International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 24 (2017) pp. 15501-15508

An Analysis of Most Effective Virtual Machine Image Encryption Technique for Cloud Security

Mr. RakeshNag Dasari
Research Scholar, Department of computer science & Engineering,
KL University, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India.
Orcid Id: 0000-0001-6504-650X

Dr. Y. Prasanth
Professor, Department of computer science & Engineering,
KL University, Green Fields, Vaddeswaram, Guntur, Andhra Pradesh, India.

Dr. O. NagaRaju
Head & Asst. Professor, Department of Computer Science & Engineering,
SKBR Govt. Degree College, Macherla, Andhra Pradesh, India.
Orcid Id: 0000-0002-4906-529X

Abstract

Tremendous growth in cloud computing forced the application owners to push their application on to the cloud due to the demand for high availability of the customers. These migrations bring a high value addition to the customers and the application owners. Nevertheless, the security threads and vulnerability of the data with applications stopped various legacy applications to be moved to the cloud. A numerous number of research attempts made towards increasing the security of the cloud infrastructure, application access strategy, auditing methods or data security methods. However, the fundamental risk factors of stealing the raw data formats in terms of deployed virtual machine images cannot be addressed. Hence, this work proposes a framework to analyses and on demand deployment of the encryption methods for securing the VM image formats. The simplified approaches towards making a file secured cannot be directly concluded as the best method for VM image encryption as the speed of encryption and decryption will impact the service level agreements or the SLA from the cloud service providers. Thus the work addresses this issue and results into an automatic framework to dynamically change the encryption method. Also, a proper study of the encryption and decryption algorithms dealing with high volume data files is another outcome of this work.

Keywords: VM Image formats, DES, RSA, AES, Dynamic Encryption

INTRODUCTION

A wide range of security protocols are available for securing the content offline or while transmitting online. The security protocols deploy the security algorithms in order to achieve the goals. The security algorithms are popularly known as encryption algorithms. The encryption algorithms convert a plain data into human unreadable formats. Thus makes it significantly difficult from unauthorized access. Further, in order to read the data, the data owners must apply the reverse policy to decrypt the data by deploying decryption algorithms. These algorithms for encryption and decryption can be categorised into two major segments as symmetric and asymmetric based on the use of the secure key, which manipulates the algorithms. The symmetric algorithms use single sharable key for the encryption and decryption purposes and the asymmetric algorithms use a pair of public and private keys [1]. The existing algorithms use public key for the encryption algorithms and the private keys are used for decryption. A strong mathematical formulation is used for generating the public key. The strength of the algorithm depends on the key generation methods and thus makes the algorithms difficult to crack.

In the recent advancements of the research demonstrates the examples of the secure key algorithms such as DES and AES. The DES is considered to be a weaker than the AES algorithm as DES generates only 64 bit key and AES can generate keys of 128 bits or 192 bits or 256 bits [2].

The symmetric and asymmetric algorithms are different in the nature and classified based on the type of key used. Nevertheless, the algorithm categories are also different in terms of the network transmission. In case of symmetric algorithms, the encryption and decryption can be operated using a single public key and does not demand for a key distribution technique applied especially for cloud based applications. Also, the public key encryption is based on the mathematical calculations, which turns into inefficient methods in case of high volume of the data for a small computing capacity device [3]. In the other hand, the asymmetric algorithms uses a pair of public and private key, where before the transmission of the actual data key sharing is must and may cause additional load on the required network. This bottleneck or the trade-off between distribution [4] and computational load needs to be addressed in order to justify the demand of the application consumers for cloud service providers [5].

The rest of the work is organized such that, the Section – II reviews the popular algorithms for encryptions, the Section – III describes the characteristics of the VM image formats and clarified the guidelines for the appropriate encryption technique characteristics to be reached, in the Section – IV the proposed functional requirement evaluation framework is elaborated, the results are been discussed in the Section – V and this work presents the conclusion in the Section – VI.

