January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

Mitigating Security Issues in Cloud Environments Using Enhanced Hybrid Secure Algorithm

P.Nagamani[1], Dr.S.Sreekanth[2]

[1] Research Scholar, CSE Department, Rayalaseema University, Kurnool, Andhra Pradesh
[2] Professor, Department of CSE, SITAMS, Chittoor, Andhra Pradesh
[1] nagamani.koli@gmail.com, [2] pranavasree_2000@rediffmail.com

Article Info
Volume 82
Page Number: 11072 - 11084
Publication Issue:
January-February 2020

Article History

Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 21 February 2020*

Abstract

Cloud computing has emerged as an infrastructure-based and software-based model for several data storage applications like shared storage pools, networks and servers. While numerous research works were being carried out in recent years, securing the data in a cloud environment has emerged as a challenging area of concern. To mitigate the security aspects, a novel security algorithm for cloud computing called as, Enhanced Hybrid Privacy & Secure (Enhanced HPS) Algorithm by the employment of symmetric cipher AES and asymmetric cipher RSA, has been formulated and investigated properly. The chief intention of the proposed algorithm is to improve the security over the existing algorithms. The proposed strategy incorporates three distinct security scanners with divergent selections based on the request from concerned party for usage in cloud computing. The performance of the proposed algorithm is evaluated in terms of encryption time, decryption time, time to encrypt the data and upload it to the cloud server, time to decrypt the data wile downloading the file from the cloud server, key generation time and key updation time. The proposed algorithm is compared with the well-evaluated existing cloud security-based algorithms like RHIBE_AES, RHIBE_HYBRID, RHABE_AES and RHABE_HYBRID. Simulation results clearly revealed that, the proposed algorithm outperforms all the existing cloud security algorithms in terms of the aforementioned parameters.

Keywords**:** *Cloud computing, Cloud security, Encryption and Decryption, Hybrid cryptographic systems, Plaintext, Ciphertext, Key Generation and Key Updation*

I. INTRODUCTION

Cloud computing is a structure or framework for attaining pervasive, convenient, on-demand network accessing over communal group of configured computation of resources (e.g., network, server, application, and service), which could be quicker in provision and shall be released with nominal administration efforts or service provider interactions [1]. Cloud can be articulated as an internet-based setting that offers service on the basis of hardwares and softwares. In recent times, employment of cloud computing is getting increased swiftly because of ease in user friendliness. This permits people to accomplish any activities easily even without thorough knowledge of the fundamental technologies. The number of users shall effortlessly be associated to the cloud, and share the information over thew web. Moreover, few users and small scale business people can avoid the difficulties in their regular activities by uploading their data in to the cloud with better security mechanisms [2]. Therefore, they demand the cloud service provider to distribute these facilities, that requires complete confidence towards service

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

provider. At the same time, the concerned users have to accomplish and put forward the information security mechanisms for their own information. Consequently, the third party service usage and accomplishing corresponding security for their information is the basic challenging task when concerning wioth cloud infrastructures [3].

Concerning with the security parameter, cryptography is the basic phenomenon to protect the information when outsourcing it. This is procedure by which the actual information gets encrypted by means of dissimilar cryptographic algorithms. Numerous symmetric and asymmetric cryptographic methods are existing in the domain like Creaser cipher, Hill cipher, Playfair cipher, DES, AES and RSA [4].

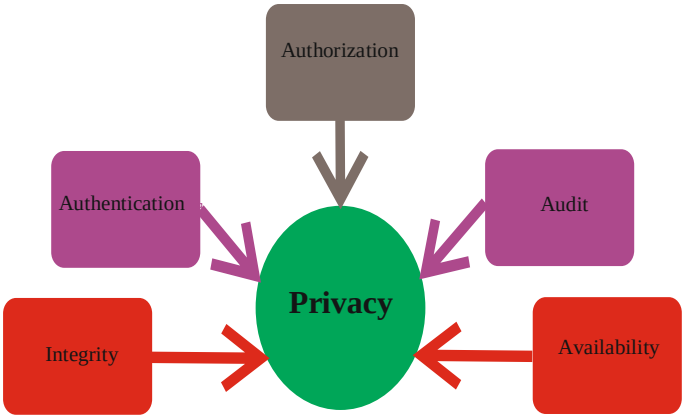

Figure 1: Articulation of basic security factors [5]

Hybrid cryptographic systems (grouping of symmetric and asymmetric encryption process) rise the information privacy when compared with elementary cryptographic algorithms. Security has developed to be the foremost problem that everybody faces when consuming internet in their everyday life, security shall be attained by few foremost types like authentication, confidentiality and integrity as illustrated in Figure 1. Authentication is the process by which, the illegal operator shall not access our sites or networks. Authorization is the process by which, only authenticated operator will be permitted to access the data. Integrity is the mechanism that checks that the data transmitted does not involve any modifications on the way towards the receiver. Audit is the methodical assessment of the data security. Availability is the greatest guaranteed mechanism by thoroughly upholding the data [6].

Plain text is the text message that somebody wants to encrypt it and direct it to alternative user, and be guaranteed that no one shall be able to read it excluding the reciver. Key is the module that has to be known amid the sender or receiver message, and if the intermediate hacker knows it, all the data will be hacked by the hacker. The two categories of keys are Public and Private keys. Encryption algorithm is the set of procedures that are used for encryption procedure, and there are many algorithms prevailing in the literature that are based on symmetric or asymmetric encryption.

Cipher text corresponds to the resultant of encryption procedure after putting on definite cryptographic procedure for encrypting the plain text. Decryption corresponds to the extraction of plaintext from the encrypted text. Symmetric key is also referred as private key cryptography, which employs identical private key for both encryption and decryption procedures, therefore the sender and receiver should have knowledge about this key. The foremost well-known procedures that employ this practice are Data Encryption Standard (DES) and Advanced Encryption Standard (AES) [7,8].

