An Improved Encryption and time effective method for live VM migrations with Reduced SLA Violation

Shesagiri Taminana1 , D.Lalitha Bhaskari2

1Research Scholar, Computer Science & Systems Engineering, Andhra University College of Engineering(A), Andhra University, Visakhapatnam, India.

2Professor, Dept of Computer Science & Systems Engineering, Andhra University College of Engineering(A), Andhra University, Visakhapatnam, India.

[1]tsgiri32@gmail.com, [2]lalithabhaskari@yahoo.co.in

ABSTRACT : The immense growth in the field of cloud-based hosting for higher application reliability, the demand for security aspects on the cloud, not only for the data, rather for the application resources are also increasing. The application management on cloud can utilize the benefits of micro-services and the platform readiness of the cloud service providers. Nevertheless, the hosting of the applications and application resources on the cloud are realized using the virtualization contents. The virtualization again relies on the virtual machines on the cloud-based data centres. During dynamic load balancing the virtual machines migrates from one physical instance to another and during the migration process, the virtual machines often get exposed to the other unauthorized parties, who have access to the same network or communication channel. As a matter of fact, the virtual machine file formats or virtual machine images are transmitted over the network in plain file format and this makes the virtual machine data highly vulnerable to the attacks. In the recent time, a good number of research attempts can be observed which aim to solve this challenge. Nonetheless, the effectiveness of these methods are highly argued for higher complex computations and the extra computing demands for encryption and decryption are utilized from the assigned computing capabilities for application hosting, eventually making the application performance compromised and failing the complete purpose of the application hosting on cloud. Hence, this work proposes a novel encryption algorithm specifically designed for the large-scale data encryption and decryption on the virtual machine images. The proposed algorithms are tested on the real time benchmarked applications and during the testing, apart from increasing the application security with 20% improvements and reduced time complexity by 40%, 30% improvement on the SLA violation reduction can also be observed.

Keywords: Virtual Machine, Encryption, Progressive Algorithm, Security, Network Transmission Security, Adaptive Algorithm

DOI Number: 10.48047/nq.2022.20.19.NQ99232 **NeuroQuantology2022;20(19): 2723-2733**

1. Research Introduction

The dedicated industry for application development is always prioritized the application performance and deployment effectiveness for the customers. These non-functional requirements have accelerated the adaptation of the cloud computing and application hosting on the cloud-based data centres. On the cloud data centres, the physical infrastructure is shared between multiple consumers and the isolation is achieved using virtualization.

The work by Barham et al. [1] have significantly elaborated the benefits and challenges of utilizing the virtualization technology for cloud-based infrastructure

management. The major benefit of the cloud-based hosting is the dynamic load balancing to improve the application reliability with a higher responsiveness and almost zero downtime. This fact is well demonstrated in the work by Clark et al. [2].

For the live migration, the performance relies on the virtualization technique to host the applications are supporting infrastructure on the virtual machine images and the improvements over the traditional architecture is compared in the work by Padala et al. [3]. Nonetheless, the maintainability of the virtual images, apart from the security aspects, is high and the service providers of cloud services struggle to keep it environment friendly as demonstrated in the report by Murugesan et al. [4].

The environment suitability is the discussion for the data centre owners and cannot be really justified in the scope of this research. Henceforth, this research focuses on the security aspects of the virtual machine images during live migration [Fig – 1].

The rest of the work is furnished such that in Section – II, the parallel research outcomes are discussed, in Section – III, the security issues of the virtual machine files are discussed, in Section – IV, the proposed algorithms are furnished, in Section – V, the obtained results are discussed, in Section – VI, the comparative analysis is furnished and finally in Section – VII, the research conclusion is presented.