REVIEW OF THE CURRENT RESEARCH OUTCOMES

The encryption algorithms as demonstrated in the work by Padmapriya et al. [6] and Prashanti.G et al. [7] are a widely accepted and used measures for securing the data. In case of the cloud services apart from the data, the virtual machine images are also to be protected. Thus in this section of the work, the analysis of the popular encryption algorithms is presented here:

A. Data Encryption Standard or DES

The first algorithm in this study is DES and referred under the category of symmetric algorithms.

Algorithm:

Step -1. Accept 64 bit plain text

Step -2. Generate 56 bit key

Step -3. Shift the plain text block parallel to the key bits

Step -4. Remove parity bits from the key

Step -5. Split key into 28 sections

Step -6. For each

Step -7. Rotate the keys

Step -8. Combine the sections

Step -9. Compression permutation to reduce the key from 56 bits to 48 bits

Step -10. End For

Step -11. The data block is split into two 32-bit sections.

Step -12. One half is subject to an expansion permutation to increase its size to 48 bits

Step -13. 48 bit key is exclusive-OR'ed with the 48 bit data section.

Step -14. Reduces the 48-bit block back down to 32-bits

Graphical Analysis of the DES Algorithms [Figure – 1]:

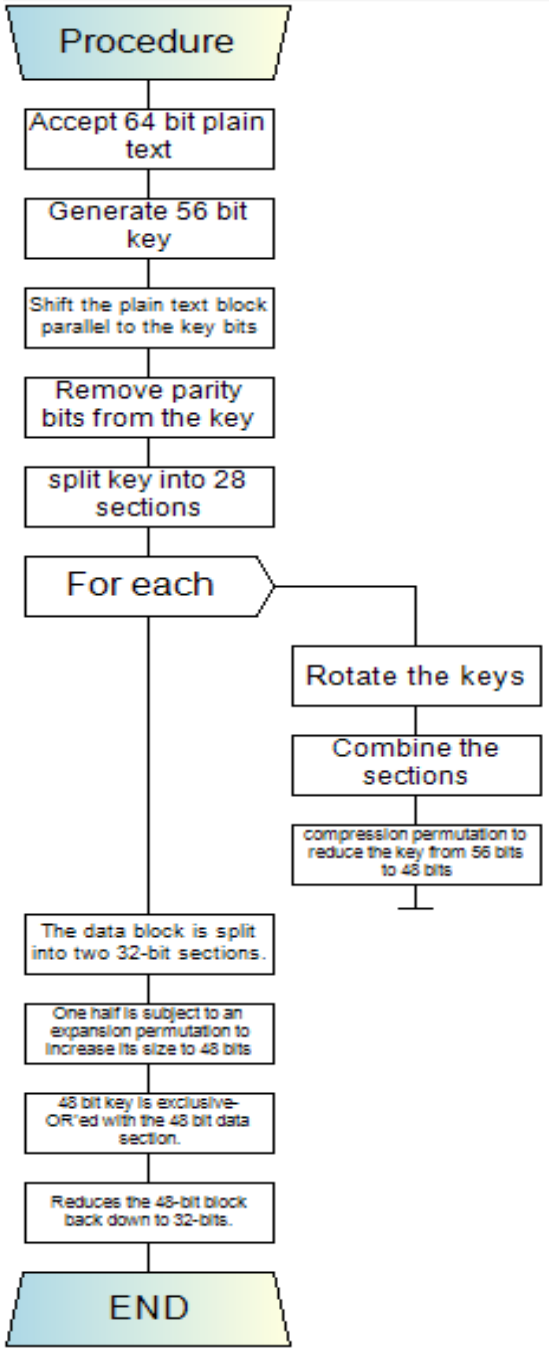

Figure 1: DES Algorithm Scheme

B. Advanced Encryption Standard or AES

The advanced encryption standard or the AES algorithm is highly popular for high security and high operational speeds.

