International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 02 | Feb 2020 www.irjet.net p-ISSN: 2395-0072

DATA SECURITY IN CLOUD COMPUTING USING HOMOMORPHIC ALGORITHAM

Amruta Patil[1], Apurva Kirve[2], Sayali Nandeshwar[3], Swati Taru[4]

[1,2,3,4]*Dept. of Information Technology, Zeal College of Engineering Research, Narhe, Pune, 411041*

ABSTRACT: *The framework of cloud computing receiving a good deal of attention each in publication and different users. Cloud computing is that the system of computing solution over the web. Cloud computing services enable people and businesses to use hardware and computer code technique that area unit control by cloud suppliers at remote locations. The space between the user and therefore the physical location of his information creates a stopper as a result of this information is accessed by a 3rd party and this is able to have an effect on the privacy of user information. The mistreatment of ancient secret writing schemes to encipher the remoted information before transfer to the cloud supplier has been most generally used system to bridge this security tittle-tattle. But, the user can got to give the non-public key to the server to decode the info before perform the action needed. Homomorphic secret writing use to execute computations on encrypted information while not coding. The need of homomorphic secret writing to encipher the user information in cloud server and conjointly it'll be accustomed execute needed perform on this encrypted file or information.*

Keywords: *cloud computing, Homomorphic encryption, Key generation, OTP.*

1. INTRODUCTION:

Cloud Computing has seem as a vital paradigm that has attract tidy attention in each business and world. Cloud Computing have totally different names referred to as as "outsourcing" and "server hosting." however the less action taken by the processors used, fine net connections and therefore the enthusiastically prices of the substances used, don't enable the employment of facility and storage areas. However, current advances in resent technology via virtualization paved the method for these functions with quicker process.

Cloud Computing security challenges associated it's additionally a drawback to several researchers; very first thing was to specialize in security that is that the biggest entity of organizations that area unit considering a proceed to the cloud. The employment of cloud computing guide loads of benefits together with decreases prices, simple to use and provisioning of functions. The primary real use of the tactic of cloud computing was in 2002 by the corporate Amazon net Services, once it borrow its resources to corporations throughout interval off on demand.

Many users use the cloud daily while not knowing. A bit like altogether versions of email and access to the applications that don't seem to be part put in on the native computer as paint, Microsoft Word. This use is finished due to Ethernet, however customers might not understand the situation of the servers that keep their emails and hosting the supply file of the applications that user uses. The functions offered by the Cloud Computing suppliers, come back from giant digital stations referred to as Datacenters, victimization ways supported virtualization. The virtualization is all the technical substances and/or software system which will run on one machine multiple operational systems and/or multiple applications, one by one from one another, as if they were performing on unrelated physical machines. Virtualization and consolidation will simply the management of the server's park, by decreasing the amount of systems to be maintained by optimizing the employment of resources and enabling high accessibility. However the adoption and therefore the passage to the Cloud Computing remodel provided that the protection is ensured. The way to warranty a higher file security and additionally however will we have a tendency to keep the user non-public info confidential? There are a unit 2 main queries that gift a challenge to Cloud Computing suppliers.

2. PROBLEM DEFINITION AND OBJECTIVE:

Industries start switching from local to cloud server because cloud service providers are more relating and provides large amount of storage space. However, such great advantages, problem of data security and privacy comes towards company. The data outsourced by various data users may get harmed by attacker, malware or threats.

3. LITERATURE SURVEY

3.1 Authentication Scheme using Unique Identification method with Homomorphic Encryption in Mobile Cloud Computing:

In this paper, secret writing perform like RSA and Daffier playwright cryptosystem proves to be useless against the attacks done by quantum laptop. Hence, Homomorphic Signature theme is present alongside the Identity Management (IDM) used into the mobile cloud computing so as to trace this issue by applying implicit verification methodology to classification between the real and non-genuine persons that permits system to manifest the users properly. The small print of the system are more examine later during this paper, wherever the user are genuine with IDM as development and no secret is employed throughout the verification method, permitting the users to be safely genuine at the tip of the program in execution.

3.2 Secure File storage in Cloud Computing using Hybrid Cryptography Algorithm:

In this survey we've make a case for concerning new security system victimization interchangeable key cryptography rule and steganography .In this planned framework AES, blowfish, RC6 and bandeau algorithms are accustomed style block wise safety to file. All rule key size is 128 bit's steganography system is introduced for key info safety. Key info contributes that a part of file is encrypted victimization by that rule and key .File is collapse into 8 components. Every and each a part of information is encrypted victimization totally different rule. All components of file are encrypted sequins with the assistance of multithreading functions. Encoding Keys are inserted into cowl image victimization LSB technique. Steno image is transfer to valid receiver victimization email. For information coding purpose reverse method of encoding is applied.

3.3 Secure Cloud Computing Algorithm Using Homomorphic Encryption And Multi Party Computation:

In this survey, the user's file is encrypted victimization artifact techniques, referred to as optimum uneven encoding artifact (OAEP) along with Hybrid encoding algorithmic program that's gift on RSA (i.e., HE-RSA), so as to permit multiple parties to transmit a perform on their inputs whereas protective Integrity and Confidentiality. The Homomorphic Encryption (HE) is employed on the encrypted information while not decrypting it in computationally powerful clouds and also the Secure Multi-Party Computation (SMPC) will be utilized in the cloud to make sure security and privacy of the purchasers. During this paper, we've planned a system that integrates the multi-party computation with homomorphic encoding to permit mathematical calculations of encrypted information while not secret writing. The cryptologic system utilized in our cloud model square measure represented and also the overheads square measure compared with Homomorphic encoding and Multi-Party Computation.