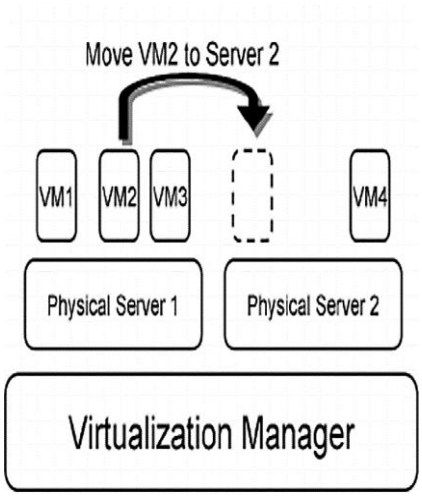

Figure 1: Virtual Machine Migration

2. VIRTUAL MACHINE SECURITY – PARALLEL RESEARCH OUTCOMES

The demand for the higher performing and higher responsiveness from the application have intrigued the adaptation of the cloud services for application hosting and management. Nonetheless, this adaptation has also increased the risk factors on application securities. The work Djenna et al. [5] have clearly listed the potential risk factors for cloud-based application hosting.This work is basically an updated and tested report on the projections made in the work by Ristenpart et al. [6] in the year of 2009, which was the early cloud adaptation years. Nonetheless, the security aspects of the virtual machines are always been a challenge to address due to various reasons such as the huge size of the VM image file formats and the time restrictions for the migration tasks. The work Fan et al. [7] have significantly outlined the bottlenecks. Thus, many researchers have also aimed to identify the phases of the live migrations and the effect on the virtual machine images to discover the correct phase for applying the security aspects. This is clearly demonstrated in the work by Oberheide et al. [8]. Must later, based on the principles recommended,

the work of Yamunadevi et al. [9] showcases the encryption methods. This is also highly criticised for higher time complexity and not been able to justify the need for SLA validations [Fig – 2].

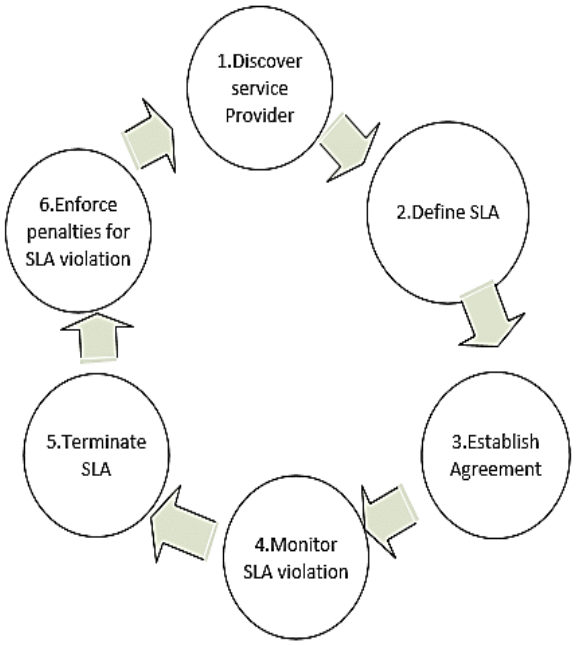

Figure 2: Sla Life Cycle

In the recent times, many of the parallel research outcomes can be observed to justify the security aspects during live migration process. One such attempt is the work of Huang et al. [10]. This work primary proposes multiple solutions to handle the memory leakages of the virtual machine images. Nonetheless, this work is also been criticised for not considering the other security aspects. In the similar direction, the work by Dawoud et al. [11] proposes embedding the security modules into the infrastructure, such that during the virtualization process, the security mechanisms can work like a service to the applications.

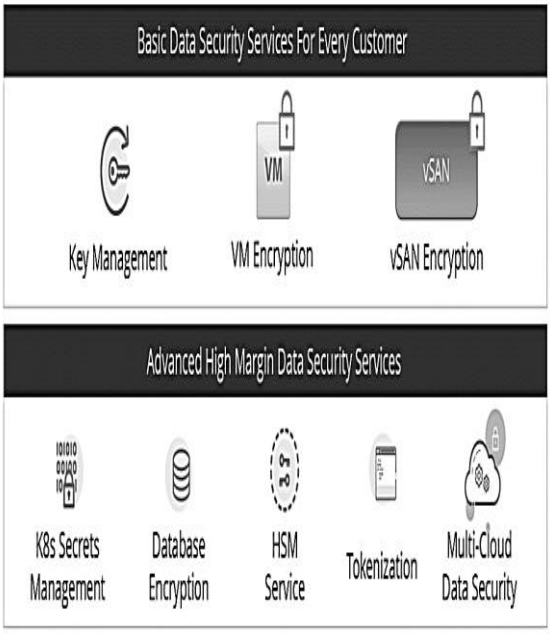

Figure 3: Security as a service

In the continuation of the security aspects for virtual machine during live migrations, the work of Anala et al. [12] have recommended a complete single solution for all around security for the virtual machines. This work is also been criticised for higher complexity for adaptations.In the same year, yet another outcome can be observed to improve these recommendations in the work by S. Biedermann et al. [13]. Many of the recommendations are argued relying on the fundamental principles designed and presented byA. Back et al. [14] and J. Oberheide et al. [15].