In this paper, we have proposed a novel secure algorithm for cloud computing called as, Enhanced Hybrid Privacy & Secure (Enhanced HPS) Algorithm by the employment of symmetric cipher AES and asymmetric cipher RSA. The foremost aim of the proposed algorithm is to improve the security in the existing algorithm. The proposed strategy incorporates three dissimilar security scanners with dissimilar selections based on the request from concerned party for usage in cloud computing. The proposed work is based on the results of existing security for Linux Kernel Virtual Machine. By this proposed algorithm, it is probable in protecting the integrity of virtual machines (VM) and distributed

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

computing middleware that appears as a subsidiary element in cloud computing.

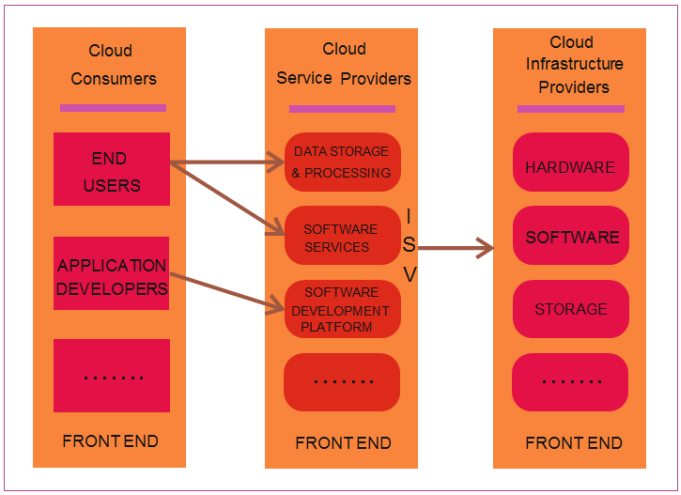

Figure 2. Levels of Abstractions in Cloud Computing

The performance of the proposed algorithm is evaluated in terms of encryption time, decryption time, time to encrypt the data and upload it to the cloud server, time to decrypt the data wile downloading the file from the cloud server, key generation time and key updation time. The proposed algorithm is compared with the well evaluated existing cloud security based algorithms like RHIBE_AES, RHIBE_HYBRID, RHABE_AES and RHABE_HYBRID. Figure 2 entails the levels of abstractions of cloud computing, that forms a backbone for the proposed algorithm, that includes cloud consumers, cloud service providers and cloud infrastructure providers. The cloud consumers is based on the end users and application developers, cloud service providers are based on the data storage, data processing, software services and software development platform, cloud infrastructure providers are based on the hardware, software and corresponding storage.

II. REVIEW OF LITERATURE

The authors in [9] examined the progressing problems over usage of XML Signatures and Web Service security framework (confronting the structure itself), and also deliberated the prominence and competences of browser securities in Cloud computing context (SaaS), and also upstretched the concenterations on Cloud service reliability and binding issue (PaaS), thereby outlined the danger concerning flooding attacks.

Researchers in [10] have discussed about the basic security issues concerned with data security in cloud computing. For an user to attain contented with the service, the solutions that grips the softwares, information and procedures, there must be present substantial guarantees that services are extremely dependable and accessible, protected and safer, also privacy is being sheltered. This increases the matters of endwise services separation over VPN, SSH and VLANs. This suggests a service oriented design, abridged data overhead for end users, greater tractability, lower overall cost of possession, on-demand service, etc.

Research works carried out in [11] have investigated the security issues in cloud infrastructure and concluded that, numerous unresolved problems are being present, predominantly connected with service-level agreement (SLA), security, privacy, and power effectiveness. Moreover, present security aspects has numerous loop holes that shocks the concerned user. Unless appropriate security modules were formulated, the user shall not be viable in leveraging the benefits of cloud computing. The formulated unit must provide a generous solution to every problems rising from entire directions in cloud. A combined security prototype that targets dissimilar stages of securing the information for a characteristic cloud infrastructure is still under investigation. The framework in this research work correlates with storage of interrelated information at different places on the basis of meta-data statistics that shall create the data to be irreplaceable if a malicious user recovers it.

Review carried out by investigators in [12] clearly showed that cloud environment worries basically on the apparent loss of control towards sensitive

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

information. Existing regulatory procedures shall not sufficiently discourse the third party information storage and processing need. This existing strategy extends controlling measure from the enterprises into the cloud via the usage of trusted computation and employed cryptographic methods. These procedures must relieve considerable fear when thinking of cloud computation, thereby has the ability in providing perceptible business intellect benefits towards cloud contribution. The revelation also recounts towards similar difficulties and exploitations rising from a superior dependence over cloud, thereby to preserve the privacy in the face of such outbreaks. Specifically, fresh threats necessitate first-hand construction to uphold and increase security.

Investigations in [13], with a concenteration on the way to the final-aim of a systematic understanding in the domain of cloud computing and a supplementary speedy approval from technical communities, the articulation is proposed that validates the separation of cloud into five foremost levels, and demonstrates their inter-relations and inter-dependence over previous strategies. The contributions in this research lie in the existence of one of the principal efforts to begin an exhaustive feature of the cloud. Improved understanding of the technologies shall encourage the user to enterprise more effectual gateways in cloud, and enables the implementation of this innovative method in technical settings. Thus, this strategy was found to support the technical communities to advance its contribution and insight over this growing computational domain.

The authors in [14] have concenterated on the problem of how to deliver suitable secrecy fortification for cloud that are yet being unresolved. This research work has delivered a methodology in which the technical and practical answers were co-formulated for demonstrating the responsibility as a trail frontward in solving severe secrecy and safety related threats inside the cloud.

