INTERNATIONAL JOURNAL OF RESEARCH IN SCIENCE & TECHNOLOGY

e-ISSN:2249-0604; p-ISSN: 2454-180X

Leveraging the 'Dual Layer' in Enhancing the Data Security Safeguards in Cloud Environment

Anoushka Gupta

Step by Step, Noida

Paper Received: 10th May, 2021; **Paper Accepted:** 04th June, 2021;
Paper Published: 25th June, 2021

DOI: http://doi.org/10.37648/ijrst.v11i02.004

How to cite the article:

Anoushka Gupta, Leveraging the Dual Layer in Enhancing the Data Security Safeguards in Cloud Environment, IJRST, Apr-Jun 2021, Vol 11, Issue 2, 36-42, DOI: http://doi.org/10.37648/ijrst.v11i02.004

ABSTRACT

One of the significant benefits of distributed computing is dividing information between different organizations. Notwithstanding, this benefit itself has a danger to information. It is important to ensure communication to refute likely risks to the data. Encryption is a tremendously powerful instrument concerning securing information. This paper proposes another span of cryptographic double-layer encryption to make the information put away in the cloud safer and dependable. There are promptly accessible numerous different encryption methods accessible at present; however incapable of giving adequate security. This paper intends to propose a new encryption strategy named double encryption. It depends on the well-known encryption analysis, ais a symmetric-key study. We will offer an extra layer of rabbit calculation around encoded information, which will assist with giving greater protection from Brute force and one more sort of attack. Assuming that an interloper recognizes a solitary key of the cryptosystem, it isn't easy to unscramble the first message. This paper plans to recommend a viewpoint that is a twofold layer encryption technique to guarantee security in the cloud. This proposed twofold layer encryption will acquire the information while securing and participating in a cloud environment. This plan utilizes the incredible handling expertise of distributed computing and can proficiently guarantee cloud information protection and security.

1. INTRODUCTION

The information is moved between the server and the customer in the cloud. Fast is the indication of administration; cryptography offers various choices to exchange data from the cloud and house it inside. Information encryption is a security method where data is encoded and must be gotten to or decoded by a client with the right encryption key. Encoded information, likewise called ciphertext, seems mixed or incoherent to an individual or substance without consent. Information Encryption is utilized to shield malevolent gatherings from getting to touchy information. A significant line of protection in Cyber security engineering, encryption makes involving caught information as troublesome as expected.

A. Symmetric Encryption

Symmetric encryption is an old and notable system that utilizes a solitary key to scramble (encode) and unscramble (interpret) information. The mysterious key can be a word, a number, or a series of letters applied to a message. Source and beneficiary know the key, and they can code and interpret any message that would utilize that particular key.

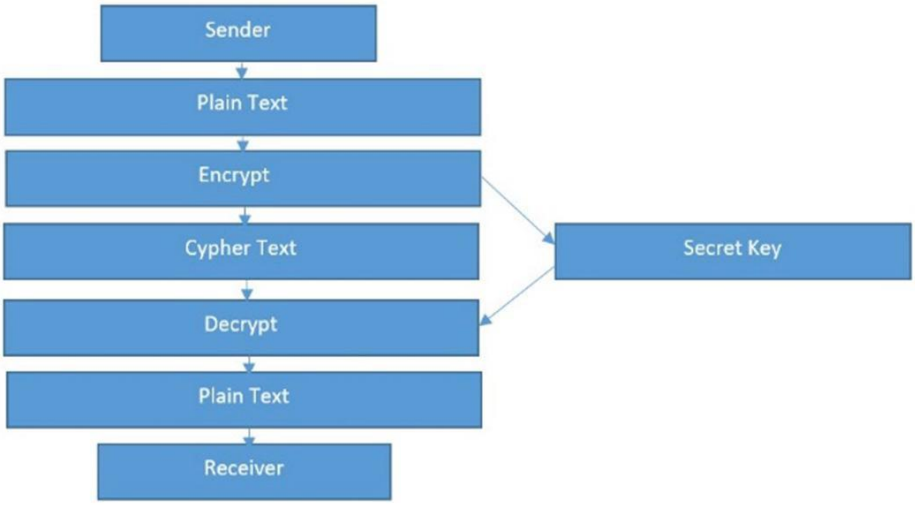


Fig.1: Fundamental cryptographic process

A straightforward illustration of an encryption calculation would be changing all N to a 3 or all Z to a 1. The routine might play out a few passes and changes, known as stages, on the plaintext. Whenever it's scrambled, you will require a key to open it. There are loads of various symmetric key calculations accessible. Each has its qualities and shortcomings. More normal models are RC4, 3DES, DES, and RC5. Just symmetric encryption has the speed and computational effectiveness in dealing with a huge volume of information encryption.

