Framework for Client Side AES Encryption Technique in Cloud Computing

Jaspreet Singh

Post Graduate Student
SVIET Banur

Abstract: **Cloud computing is essentially the most rising pattern in expertise technological know-how now days. It is attracting the firms because of its benefits of scalability, throughput, handy and low cost access and on demand up and down grading of SaaS, PaaS and IaaS. Apart from the entire salient features of cloud environment, there are the massive challenges of privateness and security. This paper propose a hybrid AES to increase the security of the cloud computing. The proposed technique implemented encryption process using RSA with HMAC. This work also ensures the integrity of data using Hash codes. Authentication security of cloud computing is enhanced using multi-level authentication. Results of the proposed technique is analyzed and compared with the existing technique on the basis of data encryption time and data decryption time.**

Keywords: **Cloud computing, Security, AES, Encryption, Decryption, RSA, HMAC, Integrity, Hash codes, Authentication.**

I. INTRODUCTION

Cloud Computing has been pictured as the future race in structural design of IT endeavour, for the reason that of its countless advantages inside the IT enterprise. It enables on-demand resources, popular entry of network, resource pooling, resource adaptability, pay per use pricing and danger defense. The long run step in revolutionising the IT industry is to shift the model of conventional cloud to the cloud atmosphere. In conventional cloud computing buying and to possess the s/w, software and h/w to fulfil users' essential necessitate. To configure, verify, and experiment and to assess the system s/w raises the necessity of assets protection. The useful resource utilization cost is extra to fulfil the person needs. In Cloud atmosphere the info storage and raises CPU usage allows the data storing and pay as use services according to the QoS [1]. The scalable offerings wanted by means of the person will also be purchased from the cloud proven is figure-1.1. The cloud presents countless services that can be categorized into three main fields: software-as-a-service (SaaS), Infrastructure-as-a-provider (IaaS) and Platform-as-a-provider (PaaS). The deployment units of cloud are: Hybrid model, group model, personal model, and Public model. The atmosphere in cloud additionally relates with grid computing, utility computing and obvious computing. Grid cloud computing: Its common form can be distributed computing [2]. It's composed of clusters of virtual computing as well as supercomputing, the place loosely coupled computers participate in the fundamental goals. Utility cloud computing: It consist the bundle of compute belongings. It is just like public utility offerings like water, fuel, electrical power, and telephonic amenities. Transparent cloud computing: referred to as backend cloud offerings which might be very complex. These are obvious, quandary-free and relaxed to make use of the service that gives frontend services. The expression 'cloud' had been used as a historical symbol for the online. The usage of the time period Cloud used to be first originate from its common description in network world outlines as an diagram of a cloud, used to specific the transportation of know-how crossing the transport backbones to one finish to an extra finish of the cloud. Nevertheless, the elemental proposal of cloud has been revived. It had been for the period of this factor of time that the phrase 'cloud-computing' began to forth come within the technological generation.

II. BACKGROUND

Gowrigolla et al. (2005) provided a brief prologue to Cloud figuring protection issue being tended to is at that point presented, by portraying a portion of the one of a kind variables to be considered when information enters the Cloud. At long last, an information assurance conspire with open examining plan is plot that will address some of these variables, by giving an instrument to permit to information to be encoded in the Cloud without loss of openness or usefulness for approved gatherings. This plan isn't really a swap for conventional protection and safety efforts for information, but instead an improvement which permits clients (once more, at either the individual or endeavor level) a more noteworthy level of trust in the reception of inventive, cost sparing Cloud registering advancements. [1]

Somani et al. (2010) endeavored to get to distributed storage technique and information security in cloud by the usage of advanced mark with RSA calculation. The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability. The predominant issue related with distributed computing is the cloud security and the proper execution of cover over the system. [2]

Wang et al. (2010) combined open key based homomorphic authenticator with arbitrary concealing to accomplish the protection safeguarding open cloud information examining framework. Distributed computing is the since a long time ago envisioned vision of registering as an utility, where clients can remotely store their information into the cloud in order to appreciate the on-request astounding applications and administrations from a common pool of configurable figuring assets. By information outsourcing, clients can be calmed from the weight of nearby information stockpiling and support. Notwithstanding, the way that clients never again have physical ownership of the conceivably substantial size of outsourced information makes the information respectability security in Cloud Computing an exceptionally difficult and possibly impressive errand, particularly for clients with obliged figuring

assets and capacities. Along these lines, empowering open auditability for cloud information stockpiling security is of basic significance with the goal that clients can fall back on an outside review gathering to check the respectability of outsourced information when required. To help proficient treatment of numerous reviewing assignments, this work additionally investigate the strategy of bilinear total mark to expand our principle result into a multi-client setting, where TPA can play out various evaluating errands at the same time. Broad security and execution investigation demonstrates the proposed plans are provably secure and profoundly proficient. [3]