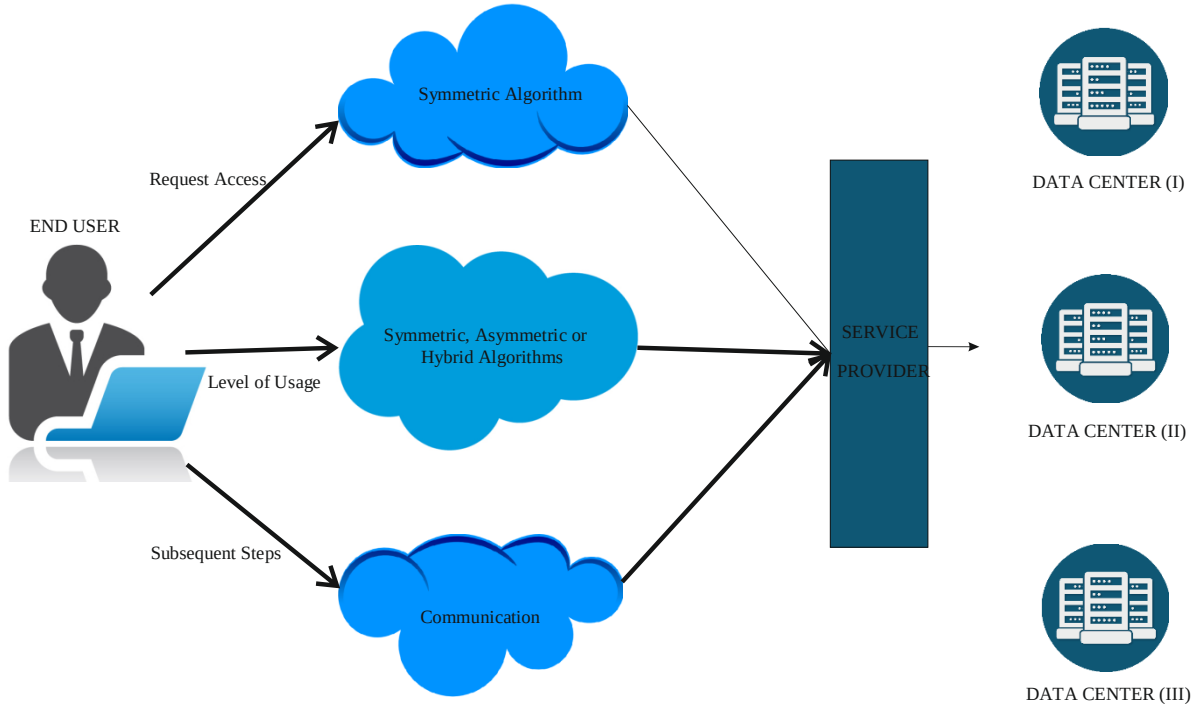

Figure 3. Scenario of proposed model in the cloud security

The existing secure systems attract much importance in getting the strength back if things goes wrong, and is not sufficient in demanding to place privacy in the principal place. Facility of a hybrid secure

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

strategy through the mixture of permissible, supervisory and practical means leveraging both public and private systems of responsibility will be one of the theoretical method of addressing this issue.

III. PROPOSED ENHANCED HPS ALGORITHM

So as to regulate the security issues from the Information Technology Service Standards (ITSS) of the organization, we have proposed a strategy as an acceptable system explanation in the cloud computing, referred as the Enhanced HPS Algorithm, and the scenario of maintaining security in the proposed algorithm has been enumerated in Figure 1. In this proposed strategy, the main agent that protects the information security over cloud environment is the organization's ITSS. Here, the ITSS partakes major roles in the cloud environments like selection of appropriate security parameter, selection of appropriate encryption algorithm and decreption algorithm, selection of appropriate keys, and partitioning of the overall data thereby enabling them to get deposited in the cloud. The foremost intention of this proposed architecture is to implement a strategy for controlling information security in cloud. In this background, the proposed strategy deals with dissimilar situations on the basis of the levels of sensitivity of information. In another angle, the proposed strategy rises the reliability of the clients in cloud computing, and this is observed to get increased by presenting control of information security to the end user ITSS.

The proposed model mainly concenterates in regulating the data security in cloud and is formulated on the basis of two main considerations:

(1) Controlling of security on the basis of ITSS of a definite company.

(2) Option in selecting the security preferences on the basis of dissimilar algorithm.

The proposed strategy is based on three scenarios so as to preserve data sensitivity. They are discussed below:

Scenario I: Security will be based on the selection of the ITSS of company based on the data suggested by the model.

Scenario II: On the basis of type of file, the proposed algorithm and the ITSS decides the choice.

Scenario III: Security will be on the basis of file encryption and dividing by ITSS of company with two prospects:

A. Files are Partitioned and then Encrypted in Particular Parts (Case 1)

This prospect is functioning on the basis of initially partitioning the files and then encryption is done on these partitioned files. This encryption is accomplished by the algorithm that gets selected by ITSS that are based on the data sensitivity in the company, as shown in Figure 3. This substitute is mainly desirable in case of reading the partition prior to complete retrieval of every partitions of the file. For instance, a video will start playing (signifies that no delay will be noticed by the user) prior to the retrieval of other segments of the file being uploaded over cloud.