4. PROPOSED SYSTEM ARCHITECTURE:

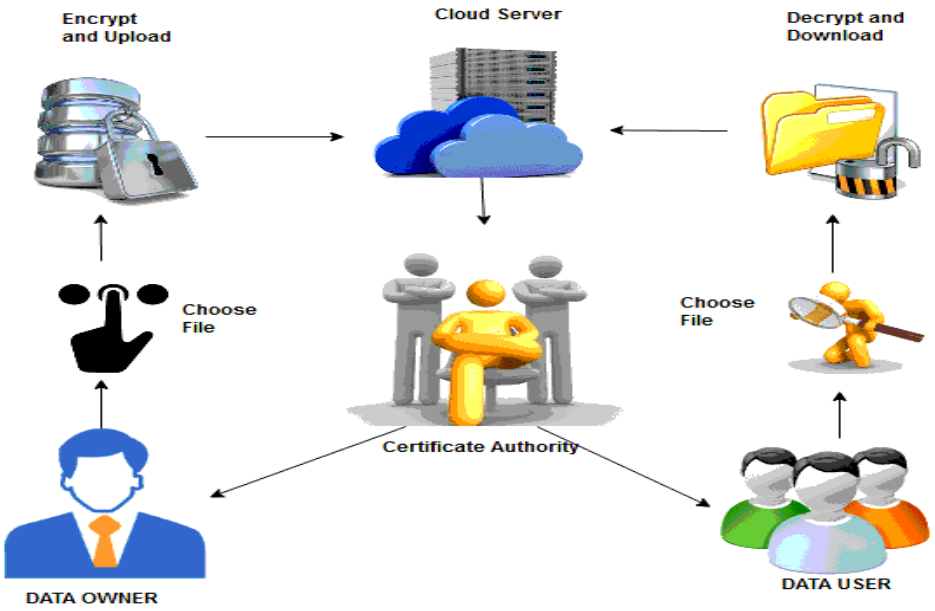

Fig 1. Proposed System Architecture

When the information transferred to the Cloud server we have a tendency to use normal coding ways to secure the operations and also the storage of the information. Our basic conception is to inscribe the information before send it to the Cloud supplier. However the last one needed to rewrite files at each operate acting. knowledge the info the information} owner can have to be compelled to give the non-public key to the server (Cloud provider) to rewrite data before execute the calculations needed, which could have an effect on the confidentiality and privacy of knowledge hold on within the Cloud. This design proposing associate degree supply of a operate to execute operations on encrypted file while not decrypting them, which can use an equivalent outputs once calculations as if we've got worked directly on the data.

Homomorphic coding wont to perform operations on encrypted information while not knowing the non-public key (without decryption), the information owner is that the solely holder of the key key. After we rewrite the outputs of any functions, it's an equivalent as if we have a tendency to have borrowed out the calculation on the unused information.

5. CONCLUSIONS:

To summarize, the work provides a model of a framework which will be utilized by organizations to safeguard and manage their knowledge hold on over untrusted public clouds. As a part of the work the likelihood of victimization delta encryption ideas beside homomorphic cryptography theme with additive homomorphy to update encrypted files, rather than sending entire encrypted versions every time once associate degree update, was explored. Below the take a look at atmosphere, the developed model has delivered promising performance results as compared to alternative common solutions. Therefore the planned approach may be thought-about to be used in universe situations.

The security topic square measure a giant downside for cloud computing development. To keep up the privacy of his file, the user should encipher knowledge before being transfer to the cloud. Cloud computing security supported homomorphic cryptography strategy, as a result of these strategy permit to perform computations on encrypted knowledge while not the employment of the key key. partly Homomorphic cryptography (PHE) like RSA and Paillier functions square measure inadequate to secure cloud computing as a result of these conspire permit to perform only 1 operation (either addition or multiplication) on the encrypted knowledge of user.

REFERENCES

1. P. Mell, T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, U. S. Department of Commerce, (2011)
2. K. Lauter, M. Naehrig, V. Vaikuntanathan, "Can Homomorphic Encryption be Practical?", CCSW' 11, Chicago, llinois, USA, pp. 113–124, (2011).
3. Craig Gentry, "Fully homomorphic encryption using ideal lattice", in Proceedings of STOC'09, (2009).
4. M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, "Fully homomorphic encryption over the Integers", in Proceedings of Advances in Cryptology, EUROCRYPT'10, pages 24–43, 2010.
5. Craig Gentry, "Computing arbitrary functions of encrypted data", Communications of The ACM, 53(3): 97-105, (2010).
6. J. Li, D. Song, S. Chen, X. Lu, "A Simple Fully Homomorphic Encryption Scheme Available in Cloud Computing", In Proceeding of IEEE, (2012).
7. Baohua Chen, Na Zhao, "Fully Homomorphic Encryption Application in Cloud Computing", in Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 11th International Computer Conference, (2014).