Zhou et al. (2010) had explored different Cloud Computing model suppliers about their dread on information security and information protection matters. The creator found that those worries aren't abundant and additional endeavors ought to be affixed as far as 5 viewpoints that is, information accessibility, information privacy, honesty, information control, information review as far as security arrangements in cloud. Moreover, discharged strategies on information security aren't fit and upto date to ensure cloud clients' most vital and private information data in the new condition that is, Cloud condition. As they can't be material to the new relationship exists between cloud clients' and cloud specialist organizations. This would contains 3 parties that is, Cloud user's, Cloud specialist co-op (CSP), Cloud suppliers'. Multi area databases and administrations or applications in the Cloud had aggravated the protection issues. In this way, adapt of some discharged arrangements for new conditions in the Cloud condition. [4]

Li et al. (2010) formalized and solved the issue of viable fluffy catchphrase look over encoded cloud information while keeping up watchword security. Fluffy watchword look significantly improves framework ease of use by restoring the coordinating records when clients' seeking inputs precisely coordinate the predefined catchphrases or the nearest conceivable coordinating documents in light of watchword closeness semantics, when correct match comes up short. This work misused alter separation to evaluate watchwords likeness and build up a propelled system on developing fluffy catchphrase sets, which extraordinarily decreases the capacity and portrayal overheads. Through thorough security examination, they demonstrated that proposed arrangement is secure and protection safeguarding, while accurately understanding the objective of fluffy catchphrase look. [5]

Yu et al. (2010) enforced access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to un trusted cloud servers without disclosing the underlying data contents. Achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. [6]

Somani et al. (2010) endeavored to survey Cloud Storage Methodology and Data Security in cloud by the Implementation of computerized signature with RSA calculation. The cloud is a cutting edge stage that gives dynamic asset pools, virtualization, and high accessibility. Today, we can use versatile, dispersed processing conditions inside the bounds of the Internet, a training known as distributed computing. Distributed computing is the Concept Implemented to disentangle the Daily Computing Problems, preferences of Hardware Software and Resource Availability unhurried by Computer clients. The distributed computing gives an undemanding and Non inadequate Solution for Daily Computing. The pervasive Problem Associated with Cloud Computing is the Cloud security and the fitting Implementation of Cloud over the Network. Distributed computing declared an ease supercomputing administrations to give the likelihood, while there are a substantial number of makers behind, there is most likely that distributed computing has a splendid future. [7]

Ramgovind et al. (2010) provided an general security point of view of Cloud figuring with the expect to feature the security worries that ought to be appropriately tended to and figured out how to understand the maximum capacity of Cloud processing. Distributed computing has raised IT to more up as far as possible by offering the market condition information stockpiling and limit with adaptable versatile registering preparing energy to coordinate flexible request and supply, while diminishing capital consumption. However the open door cost of the fruitful execution of Cloud processing is to successfully deal with the security in the cloud applications. Security awareness and concerns emerge when one starts to run applications past the assigned firewall and draw nearer towards general society area. Gartner's rundown on cloud security issues, also the discoveries from the International Data Corporation venture board overview in view of cloud dangers, will be examined in this paper. In this paper key security considerations and challenges which are currently faced in the Cloud computing industry are highlighted. [8]

Dubey et al. (2012) proposed another distributed computing condition where a trusted cloud condition approach is utilized which is controlled by both the customer and the cloud condition administrator. The expanded level of network and the expanding measure of information has driven numerous suppliers and specifically server farms to utilize bigger foundations with dynamic load and access adjusting. This prompt the request of distributed computing. Be that as it may, there are a few security concerns when we handle and offer information in the distributed computing condition. [9]

Sood et al. (2012) outline work including diverse strategies and particular systems is recommended that can effectively shield the information from the earliest starting point to the end, i.e., from the proprietor to the cloud and after that to the client. characterization of information based on three cryptographic parameters displayed by the client, i.e., Confidentiality (C), Availability (An) and Integrity (I).The technique took after to ensure the information uses different measures, for example, the SSL (Secure Socket Layer) 128-piece encryption and can likewise be raised to 256-piece encryption if necessary, MAC (Message Authentication Code) is utilized for trustworthiness check of information, accessible encryption and division of information into three segments in cloud for capacity. The division of information into three segments renders supplementary security and straightforward access to the information. The client who wishes to get to the information is required to give the proprietor login character and secret word, before induction is given to the encoded information. [10]