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

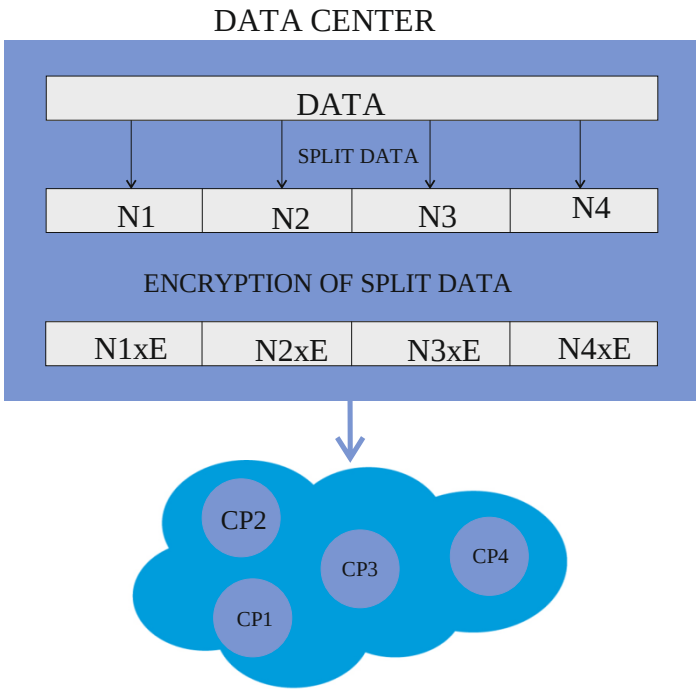

Figure 4. Schematic articulation of Files been partitioned, then Encrypted in particular parts (Case 1)

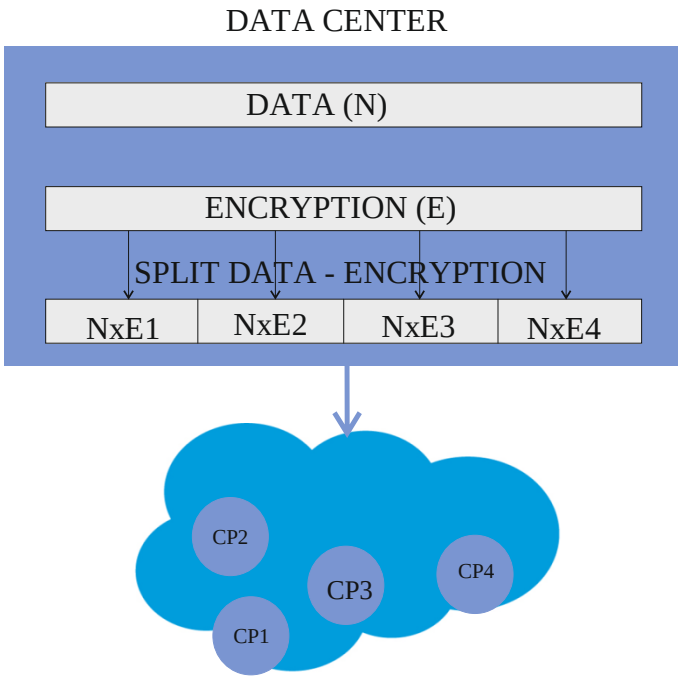

Figure 5. Articulation of files being encrypted and then partitioned into particular parts (Case 2)

The unpartitioned data (N) gets pattitioned in to N1, N2, N3, N4 and this is also called as data splitting, such that N= N1+N2+N3+N4. Subsequent to data split, the encryption of split data will be carried out, such that M= (N1xE)+(N2xE)+(N3xE)+(N4xE). Thereby, the encrypted data partitions will be uploaded in to the cloud storage.

B. The Files are Encrypted and then Partitioned into Particular Parts (Case 2)

In the second perspective of the proposed strategy, first the files are encrypted and then splitted into partitions on the basis of required conditions and the nature of algorithms to be employed. When compared with the previous prospective, this strategy is found to offer increased privacy while uploading the information to the cloud server, because the files cannot be read only using a single partition, every partitions are required to decrypt the encrypted file and to read the complete information. The articulation of files being encrypted and then partitioned into particular parts has been enumerated in Figure 5.

Every parts will be deposited in dissimilar clouds. An original file *N1*, encompasses nominated algorithm, indexing and location of the file. File *N1* will be considerably lesser in size, thereby encrypted by using the existing DSA procedure and will be stored wherever possible in the cloud server or at local appliance. The stages desired for our proposed strategy for increasing security over cloud storage is nominated using the following steps and hence called as a hybrid approach:

Step1. Key Generation Algorithm

Both the public and private keys are produced with the aid of RSA algorithm. The following are the steps involved in this algorithm:

a) Two separate outsized random prime numbers p and q were picked up.

b) Evaluate n = pxq, where n corresponds to modulo of public key and private key.

c) Evaluate totient as: $\phi(n) = (p-1)x(q-1)$.

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

d) Pick one integer e that corresponds to $1< e <\phi(n)$, and e and ϕ (n) possess nil factor except 1, where e represents the public key exponential.

e) Calculate d in order to satiate similarity relation $d \times e = 1$ modulo ϕ (n), here d represents the private key exponential.

f) The public key will be observed as (n, e) and private key will be observed as (n, d). Every parameters d, p, q have to be maintained secretly.

Step 2. Generation of Digital Signature

a) Prior to signing the documents, sender generates one message digest with the aid of hash functions.

b) Message digest represents crushed format of whole message, thereby any of the hash functions shall be employed to create the message digest.

c) The message digest M being generated, this shall be employed to sign the document by the usage of the private key.

d) The private key is represented by (n,d) and is employed for signing the document with the aid of S=Md modulo n.

e) The document being signed, subsequently it gets encrypted.

Step 3. Encryption of the Document

a) The document being signed, it will get encrypted.

b) For encryption of the document, Blowfish algorithm has been employed here.

c) This algorithm features sixteen round Fiestel structure with key dependent S-boxes.

d) XOR logic function is the principal operation being performed here at the outputs of each rows.

e) Completion of sixteen rounds of XOR operation, the encryption process gets completed.

Step 4. Decryption of the Document

a) Reversed Blowfish algorithm gets applicable here for decryption.

b) This offers message digest produced through digital signing of document.

Step 5. Verifying the Digital Signature

a) The receiver verifies the sender with the comparison of the digital signature gained post decryption and with the one saved in cloud server.

b) If the signatures are matched, the sender is designated as a verified sender.