Algorithm:

Step -1. Derive the set of round keys from the cipher key.
Step -2. Initialize the state array with the block data (plaintext).
Step -3. Add the initial round key to the starting state array.

Step -4. Perform nine rounds of state manipulation.
Step -5. Perform the tenth and final round of state manipulation.
Step -6. Copy the final state array out as the encrypted data (ciphertext).

Graphical Analysis of the AES Algorithms [Figure – 2]:

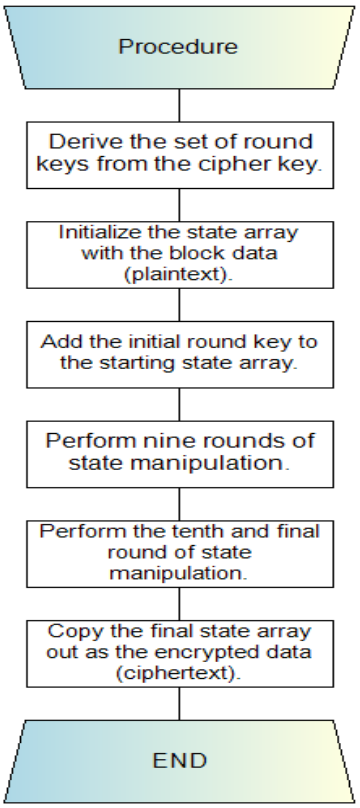

Figure 2: AES Algorithm Scheme

C. RIVEST, SHAMIR and ADLEMAN Standard or RSA

The recent advancements on the security key encryptions are based on RSA algorithm due to its nature of robustness.

Algorithm:

Step -1. Select a value of e from {3, 5, 17, 257,.. 65537}
Step -2. repeat
Step -3. p ← genprime(k/2)
Step -4. until (p mod e) ≠ 1
Step -5. repeat
Step -6. q ← genprime(k - k/2)
Step -7. until (q mod e) ≠ 1
Step -8. N ← pq
Step -9. L ← (p-1)(q-1)
Step -10. d ← modinv(e, L)
Step -11. return (N, e, d)
Step -12. Obtains the recipient B's public key (n, e).
Step -13. Represents the plaintext message as a positive integer m, 1 < m < n [see note 4]
Step -14. Computes the ciphertext c = me mod n.
Step -15. Sends the ciphertext c to B
Step -16. Uses his private key (n, d) to compute m = cd mod n.
Step -17. Extracts the plaintext from the message representative m

Graphical Analysis of the RSA Algorithms [Figure – 3]:

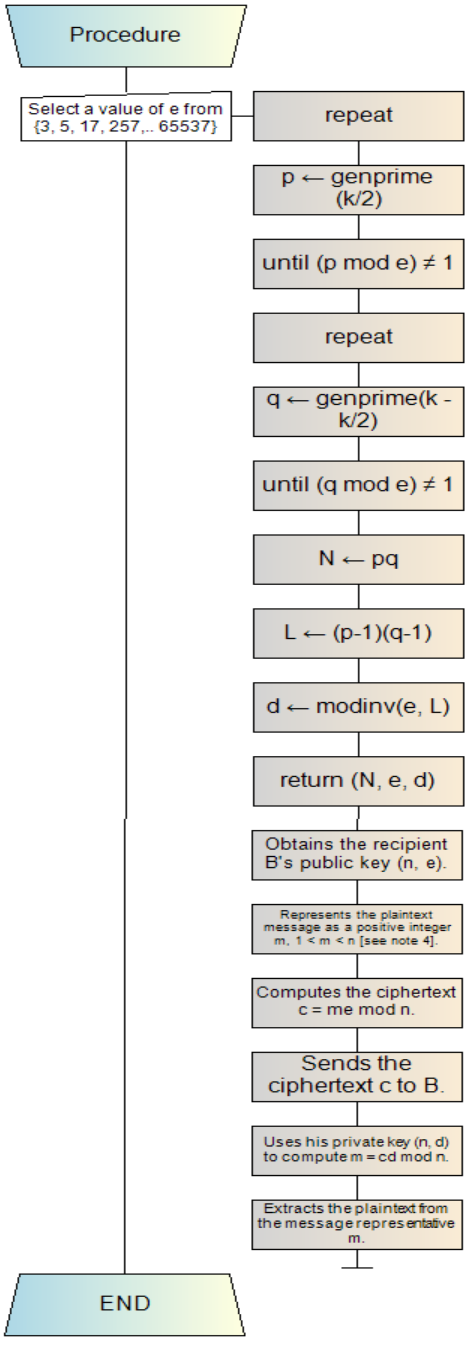

Figure 3: RSA Algorithm Scheme

Thus with the understanding of the security algorithms, this work analyses the VM image format and characteristics in the next section.

VM IMAGE FORMAT CHARACTERISTICS

The Virtual Machine Image is similar to the standard hard disk file. The partitioned properties are also similar to the physical hard disk containers [8] [9].

The virtual machine image or the virtual hard disk is very popular for the properties like moving the image file seamlessly over multiple host server systems, easy backups and recovery powered by snapshot mechanism, applicability of security patch and antivirus software stacks, replication control powered by guest to host and vice versa and finally the life cycle management controls.

Here also we understand the types or the formats of virtual machine images to be stored and compared [10] [11]:

A. Fixed Length Image File Format:

The Fixed Length Image File Format needs to be configured at the beginning of the virtual machine creation. Once created the complete file size allocation needs to assigned and once assigned the size cannot be reduced or increased.

This file format is limited in use as the growth of data and applications generating more data cannot be predefined.

B. Dynamic Length Image File:

On the other hand, Dynamic Length Image File is a variable length image format. The Dynamic Length Image File can be extended by size automatically when the data or the size of the software stacks need to be increased.

However the increment happens by the multiple of data block size, which is generally defined at 512MB in most of the systems.

The problem with Dynamic Length Image File is if the small amount changes need to be applied on parallel replicated systems, then the complete file needs to be replaced.

Hence due to the lack of delta change management properties, the portability is restricted in these files.

C. Dependent Image File:

Due to the problems of delta change management in previous file formats, the Dependent Image File manages the complete change management with a property called Undo Change. This property connects the modified file with the previous file as child file only with the change information.

Hence this file format is majorly accepted due to its portability for movements over multiple host servers.

However in above mentioned file formats, the complete isolation is employed from host server file systems for security reasons. Sometimes the need to share the files or locally generated server logs can be useful for managing applications better, thus this is a noted limitations in all the file formats.

D. Linked Image File:

The Linked Image File formats are majorly similar to the other file formats, except the property of connectivity between the physical hard drive and the logical hard drives.

This feature enables the developers and researchers to closely analyses and incorporates the server based file systems into the application and increases the efficiencies for some cases of application development like emulated storage or physically reading the network parameters through the applications.

PROPOSED EVALUATION FRAMEWORK

The proposed framework is built on the existing data centre architecture. The enhancements in this framework are inclusion of two additional layers including four different components [Figure – 4].