III.PROPOSED TECHNIQUE

Cloud computing is a modern advancement in IT communications and organizations the clients' can utilize cloud applications which are named as "cloud services". The client can utilize the cloud administrations from all over the world and at any time. This has diminished the heavy hardware transportation cost. However, in today's scenario the main focus is on the solution of 3 major security aspects named as Availability, Confidentiality and Integrity [4]. As the growing stage of industry, rather than purchasing any application, the client simply needs to pay for the applications he/she is utilizing. The cloud application cost can incorporate time, administrations and capacity the client doesn't have to possess the administrations which diminish the cost of owning the applications Bulk of data is stored in cloud server. This data is also exposed to various security issues. In this way, guaranteeing the information security in cloud is dependably a fundamental test in distributed computing. In this study different security part of security issues has been analyzed and after that proposes a structure to ease security issues at the level approval and limit level in dispersed processing. Effective security instruments ought to be sent by methods for encryption, validation, and approval or by some other technique to guarantee the protection of shopper's information on distributed storage. The objectives of the proposed technique are:

- To do the comparative study of existing security algorithm as AES.
- To propose a new technique Hybrid AES to increase the security of the cloud computing.
- To ensure the integrity of the data using Hash codes.
- To enhance the authentication security of the cloud computing using multi-level authentication.
- To compare the results of proposed technique with the existing techniques on the basis of:

a. Data Encryption time
b. Data Decryption time

The methodology for proposed technique is as follows:
Uploading data on cloud securely by encrypting its data using RSA with HMAC i.e. hashed message authentication code. Data is encrypted using RSA and the HMAC code file of that data is generated and sending both the files Encrypted File + HMAC code file to the cloud. Also, saved HMAC code file to the LOCAL storage also to preserve the integrity of the data in cloud. The cloud sends the encrypted file to the consumer by utilizing the decryption key for file. After decrypting the file, the integrity check can be applied by the user using HMAC. The user receives the HMAC along with the file. The user can compute the HMAC on the file and check if both are equal. It can in this way distinguish if there is any altering of information amid transmission

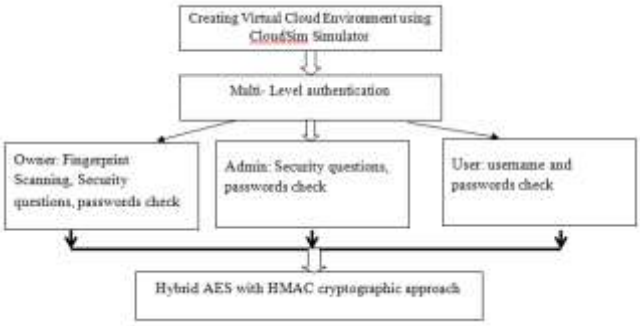

Figure 3.1 Proposed Technique

IV. EXPERIMENTAL RESULTS

The proposed system is actualized with the assistance of CloudSim and Net beans IDE 8.0. CloudSim is the library that gives the reproduction condition of distributed computing and furthermore give essential classes portraying virtual machines, server farms, clients and applications.