IV. SIMULATION RESULTS AND DISCUSSIONS

The proposed algorithm has been implemented using Java NetBeans and the evaluated outcomes have been simulated with the aid of CloudSim. Simulation has been worked out for few parameters like uploading of the encrypted information in to the cloud, downloading of the decrypted information from the cloud, key generation and key updation. The performance of the proposed algorithm has been assessed against few well-evaluated existing algorithms like RHIBE_AES , RHIBE_HYBRID, RHABE_AES and RHABE_HYBRID, for the aforementioned parameters. Figure 6 and Table 1 shows the encryption times of the existing approaches. For a file size of 50 KB, RHIBE_AES, RHIBE_HYBRID, RHABE_AES and RHABE_HYBRID exhibits encryption times of 165 Sec, 170 Sec, 191 Sec and 127 Sec. Similarly, for a file size of 200 KB, RHIBE_AES, RHIBE_HYBRID, RHABE_AES and RHABE_HYBRID exhibits encryption times of 109 Sec, 111 Sec, 128 Sec and 58 Sec. Internal comparison amid the existing approach clearly show that RHABE_HYBRID exhibits least encryption time when compared to RHIBE_AES, RHIBE_HYBRID and RHABE_AES.

Table 1. Encryption Time of Existing Systems

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

File size (KB)	Encryption Time in Seconds			
	RHIBE_AES	RHIBE_HYBRID	RHABE_AES	RHABE_HYBRID
50	165	170	191	127
100	164	165	183	113
150	191	183	170	128
200	109	111	128	58

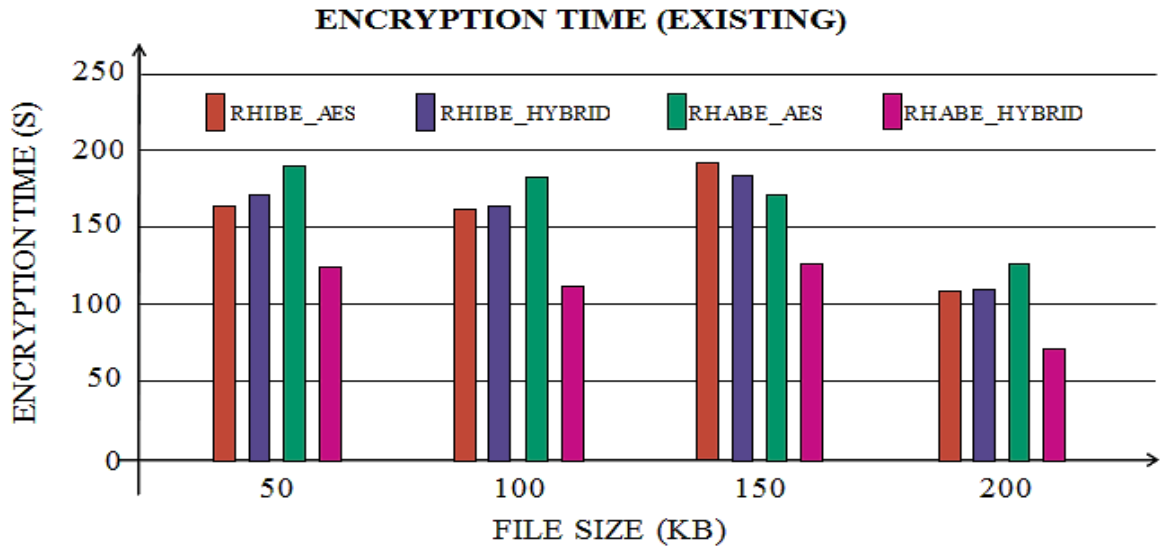

Figure 6. Evaluation of Encryption Time of Existing Systems

Figure 7 and Table 2 shows the encryption times of the existing approaches and the proposed approach. For a file size of 50 KB, RHIBE_AES, RHIBE_HYBRID, RHABE_AES, RHABE_HYBRID and Enhanced HPS exhibits encryption times of 165 Sec, 170 Sec, 191 Sec, 127 Sec and 98 Sec.

Table 2. Encryption Time in Enhanced HPS

File size (KB)	Encryption Time in Seconds				
	RHIBE_AES	RHIBE_HYBRID	RHABE_AES	RHABE_HYBRID	Enhanced HPS
50	165	170	191	127	98
100	164	165	183	113	86
150	191	183	170	128	96
200	109	111	128	58	30

