International Journal of Research in Engineering, Science and Management
Volume 4, Issue 11, November 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

A Proficient Privacy Protection Method for Cloud Computing

M. Somu[1], S. Mounika[2*], V. Sharmila[3], N. Saravanan[4]
[1,3,4]*Assistant professor, Department of Computer Science and Engineering, KSR College of Engineering, Tiruchengode, India*
[2]*Masters Student, Department of Computer Science and Engineering, KSR College of Engineering, Tiruchengode, India*

***Abstract*: With the quick improvement of distributed computing, more cloud administrations are into our day to day existence, and in this way security assurance of cloud administrations, particularly information protection insurance, turns out to be more significant. Anyway to perform security insurance causes tremendous overhead. Hence it is a basic issue to play out the most appropriate security to decay execution utilization while give protection assurance. In this venture, the Proficient Privacy Protection Scheme (PPPS) is proposed to give the suitable security insurance which is fulfilling the client request security prerequisite and keeping up with framework execution all the while. From the get go, the protection level is dissected by clients those require and evaluate security degree and execution of encryption calculations. Then, at that point, a proper security arrangement is inferred by the consequences of examination and evaluated information. At long last, the reproduction results show that the PPPS satisfies the client request security as well as keeps up with the cloud framework execution in various cloud conditions. The application is planned utilizing Microsoft Visual Studio .Net 2005 as front end. The coding language utilized is Visual C# .Net. MS-SQL Server 2000 is utilized as back end information base.**

***Keywords*: Proficient Privacy Protection Scheme (PPPS), Cloud computing, Encryption, Decryption.**

1. Introduction

To scramble/unscramble the information of less significance utilizing feeble encryption strategy so correspondence is quick. The encryption interaction of the halfway information utilizing 3DES encryption technique and other incomplete information in solid encryption strategy with the goal that correspondence is quick and security level is raised. Scrambling and decoding the a few fields utilizing solid encryption technique and some different fields utilizing frail encryption strategy so that all fields are shown to high advantage clients and a few fields are shown to low special clients. The 3DES (Data Encryption Standard) is utilized to decrease the expense for the customers. This three-layer execution can expand the information protection to the end client by devouring additional time than existing framework.

From the beginning, the protection level is investigated by clients those require and evaluate security degree and execution of encryption calculations. Then, at that point, a suitable security piece is inferred by the aftereffects of investigation and measured information. It tends to be performed by encode /unscramble the watermarked substance with frail encryption technique and non-watermarked substance with solid encryption strategy.

2. Existing Privacy Protection Method for Cloud Computing

Distributed computing is an arising registering style which offers dynamic types of assistance, adaptable and pay-per-use. The distinctive between distributed computing and other processing models are administration driven, sharing asset, and information facilitating in reevaluating stockpiling. Sharing asset causes the equipment execution to be utilized more effective and gives financial advantages to clients to decrease the capital expense and extra consumption.

In the current framework, progressed encryption standard is utilized, since it is accepted that clients cannot plainly recognize their security necessities and expanding cost. In this situation, the levels can be viewed as significant expense.

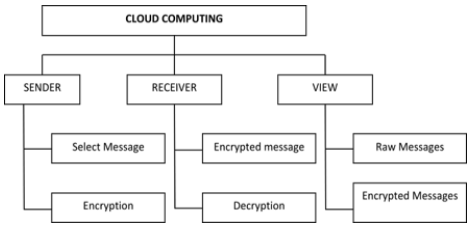

Fig. 1. System flow diagram

3. Methodology

The following modules are present in the project.

- Message selection
- Encryption
- Decryption

A. Message Selection

In this module, the message content is entered in message box control or chose from document. The message is saved into the 'Raw Messages' table.

B. Encryption

The prerequisite of this level presents that no delicate data in

*Corresponding author: mounikavelu@gmail.com

the information. Clients need to utilize the feeble encryption synthesis to acquire more execution for utilizing cloud administrations.

The prerequisite of this level presents that information incorporates some delicate data. The information requires feeble encryption for halfway information (like location, mail id of corporates') and solid encryption for residual information, (for example, account adjusts and other secure data).

In this protection level, the information contains most significant data. To ensure the information security, more special clients view the majority of the information and less advantaged clients view restricted information, a portion of the report types, for example, as of now watermarked pictures and sound substance are given less security and got to by all sort of clients while ordinary substance are given greater security i.e., solid cryptography is applied.

C. Decryption

In this module, the cycle can unscramble the information got from past process done by a similar framework

4. Conclusion

Through this undertaking, the issue of secure correspondence is disposed of. Also, the application required less working involvement with frameworks to run the product. The application is tried well so the end clients utilize this product for their entire tasks.

It is accepted that practically all the framework destinations that have been arranged at the initiation of the product advancement have been net with and the execution interaction of the undertaking is finished. A preliminary attempt of the framework has been made and is giving acceptable outcomes the methodology for handling is straightforward and ordinary request. The method involved with getting ready plans been passed up a great opportunity which may be considered for additional adjustment of the application. The undertaking successfully stores and recovers the records from the cloud space information base server. The records are encoded and decoded at whatever point essential with the goal that they are secure.