Encryption Process

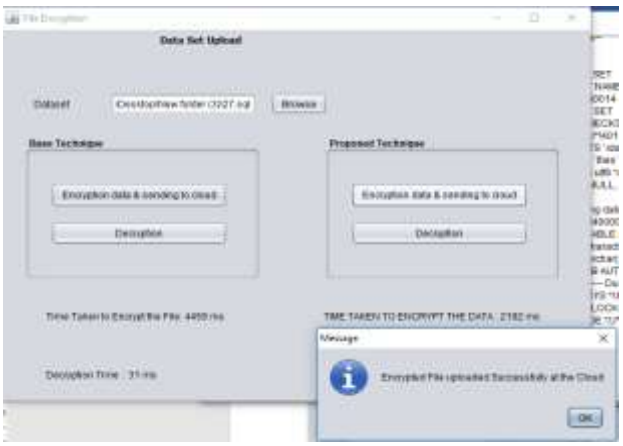

Figure 4.1 Proposed Encryption Technique

Figure 4.2 Generating the hash codes

Figure 4.3 Hash codes sent to cloud along with encrypted file Decryption Process

Figure 4.4 Matching the hash codes first

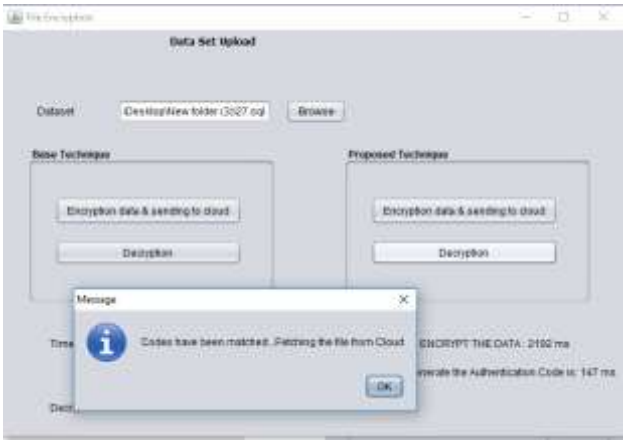

Figure 4.5 Hash codes matched

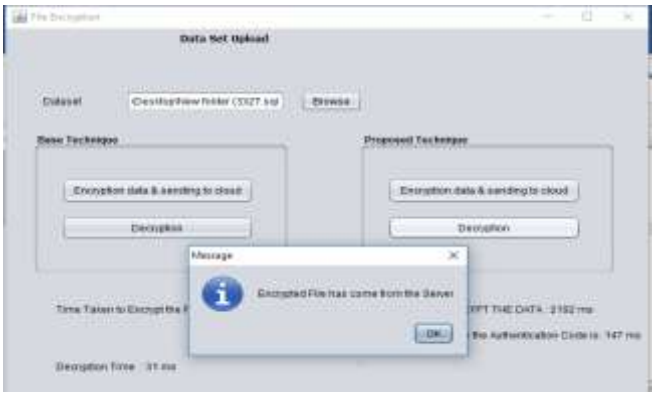

Figure 4.6 fetching the file from cloud if hash codes matches

Comparison of Proposed Hybrid RSA-HMAC with AES

Table 4.1 Encryption time with AES and Proposed Hybrid RSA with HMAC

Techniques	Encryption Time
Base paper technique with AES	4459 milliseconds
Proposed Encryption with HMAC	2192 milliseconds

Figure 4.7 Representing comparison of encryption time of proposed algorithm with respect to AES algorithm

Table 4.2 Decryption time with AES and Proposed Hybrid RSA with HMAC

Techniques	Encryption Time
Base paper technique with AES	31 milliseconds
Proposed Decryption with HMAC	1576 milliseconds

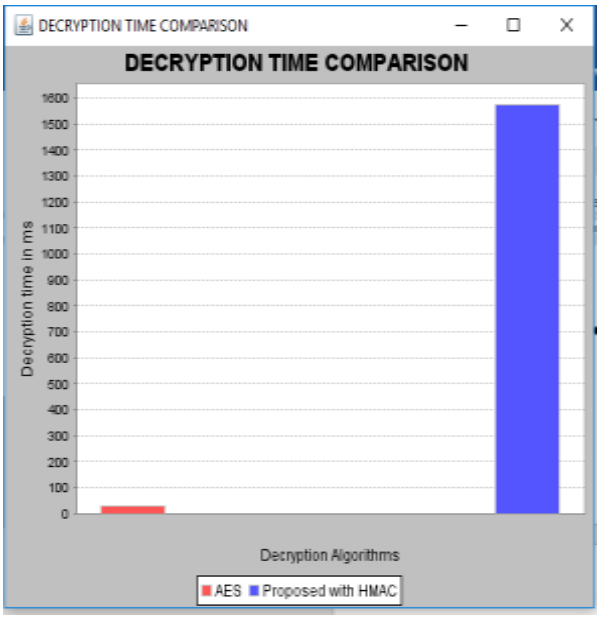

Figure 4.8 Representing comparison of decryption time of proposed algorithm with respect to AES algorithm