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

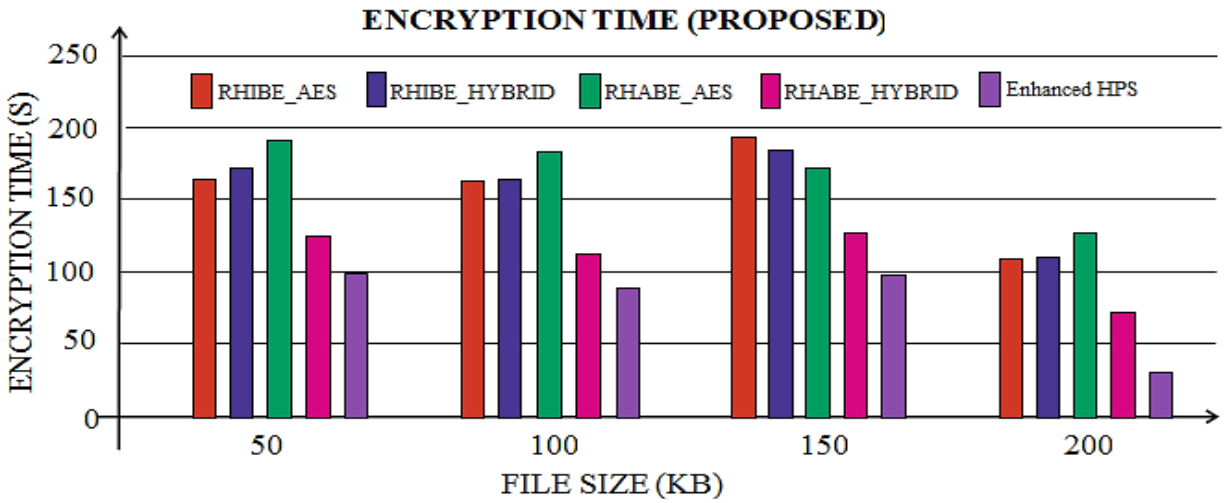

Figure 7. Assessment of Encryption Time in the Proposed Algorithm

Similarly, for a file size of 200 KB, RHIBE_AES, RHIBE_HYBRID, RHABE_AES, RHABE_HYBRID and Enhanced HPS exhibits encryption times of 109 Sec, 111 Sec, 128 Sec, 58 Sec and 30 Sec. The average encryption times of RHIBE_AES, RHIBE_HYBRID, RHABE_AES, RHABE_HYBRID and Enhanced HPS are 157.25 Sec, 157.25 Sec, 168 Sec, 106.5 Sec and 77.5 Sec. This clearly shows that, the proposed approach use least encryption time when compared with RHIBE_AES, RHIBE_HYBRID, RHABE_AES and RHABE_HYBRID.

Figure 8 and Table 3 shows the decryption times of the existing approaches. For a file size of 50 KB, RHIBE_AES, RHIBE_HYBRID, RHABE_AES and RHABE_HYBRID exhibits decryption times of 161 Sec, 168 Sec, 190 Sec and 125 Sec. Similarly, for a file size of 200 KB, RHIBE_AES, RHIBE_HYBRID, RHABE_AES and RHABE_HYBRID exhibits decryption times of 108 Sec, 109 Sec, 125 Sec and 56 Sec. Internal comparison between the existing approaches clearly reveal that, RHABE_HYBRID exhibits least decryption time when compared to RHIBE_AES, RHIBE_HYBRID and RHABE_AES.

Table 3. Decryption Time in Existing Systems

File size (KB)	Decryption Time in Seconds			
	RHIBE_AES	**RHIBE_HYBRID**	**RHABE_AES**	**RHABE_HYBRID**
50	161	168	190	125
100	161	160	180	110
150	150	151	168	98
200	108	109	125	56

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

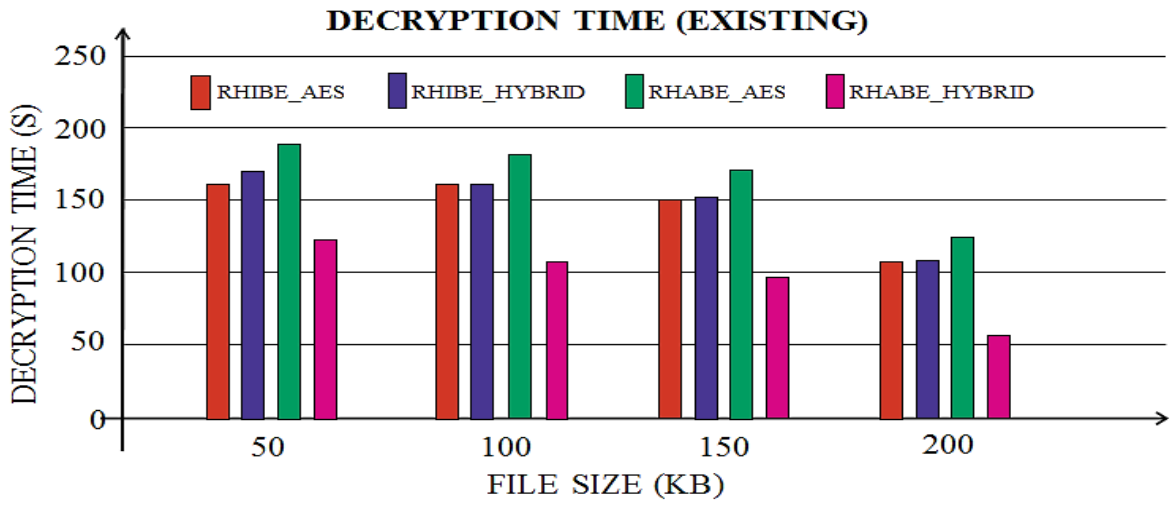

Figure 8. Assessment of Decryption Time in Existing Systems

Figure 9 and Table 4 shows the decryption times of the existing approaches and Enhanced HPS. Considering 50 KB file size, RHIBE_AES, RHIBE_HYBRID, RHABE_AES, RHABE_HYBRID and Enhanced HPS exhibits decryption times of 161 Sec, 168 Sec, 190 Sec, 125 Sec and 96 Sec. Correspondingly, for 200 KB file size, RHIBE_AES, RHIBE_HYBRID, RHABE_AES, RHABE_HYBRID and Enhanced HPS exhibits decryption times of 108 Sec, 109 Sec, 125 Sec, 56 Sec and 32 Sec. The average decryption times of RHIBE_AES, RHIBE_HYBRID, RHABE_AES, RHABE_HYBRID and Enhanced HPS are 145.00 Sec, 147.00 Sec, 165.75 Sec, 97.25 Sec and 71.75 Sec. Enhanced HPS use minimum decryption time when compared with other existing algorithms. This proves that data can easily be downloaded from cloud server using the proposed algorithm.