5. Future Development

The accompanying upgrades are ought to be in future.

- The application whenever created as web administrations, then, at that point, numerous applications can utilize the records.
- The information honesty in cloud climate isn't thought of. The blunder circumstance can be recuperated in case there is any confuse.
- The site and data set can be facilitated in genuine cloud place during the execution.

References

[1] Jennings, B, R Stadler. Resource management in clouds: Survey and research challenges. Journal of Network and Systems Management, 2015;23(3): pp. 567-619.

[2] Mell, P, T Grance. The NIST definition of cloud computing. 2011.

[3] Arianyan, E, H Taheri, S Sharifian. Novel energy and SLA efficient resource management heuristics for consolidation of virtual machines in cloud data centers. Computers & Electrical Engineering, 2015;47: pp. 222-240

[4] Zhang, J, H Huang, X Wang. Resource provision algorithms in cloud computing: A survey. Journal of Network and Computer Applications, 2016;64: pp. 23-42.

[5] Shi, W, et al. An online auction framework for dynamic resource provisioning in cloud computing. IEEE/ACM Transactions on Networking, 2016;24(4): pp. 2060-2073.

[6] Wang, X, et al. An intelligent economic approach for dynamic resource allocation in cloud services. IEEE Transactions on Cloud Computing, 2015;3(3): pp. 275-289

[7] Jintao, J, Y Wensen, G Lei. Research on Batch Scheduling in Cloud Computing. TELKOMNIKA (Telecommunication Computing Electronics and Control), 2016;14(4): pp. 1454-1461.

[8] Kaur, M, S. S Kadam. Discovery of resources using MADM approaches for parallel and distributed computing. Engineering Science and Technology, 2017.

[9] Pietri, I, R Sakellariou. Mapping virtual machines onto physical machines in cloud computing: A survey. ACM Computing Surveys (CSUR), 2016;49(3): pp. 49.

[10] Endo, PT, et al. Self-organizing strategies for resource management in Cloud Computing: State-of-the-art and challenges. in Cloud Computing and Communications (Latin Cloud), 2nd IEEE Latin American Conference on. 2013. IEEE.

[11] Singh, A, K Chatterjee. Cloud security issues and challenges: A survey. Journal of Network and Computer Applications,2017;79: pp. 88-115.

[12] Nguyen Van, H, F Dang Tran, J-M. Menaud. Autonomic virtual resource management for service hosting platforms. in Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. 2009. IEEE Computer Society.

[13] Manvi, S. S, G. K Shyam. Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey. Journal of Network and Computer Applications, 2014;41: pp. 424-440.

[14] Parikh, S. M. A survey on cloud computing resource allocation techniques. in Engineering (NUiCONE), 2013 Nirma University International Conference on. 2013. IEEE.

[15] Madni, SHH, et al. Resource scheduling for infrastructure as a service (IaaS) in cloud computing: Challenges and opportunities. Journal of Network and Computer Applications, 2016;68: pp. 173-200.

[16] Vakilinia, S, MM Ali, D Qiu. Modeling of the resource allocation in cloud computing centers. Computer Networks, 2015;91: pp. 453-470.

[17] Han, D, W Sun, X Fan. Dynamic energy management in smart grid: A fast randomized first-order optimization algorithm. International Journal of Electrical Power & Energy Systems, 2018;94: pp. 179-187.

[18] Lee, L-T, et al., A dynamic resource management with energy saving mechanism for supporting cloud computing. International Journal of Grid and Distributed Computing, 2013;6(1): pp. 67-76.

[19] Kim, N, J Cho, E Seo. Energy-credit scheduler: an energy-aware virtual machine scheduler for cloud systems. Future Generation Computer Systems, 2014. 32: pp. 128-137.

[20] Ding, Y, et al. Energy efficient scheduling of virtual machines in cloud with deadline constraint. Future Generation Computer Systems, 2015;50: pp. 62-74.

[21] Wang, W, Y Jiang, W Wu. Multiagent-Based Resource Allocation for Energy Minimization in Cloud Computing Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2016.

[22] Younge, A. J, et al. Efficient resource management for cloud computing environments. in Green Computing Conference, 2010 International. 2010. IEEE.

[23] N. Saravanan, M. Geethanjali. Attribute Based Encryption with Privacy Production in Clouds, International journal of Innovative Research in Computer and Communication Engineering, vol. 2 Special Issue 1, pp. 1502-1502, March 2014.

[24] M. K. Nivodhini, P. Vasuki, Kiruthika K, Lokesh P N, Sangeetha C, Suriya Kumar S, On The Security of Data Access Cloud Control for Multi Authority Cloud Storage Systems, International Journal of Intellectual Advancements and Research in Engineering Computations, vol. 6, no. 2, April 2018.

[25] V. Sharmila. A Survey on Cloud Computing, South Asian Journal of Engineering and Technology, 2017.