2. INFORMATION SECURITY IN CLOUD COMPUTING

This paper will examine diverse security strategies for information stockpiling security and protection assurances in the distributed computing climate. This paper concerns the method utilized in distributed computing through information security perspectives, including information trustworthiness, privacy, and accessibility. Likewise, information protection issues and advances in the cloud are examined because information security is related to information security. Studies on information protection and security could assist with upgrading the client's trust by getting information in the distributed computing climate.

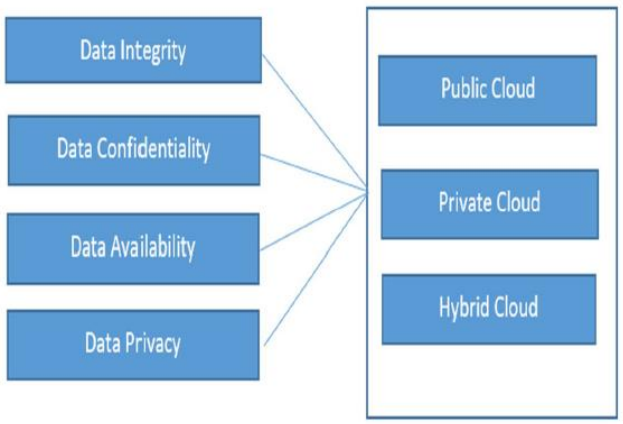


Fig2: Data privacy and security in cloud

A. Information Integrity

Data uprightness is one of the fundamental parts in any information structure. All things considered, data decency infers getting data from unapproved creation, undoing to ensure that significant data and organizations are not mistreated, manhandled, or taken. Data dependability is cultivated in an autonomous system with a singular informational index. Data dependability in the free system is stayed aware of through informational collection prerequisites and trades, for the most part wrapped up by an informational collection organization structure (DBMS). Data set should follow ACID properties to ensure data honesty. A considerable lot of the data bases support ACID trades and stay aware of data uprightness.

B. Information Confidentiality

Information classification is huge for clients to store their private information in the cloud. Confirmation and access control procedures are utilized to guarantee information privacy. Expanding cloud dependability and reliability can address information classification, verification, and access control issues in distributed computing.

C. Information Availability

At the point when mishaps, for example, hard plate harm, IDC fire, and organization disappointments happened, the degree that clients' information can be utilized or recuperated and how the clients confirm their information by strategies rather than relying upon the credit ensure by the cloud specialist co-op alone.

D. Information Privacy

In the cloud, protection implies when clients visit the delicate information, the cloud administrations can keep a likely foe from deriving the client's conduct by the client's visit model (not immediate information spillage). Scientists have zeroed in on Oblivious RAM (ORAM) innovation. Unaware RAM innovation visits the vast majority of the duplicates of information to conceal the genuine visiting points of clients. ORAM has been broadly utilized in programming assurance and has been used in ensuring protection in the cloud as a promising innovation

3. PROPOSED METHOD

This paper's fundamental motivation is to propose new encryption innovation as a blend of AES and Rabbit calculations. Prior various combinations are utilized of RSA, AES and HMAC. Dissimilar to this mix, we will use a combination of the rabbit calculation and the AES calculation.

A. Rabbit Algorithm

Rabbit calculation is likewise called a stream figure calculation that has been intended for elite execution in programming executions.

Rabbit comprises a pseudo-arbitrary piece stream generator that takes a 128-digit key and a 64-cycle introduction vector (IV) as info and produces a flood of 128-bit blocks. Encryption is performed by joining this result with the message, utilizing the elite OR activity. Decoding is led similarly to encryption. Both key arrangement and encryption are extremely quick, making the calculation especially appropriate for all applications where should scramble a lot of information.

B. AES Algorithm

Regarding network protection, AES is one of those abbreviations springing up all over the place. That is because it is not difficult to execute and has turned into the widespread acknowledgement of encryption, and it is utilized to keep a lot of our correspondences safe.