V. CONCLUSION

This research work, deploy two-way technique to prevent security breaches on cloud computing. The proposed technique implemented encryption process using RSA with HMAC. The data is first encrypted using RSA and time taken to encrypt the data is 2192 milliseconds. HMAC Message authentication codes of that file are also generated using SHA 512. During the decryption process, before fetching the encrypted file from the cloud, firstly the HMAC Codes are fetched from the cloud. HMAC code of fetched file and local file are checked for match, to maintain integrity of message. Decryption process takes 1576 milliseconds. Experimental Results clearly show that the proposed with HMAC performs better as its encryption time is less as compare to the existing AES technique. The proposed algorithm will take more time to decrypt the data as it has more complex encryption. In the proposed algorithm, the file is encrypted using RSA and then HMAC Message authentication codes of that file is also generated using SHA 512. The proposed methodology is implemented with the help of CloudSim and Net beans IDE 8.0. In Future, we can reduce the decryption time, to enhance the performance of the algorithm. Also, this work can be simulated in real time. The technique may be further optimized so that it can work on large files also.

REFERENCES

[1] Bhagyaraj Gowrigolla, Sathyalakshmi Sivaji, M.Roberts Masillamani, " Design and Auditing of Cloud Computing Security", IEEE 2010, pp. 292-297.

[2] U. Somani, K. Lakhani, and M. Mundra, "Implementing digital signature with RSA encryption algorithm to enhance the data security of cloud in cloud computing," *2010 1st Int. Conf. Parallel, Distrib. Grid Comput. PDGC - 2010*, pp. 211–216, 2010.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," *Proc. - IEEE INFOCOM*, 2010.

[4] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," *Proc. - 6th Int. Conf. Semant. Knowl. Grid, SKG 2010*, no. July, pp. 105–112, 2010.

[5] Jin Li, Qian Wang, Cong Wang, Ning Cao, Kui Ren, Wenjing Lou, " Fuzzy Keyword Search over Encrypted Data in Cloud Computing", IEEE 2010,

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure,scalable ,and fine-grained data access control in cloud computing.pdf," *Ieee Infocom*, pp. 1–9, 2010.

[7] Uma Somani, Kanika Lakhani, Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", IEEE 1st International Conference on Parallel, Distributed and Grid Computing, 2010, pp. 211-216.

[8] Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing", IEEE 2010.

[9] A. K. Dubey, A. K. Dubey, M. Namdev, and S. S. Shrivastava, "Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment," *2012 CSI 6th Int. Conf. Softw. Eng. CONSEG 2012*, 2012.

[10] S. K. Sood, "A combined approach to ensure data security in cloud computing," *J. Netw. Comput. Appl.*, vol. 35, no. 6, pp. 1831–1838, 2012.

[11] P. Yellamma, C. Narasimham, and V. Sreenivas, "Data security in cloud using RSA," *2013 4th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2013*, 2013.

[12] F. F. Moghaddam, M. T. Alrashdan, and O. Karimi, "A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments," *J. Adv. Comput. Networks*, vol. 1, no. 3, pp. 238–241, 2013.

[13] Pachipala Yellamma, Challa Narasimham, Velagapudi sreenivas, "Data Security in Cloud Using Rsa", IEEE 2013.
[14] G. L. Prakash, M. Prateek, and I. Singh, "Data encryption and decryption algorithms using key rotations for data security in cloud system," *Int. Conf. Signal Propag. Comput. Technol. (ICSPCT 2014)*, vol. 3, no. 4, pp. 624–629, 2014.
[15] Hongbing Cheng, Weihong Wang, Chunming Rong, " Privacy Protection Beyond Encryption for Cloud Big Data", IEEE International Conference on Information Technology and Electronic Commerce, 2014, pp. 188-191.
[16] Y. Rahulamathavan, R. C. W. Phan, S. Veluru, K. Cumanan, and M. Rajarajan, "Privacy-Preserving Multi-Class Support Vector Machine for Outsourcing the Data Classification in Cloud," *IEEE Trans. Dependable Secur. Comput.*, vol. 11, no. 5, pp. 467–479, 2014.
[17] Vishwanath S Mahalle, Aniket K Shahade, "Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm", IEEE 2014, pp. 146-149.
[18] Zahir Tari, "Security and Privacy in Cloud Computing", IEEE Cloud Computing, 2014, pp. 54-57.
[19] V. K. Pant, J. Prakash, and A. Asthana, "Three step data security model for cloud computing based on RSA and steganography," *2015 Int. Conf. Green Comput. Internet Things*, pp. 490–494, 2015.
[20] B. K. Samanthula, Y. Elmehdwi, G. Howser, and S. Madria, "A secure data sharing and query processing framework via federation of cloud computing," *Inf. Syst.*, vol. 48, pp. 196–212, 2015.