Table 4. Decryption Time in Enhanced HPS

File size (KB)	Decryption Time in Seconds				
	RHIBE_AES	RHIBE_HYBRID	RHABE_AES	RHABE_HYBRID	Enhanced HPS
50	161	168	190	125	96
100	161	160	180	110	83
150	150	151	168	98	76
200	108	109	125	56	32

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

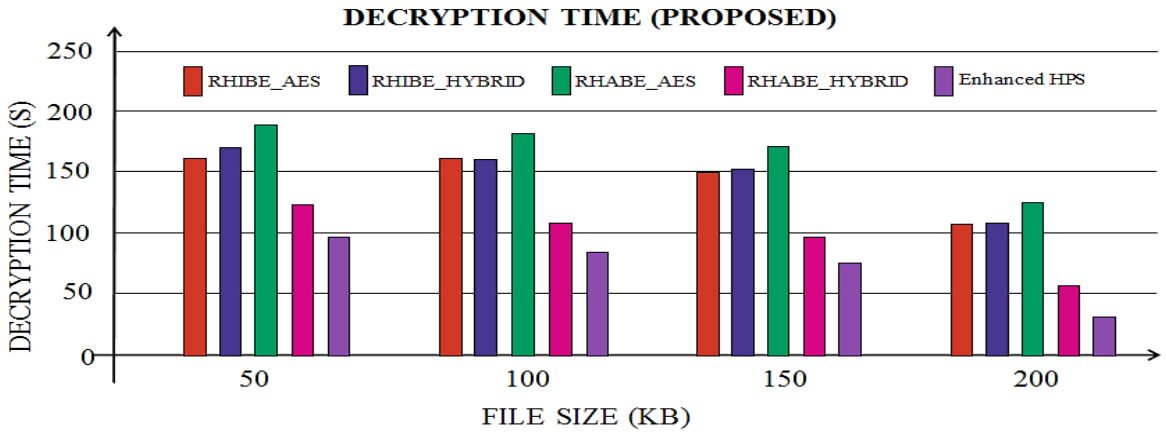

Figure 9. Evaluation of Decryption Time in Enhanced HPS

Figure 10 and Table 5 displays the key generation time of the existing approaches and Enhanced HPS for five attributes 10, 15, 20, 25 and 30. The average key generation times of RHIBE_AES, RHIBE_HYBRID, RHABE_AES, RHABE_HYBRID and Enhanced HPS are 3.7 Sec, 2.14 Sec, 3.34 Sec, 1.72 Sec and 1.32 Sec. Enhanced HPS employs minimum key generation time of 1.32 Sec., when compared with other existing algorithms. This is because of the employment of hybrid concepts in the proposed algorithm.

Table 5. Key Generation Time

Number of Attributes	Key Generation Time in Seconds				
	RHIBE_AES	RHIBE_HYBRID	RHABE_AES	RHABE_HYBRID	Enhanced HPS
10	3.2	1.8	3.0	1.6	1.2
15	3.6	2.0	3.2	1.7	1.4
20	4.0	2.0	3.5	1.7	1.5
25	4.2	3.0	4.0	2.0	1.2
30	3.5	1.9	3.0	1.6	1.3

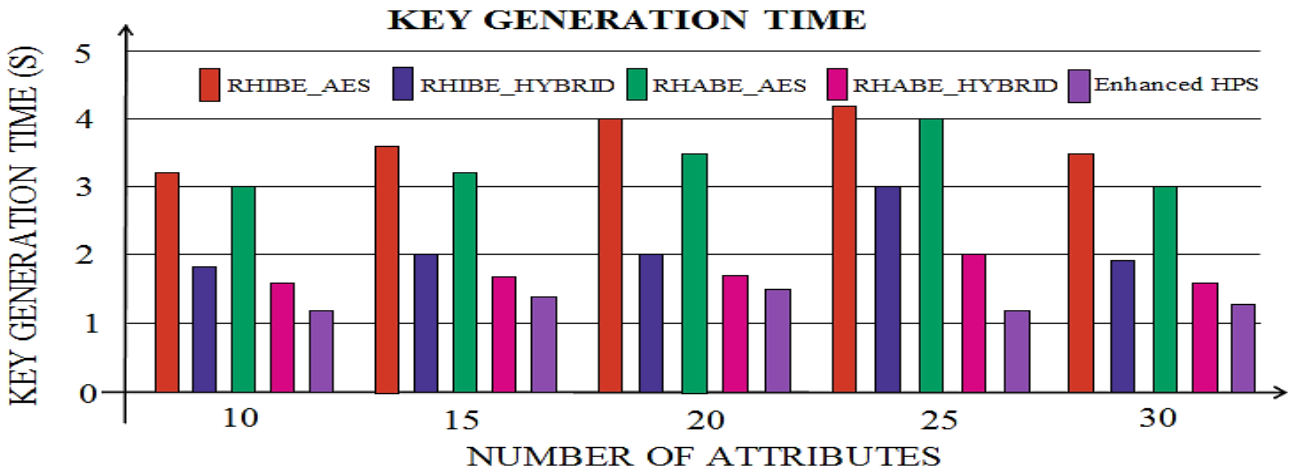

Figure 10.Assesment over Key Generation Time in Enhanced HPS

Figure 11 and Table 6 displays the assessment of key updation time in case of the existing approaches and Enhanced HPS for five attributes 10, 15, 20, 25 and 30. The average key generation times of

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

RHIBE_AES, RHIBE_HYBRID, RHABE_AES, RHABE_HYBRID and Enhanced HPS are 2.46 Sec, 2.18 Sec, 1.94 Sec, 1.66 Sec and 1.20 Sec. The proposed algorithm uses minimum key updation time of 1.20 Sec., when compared with RHIBE_AES, RHIBE_HYBRID, RHABE_AES and RHABE_HYBRID.