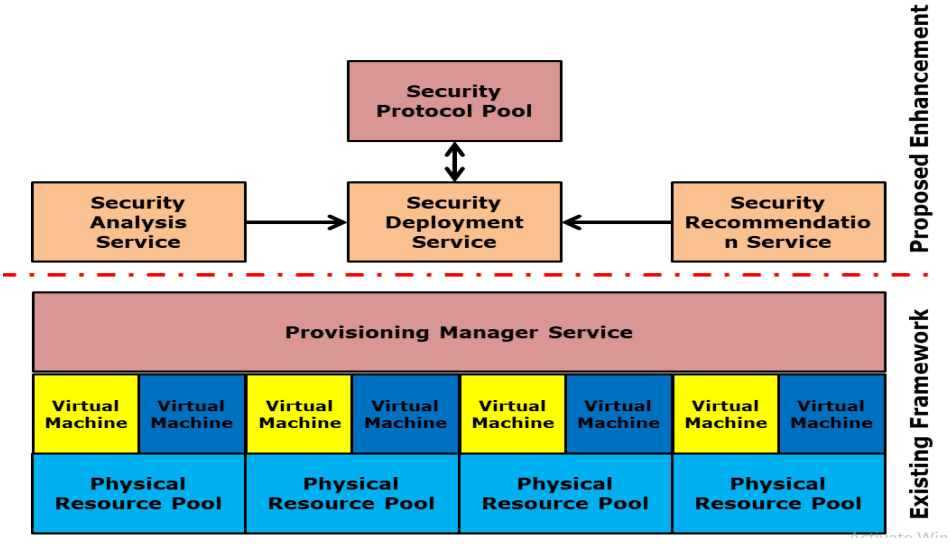

Fig. 4 Proposed Framework Enhancement

In this section of the work, the novel components are elaborated.

A. Security Analysis Service:

The first service is the security analysis service, where the virtual machines are been analyzed to find whether the virtual machine images are encrypted or not. If the virtual machine images are not encrypted, the cumulative report is send to the security recommendation service.

B. Security Recommendation Service:

The next service is the security recommendation service, where based on the size, load and the SLA time the appropriate security services are recommended to the security deployment service.

C. Security Protocol pool:

The security protocol pool is the large collection of the existing security algorithms, which are discussed in the previous section of this work. The deployment service chooses the security application based on the recommendations.

D. Security Deployment Service:

The security deployment service receives the recommendations from the recommendation services and chooses the algorithm from the security pool. Further, this service is responsible for the actual encryption and decryption operations on the demand during VM access or VM provisioning.

The proposed algorithm is furnished here:

Algorithm:

Step -1. Accumulate the virtual machine information

Step -2. for each virtual machine <<Check for security>>

Step -3. if security == encrypted

Step -4. continue

Step -5. else

Step -6. Analyse load and analyse size

Step -7. Recommend encryption technique

Step -8. if the time_for_encryption + time_for_decryption < SLA

Step -9. Choose the encryption technique

Step -10. else

Step -11. Find next security recommendation

Step -12. EndIf

Step -13. Deploy encryption technique

Step -14. EndIf

Step -15. EndFor

The flow of the algorithm is also demonstrated here [Figure -5]:

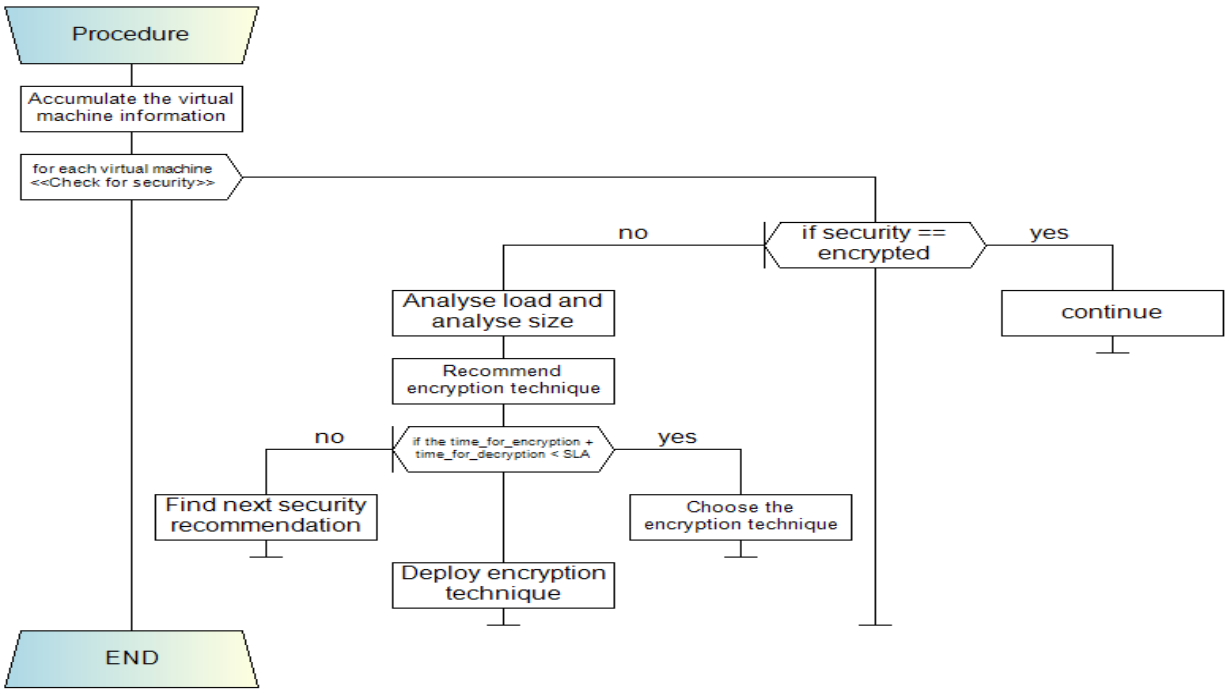

Figure 5: Proposed Algorithm for Security Recommendation

In the next sections, based on the proposed setup, the results are evaluated.

RESULTS & DISCUSSION

In the light of the security protocols and the virtual machine image formats, the security algorithms are been tested on the various virtual machine image sizes. During the analyses the duration for the encryption and the decryptions are been recorded.

A. Encryption Time Analyses

Firstly, the duration for each file size for each algorithm with encryption time is analysed [Table – 1].

TABLE I: ENCRYPTION TIME ANALYSIS

VM Image File Size	Encryption Time (Sec)		
	DES	AES	RSA
16 GB	175448.0105	328965.0196	800481.5477
32 GB	350896.0209	657930.0392	1600963.095
64 GB	701792.0418	1315860.078	3201926.191
128 GB	1403584.084	2631720.157	6403852.382
256 GB	2807168.167	5263440.314	12807704.76
512 GB	5614336.335	10526880.63	25615409.53
1 TB	11228672.67	21053761.25	51230819.05

The results are also been analysed graphically [Figure – 6].

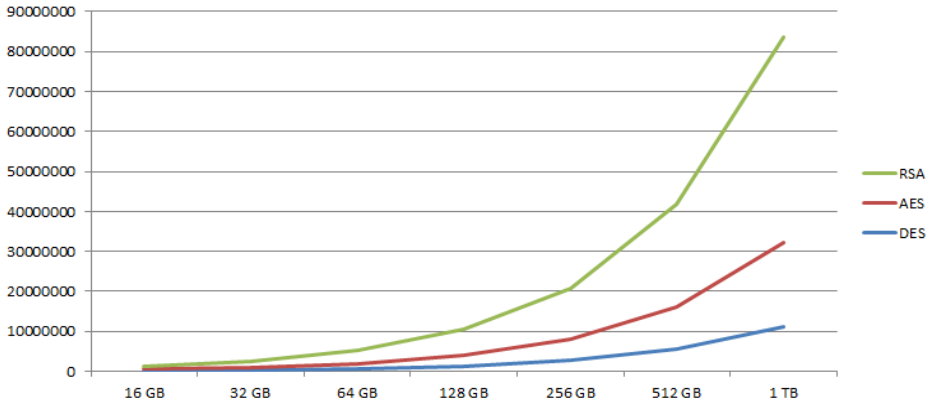

Figure 6: Encryption time for each VM Image file

B. Decryption Time Analyses

Secondly, the duration for each file size for each algorithm with decryption time is analysed [Table – 2].