The highlights of AES are as per the following −

1) Symmetric key symmetric square code

2) 128-cycle information, 128/192/256-digit keys

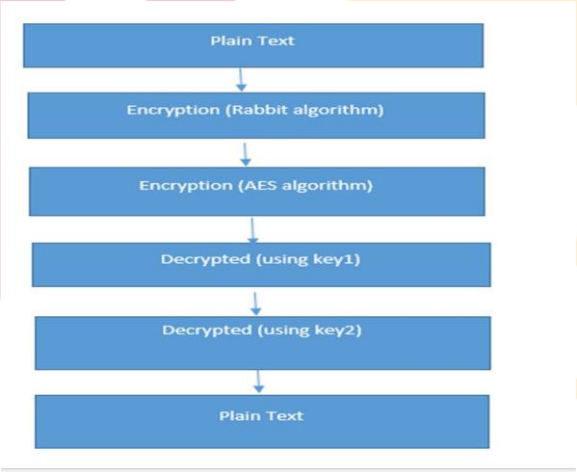
3) Stronger and quicker

C. Activity of AES

AES is an iterative code that is superior to the Feistel figure. It depends on replacement change organization'. It contains a progression of related activities, some including replacements and others including stages. AES plays out the entirety of its

calculations on bytes. That is why AES handles the 128 pieces of a plaintext block as 16 bytes. These 16 bytes are organized into four segments and four columns for operating as a framework.

Not in the slightest degree like DS, the number of rounds in AES is variable and depends upon the length of the key. For 128-cycle keys, AES includes 10 rounds and 12 rounds for 192-piece keys and 14 rounds for 256-bit keys. The main not really settled another 128-cycle round key used in each round. At the point when Sender sends the information as a plain message, it creates a (private key) using rabbit calculation and will change over it into ciphertext. This will be the main layer of encryption.



The second layer of encryption will change information over ciphertext utilizing (public key) AES calculation. Using these over two counts, information will be safer during transmission.

4. CONCLUSION

Increasing usage of distributed computing for putting away information surely improves the methods of putting away information in the cloud. Information accessible in the cloud can be in danger if not ensured in an advocated way. This paper discussed the risks and security dangers to data in the cloud and outlined double-layer information encryption procedures. One of the main issues of this paper was information security and giving its dangers answers for its dangers in distributed computing. This paper examines the double layer encryption procedure, which is effective for scrambling the information in the cloud. The review gave an outline of the Rabbit calculation and AES calculation, which are utilized for encoding the cloud information.

REFERENCES

[1] Biswajita Datta, Akash Roy, Romit Dutta, Samir Kumar Bandyopadhyay "Secure Communication

through Double Layer Security with Efficient Key Transmission" 2018 International Conference on Information Technology (ICIT) (IEEE)

[2] Dr. D.Usha, M. Subbbulakshmi "Double Layer Encryption Algorithm Key Cryptography for Secure Data Sharing in Cloud" International Journal of Scientific & Engineering Research Volume 9, Issue 5, May-2018

[3] Shivani Chauhan, Jyotsna, Janmejai Kumar, Amit Doegar "Multiple layer Text security using Variable block size Cryptography and Image Steganography" 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017)

[4] Gahan A V, Geetha D Devanagavi "An Empirical Study of Security Issues In Encryption Techniques" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 5 (2019)

[5] Ashok Kumar, Santhosha, A.Jagan "Two layer Security for data storage in cloud" 2015 1st International conference on futuristic trend in computational analysis and knowledge management (ABLAZE 2015)

[6] Naveen N, K.Thippeswamy "Security and Privacy Challenges Using Multi-Layer Encryption Approaches In Cloud Computing Environments" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8 June, 2019

[7] Afnan Ullah Khan, Manuel Oriol, Mariam Kiran, Ming Jiang, Karim Djemame "Security Risks and their Management in Cloud Computing" 2012 IEEE 4th International Conference on Cloud Computing Technology and Science

[8] F.Sabahi, "Virtualization-level security in cloud computing," 3rd Int. 2011 IEEE Conf. Commun. Softw. Networks, pp. 250–254, 2011

[9] D. Descher, M., Masser, P., Feilhauer. and Huemer, and A. Klein "Retaining data control to the client in infrastructure clouds," Int. Conf. Availability, Reliab. Secur. (pp. 9-16). IEEE., pp. pp. 9–16, 2009.

[10] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013.

[11] C. Modi, D. Patel, B. Borisaniya, M. Rajarajan, and A. Patel "A survey on security issues and solutions at different layers of Cloud computing," J.Supercomputer., vol. 63, no. 2, pp. 561–592, 2013.

[12] L. Rodero-Merino, L. M. Vaquero, E. Caron, F. Desprez, and A. Muresan, "Building safe PaaS clouds: A survey on security in multitenant software platforms," Comput. Secur., vol. 31, no. 1, pp. 96–108, 2012.

[13] E. Mohamed, "Enhance data secure model for cloud computing," Informatics Syst. (INFOS), 2012 8th Int. Conf., pp. 12–17, 2012

[14] J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," Build. Infrastruct. Cloud Secure., vol. 1, no. September 2011, pp. 3–22, 2014.

[15] P. S. Wooley, "Identifying Cloud Computing Security Risks," Contin. Educ., vol. 1277, no. February, 2011.

[16] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, Jan. 2011.