Table 6. Key Updation Time

Number of Attributes	Key Updation Time in Seconds				
	RHIBE_AES	RHIBE_HYBRID	RHABE_AES	RHABE_HYBRID	Enhanced HPS
10	1.7	1.6	1.3	1.2	0.8
15	2.5	1.9	1.7	1.5	1.1
20	3.1	2.7	2.5	2.0	1.4
25	3.3	3.1	2.9	2.4	2.0
30	1.7	1.6	1.3	1.2	0.7

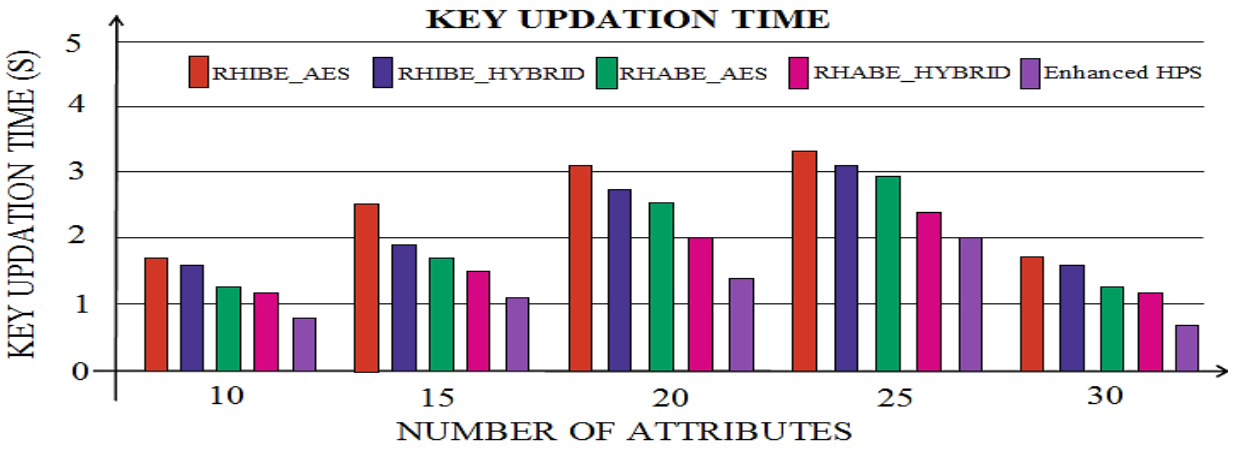

Figure 11. Evaluation of Key Updation Time in Enhanced HPS

Also, it is evident that the time to encrypt a file using the proposed hybrid algorithm fluctuates proportionately with respect to different file sizes.

V. CONCLUSION

The main reasons for moving towards cloud computing is its cost saving capability, easiness for usage, increased storage capabilities, better automation, increased flexibility, enhanced scalability, etc. Formulating secure algorithms while uploading data to cloud server, downloading data from cloud server and even when storing the data in the cloud server, has become a demanding task presently. In this paper, we have implemented a highly secure algorithm for attaining the aforementioned capabilities in cloud environment. Extensive simulation works were carried out to assess the performance of the proposed algorithm. The proposed algorithm was found to outperform the selected existing algorithms like RHIBE_AES, RHIBE_HYBRID, RHABE_AES and RHABE_HYBRID in terms of encryption while uploading, decryption while downloading and key generation/updation.

REFERENCES

[1] Gonzales, D., Kaplan, J. M., Saltzman, E., Winkelman, Z., & Woods, D. (2017). Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds.

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 11072 - 11084

IEEE Transactions on Cloud Computing, 5(3), 523–536. doi:10.1109/tcc.2015.2415794.

[2] Masiyev, K. H., Qasymov, I., Bakhishova, V., &Bahri, M. (2012). Cloud computing for business.2012 6th International Conference on Application of Information and Communication Technologies (AICT). doi:10.1109/icaict.2012.6398514.

[3] Lao, G., & Liu, H. (2011). Study of Mobile Payment Business Model Based on Third-Party Mobile Payment Service Provider.2011 International Conference on Management and Service Science. doi:10.1109/icmss.2011.5999096.

[4] Wang, X., & Min, Z. (2014). Parallel algorithm for Hill Cipher on MapReduce.2014 IEEE International Conference on Progress in Informatics and Computing. doi:10.1109/pic.2014.6972384.

[5] Eken, H. (2013). Security threats and solutions in cloud computing. World Congress on Internet Security (WorldCIS-2013). doi:10.1109/worldcis.2013.6751034.

[6] Liu, S., Zhang, C., & Bo, L. (2016). Improve security and availability for cloud storage. 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS). doi:10.1109/ccis.2016.7790288.

[7] Babitha M.P., &Babu, K. R. R. (2016). Secure cloud storage using AES encryption. 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT). doi:10.1109/icacdot.2016.7877709.

[8] Fathy, A., Tarrad, I. F., Hamed, H. F. A., &Awad, A. I. (2012). Advanced Encryption Standard Algorithm: Issues and Implementation Aspects. Advanced Machine Learning Technologies and Applications, 516–523. doi:10.1007/978-3-642-35326-0_51.

[9] Liu, L., Wang, D., Zhao, J., & Huang, M. (2013). SA4WSs: A Security Architecture for Web Services. Information and Communicatiaon Technology, 306–311. doi:10.1007/978-3-642-36818-9_32.

[10] Sharma, P., Sood, S. K., &Kaur, S. (2011). Security Issues in Cloud Computing. Communications in Computer and Information Science, 36–45. doi:10.1007/978-3-642-22577-2_5.

[11] Hani, A. F. M., Paputungan, I. V., &Fadzil Hassan, M. (2014). Service Level Agreement Renegotiation Framework for Trusted Cloud-Based System. Future Information Technology, 55–61. doi:10.1007/978-3-642-40861-8_9.

[12] Malina, L., Hajny, J., Dzurenda, P., &Zeman, V. (2015). Privacy-preserving security solution for cloud services. Journal of Applied Research and Technology, 13(1), 20–31. doi:10.1016/s1665-6423(15)30002-x.

[13] Hussain, S. A., Fatima, M., Saeed, A., Raza, I., &Shahzad, R. K. (2017). Multilevel classification of security concerns in cloud computing. Applied Computing and Informatics, 13(1), 57–65. doi:10.1016/j.aci.2016.03.001.

[14] Sengupta, N., &Chinnasamy, R. (2015). Contriving Hybrid DESCAST Algorithm for Cloud Security.Procedia Computer Science, 54, 47–56. doi:10.1016/j.procs.2015.06.006.

Published by: The Mattingley Publishing Co., Inc.