TABLE II: DECRYPTION TIME ANALYSIS

VM Image File Size	Decryption Time (Sec)		
	DES	AES	RSA
16 GB	109655.0065	120620.5072	537309.532
32 GB	219310.0131	241241.0144	1074619.064
64 GB	438620.0261	482482.0288	2149238.128
128 GB	877240.0523	964964.0575	4298476.256
256 GB	1754480.105	1929928.115	8596952.512
512 GB	3508960.209	3859856.23	17193905.02
1 TB	7017920.418	7719712.46	34387810.05

The results are also been analysed graphically [Figure – 7].

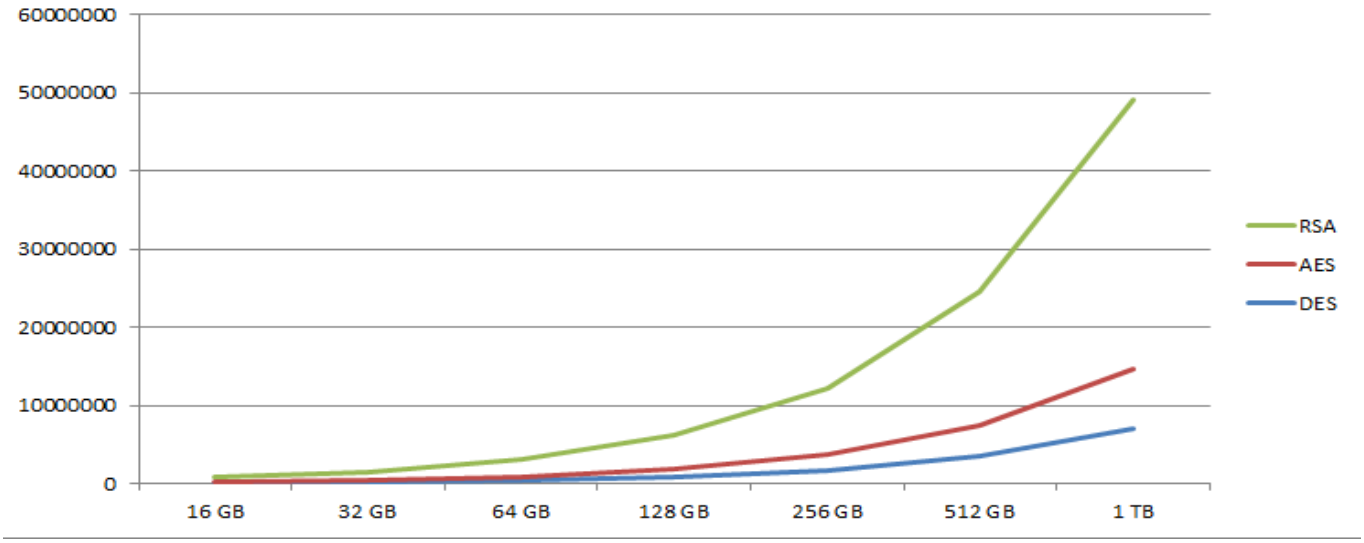

Figure 7: Decryption time for each VM Image file

C. SLA Time Analyses Overheads

Finally, the total time for VM access increased due to the encryption is considered [Table – 3].

TABLE III: ADDITIONAL SLA TIME ANALYSIS

VM Image File Size	Decryption Time (Sec)		
	DES	AES	RSA
16 GB	285103	449585.5	1337791
32 GB	570206	899171.1	2675582
64 GB	1140412	1798342	5351164
128 GB	2280824	3596684	10702329
256 GB	4561648	7193368	21404657
512 GB	9123297	14386737	42809315
1 TB	18246593	28773474	85618629

The results are also been analysed graphically [Figure – 8].

