service-Oriented and Cloud-Based Systems (MESOCA), 2012, pp 58 - 59

[3] DHIWAR, KAMLESH KUMAR. "aspect of cloud computing", IEEE Conf. on Software, Telecommunications and Computer Networks (SoftCOM), 2014, pp 192 – 200.

[4] Akintomide, O. A. "Cloud computing: The third revolution in IT." Library Progress (International) 33.1 (2013): 77-94.

[5] Mell, Peter, and Timothy Grance. "The NIST definition of cloud computing (draft)." NIST special publication 800.145 (2011): 7.

[6] Pearson, Siani, Yun Shen, and Miranda Mowbray "A privacy manager for cloud computing" Cloud Computing. Springer Berlin Heidelberg, 2009, pp. 90-106.

[7] T OGRAPH, B., and Y. RICHARD MORGENS.

[8] "Cloud computing" Communications of the ACM 51.7 (2008).

[9] Velte, Toby, Anthony Velte, and Robert Elsenpeter. Cloud computing, a practical approach. McGraw-Hill, Inc., 2009.

[10] Marinos, Alexandros, and Gerard Briscoe. "Community cloud computing."Cloud Computing. Springer Berlin Heidelberg, 2009, pp 472-484

[11] Zhang, Qi, Lu Cheng, and Raouf Boutaba. "Cloud computing: state-of-the-art and research challenges." Journal of internet services and applications 1.1 (2010), pp 7-18.

[12] Qian, Ling, et al. "Cloud computing: An overview." Cloud Computing. Springer Berlin Heidelberg, 2009. Pp 626-631.

[13] Leavitt, Neal. "Is cloud computing really ready for prime time" Growth 27.5 (2009).

[14] Voorsluys, William, James Broberg, and Rajkumar Buyya. "Introduction to cloud computing." Cloud Computing (2011), pp 1-41.

[15] Wang, Lizhe, et al. "Cloud computing: a perspective study." New Generation Computing 28.2 (2010), pp 137-146.

[16] Santos, Nuno, Krishna P. Gummadi, and Rodrigo Rodrigues. "Towards trusted cloud computing." Proceedings of the 2009 conference on hot topics in cloud computing, pp 2009.

[17] Chen, Quan, and Qianni Deng. "Cloud computing and its key techniques"Journal of Computer Applications 29.9 (2009), pp 2565.

[18] Zhang, Liang-Jie, and Qun Zhou. "CCOA: Cloud computing open architecture "Web Services, 2009. ICWS IEEE International Conference on IEEE, 2009.