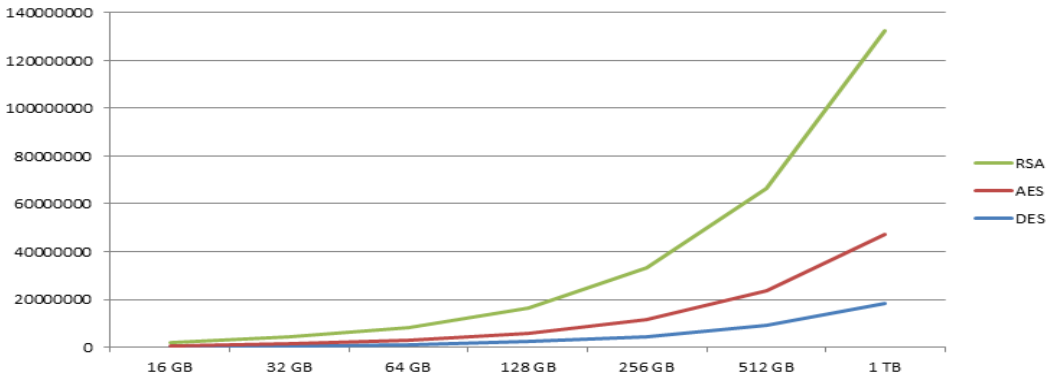

Figure 8: Time addition to the SLA

Thus this it is natural to understand that the increasing size of the virtual machine forces the RSA algorithms to take more time for encryption and decryption, thus adding more time to the SLA.

CONCLUSIONS

The security issues for the cloud computing models are unignorably critical. The research outcomes have demonstrated the security recommendations for the data, applications, data generated by the application and network. Nevertheless, the security measures are not been addressed for the underlying virtual machine images. Though, the virtual machine images are in raw format and service related information cannot be extracted directly, nonetheless the VMs can be replicated easily from the VM Images. Thus, encrypting the VM images is also a goal of cloud security, which was been ignored. This work demonstrates the use of various security algorithms for encryption and decryption for VM image security. It is to be concluded that the RSA algorithm takes a higher amount of time for the security operations but at the same time, RSA provides the higher security. Thus, this work recommends choosing the security algorithm based on SLA committed from the service providers and the application owners to the consumers.

REFERENCES

[1] Idrizi, Florim, Dalipi, Fisnik & Rustemi, Ejup. “Analyzing the speed of combined cryptographic algorithms with secret and public key”. International Journal of Engineering Research and Development, e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 8, Issue 2 (August 2013),pp. 45

[2] Abdul.Mina, D.S, Kader, H.M. Abdual & Hadhoud, M.M. “Performance Analysis of Symmetric Cryptography”. pp. 1.

[3] Chehal Ritika, Singh Kuldeep. “Efficiency and Security of Data with Symmetric Encryption Algorithms”. International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X , Volume 2, Issue 8, August 2012, pp. 1.

[4] Hardjono, "Security In Wireless LANS And MANS,"Artech House Publishers 2005.

[5] Elminaam, Diaa Salama Abd, Abdual Kader, Hatem Mohamed & Hadhoud, Mohiy Mohamed. “Evaluating The Performance of Symmetric Encryption Algorithms”. International Journal of Network Security, Vol.10, No.3, May 2010, pp. 216.

[6] Padmapriya, Dr.A, Subhasri, P. “Cloud Computing: Security Challenges & Encryption Practices”. International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 3, Issue 3, March 2013, pp. 257.

[7] Prashanti.G, Deepthi.S & Sandhya Rani.K. ”A Novel Approach for Data Encryption Standard Algorithm”. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013, pp. 264.

[8] P. Padala Automated management of virtualized data centers, 2010 :Univ. of Michigan

[9] T. Patikirikorala, A. Colman, J. Han and L. Wang "A systematic survey on the design of self-adaptive software systems using control engineering approaches", Proc. Symp. Softw. Eng. Adaptive Self-Manag. Syst., pp.33 - 42 2012

[10] X. Wang and Y. Wang "Coordinating power control and performance management for virtualized server clusters", IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 2, pp.245 -259 2011

[11] X. Wang, M. Chen and X. Fu "MIMO power control for high-density servers in an enclosure", IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 10, pp.1412 -1426 2010