Few parallel benchmarked applications such as the work by R. Mathivanan et al. [16] have elaborated the use of Two-Fish encryption algorithm for cloud-based data encryption. This algorithm is criticized for higher time complexity during the virtual machine encryption process. Also, the work by Gangireddy et al. [17] have also suggested the use of blowfish encryption algorithm for cloud-based virtual machine encryption. Nonetheless, this work is criticized by the other researchers for higher implementation complexity,

which makes it difficult to adopt. Finally, the work by S. Artheeswari et al. [18] showcases the use of IDEA encryption techniques, which is again constrained by higher number of iterations or higher time complexity.

Henceforth, this work recommends the following measures to be adapted for generating the perfect VM encryption strategy during live migration:

Analyse the existing VM encryption algorithms and identify the bottlenecks Propose a novel algorithm for analysing application behaviours and detect deviation towards a security threat using machine learning techniques Propose a novel method for encrypting a higher volume VM image in less time by deploying a progressive and adaptive encryption method Identify the SLA improvements with the proposed algorithms

Henceforth, in the next section of this work, the security restrictions are summarized for further problem formulations.

3. Security Challenges During The Virtual Machine Live Migrations

In this section of the work, the security challenges are been summarized for designing the proposed algorithms in the next section of this work.

Virtual Machine Ownership Control: Firstly, the improper access controls to any virtual machine is the server farm can conceivably permit any unapproved client to have full oversight over the virtual machine and permit those clients to make, relocate or end the virtual machine accessible.

- Virtual Machine Access Restrictions: Secondly, during the live movement of the virtual machines over the organization requests a high common trust between the actual source, network regulators and the objective actual framework. Any infringement of the trust variables can prompt the openness of the information in the organization.

- Virtual Machine Life Cycle Management: Thirdly, because of non – observing of the virtual machine life cycles can prompt the perpetual harm to the virtual machines accessible in the server farm. Additionally, it is in any case to make reference to that the observing of the virtual machines should be gotten to forestall the unapproved access by the inspectors.

- Virtual Machine Data Protection: Fourthly, as consistently examined in this work, during the relocation interaction of the virtual machines, the information can be profoundly shaky without giving any altogether effective encryptions. The virtual machines during movement can be accessible as clear content to the organization clients and can without much of a stretch be altered.

- Virtual Machine Live Migration over Secure Channels: Fifth, explaining the fourth point, the aggressors in the organization can totally access the correspondence channel and alter all information transmissions. These sorts of assaults are called channel harming. The assailants regularly utilize the ARP or DHCP or DNS conventions to convey these assaults.

- Virtual Machine State Stability: Further broadening the past focuses, the information can be for all time adjusted during the movement interaction and this can influence the information to be burned-through or delivered by the

application running on the virtual machines. Routinely, it has been seen that the information created by the influenced virtual machine applications makes genuine harms the results of the applications.

- Virtual Machine Rigidity: It is likewise being seen that the unapproved admittance to the server farm virtual machine stacks can start high volume of live movements to the focused on objective frameworks. This may cause high and unmanaged burdens to the objective frameworks making the application late responder to the solicitations and coming about into inaccessible applications or virtual machines.

- SLA and SLA Violation: A service-level agreement (SLA) defines the level of service you expect from a vendor, laying out the metrics by which service is measured, as well as remedies or penalties should agree-on service levels are not achieved. It is a critical component of any technology vendor contract. The SLA specifies the time frame within which tickets, calls and calls must be received. If the clients do not receive a response or the call is not answered within the specified time, an SLA violation occurs.

- Thus, based on the outlined recommendations made in this section of the work, in the next section of this work, the proposed algorithms are furnished.

4. PROPOSED ALGORITHMS

- After the detailed understanding of the parallel research outcomes and identification of the problem in the previous sections of this work, in this section, the proposed algorithms are furnished.

- The fundamental motivation of proposing the algorithms is mainly two as firstly, a novel algorithm for analysing application behaviours and detect deviation towards a security threat using machine learning techniques as this reduces the time complexity of the proposed algorithm and secondly, a novel method for encrypting a higher volume VM image in less time by deploying a progressive and adaptive encryption method again for reducing the time complexity and reduce SLA violations.

Firstly, the key generation algorithm is furnished.

Algorithm - I: Virtual Machine Encryption Key Generation using Adaptive Master Key Method (VMEK - AMK) Algorithm
Input: KS[], 32-bit length Key collection Output: MS as master key
Process: Step - 1. Load the KS[] Step - 2. For each element in the set KS[] as KS[i] a. Length = Length(KS[]) - i b. Count = Count(KS[]) - i c. Generate the interim key, IK[i] = KS[i] * Length * Count * P(KS[i]/KS[]) d. MS = MS XOR IK[i] e. If Count == 0 i. Then, Return MS f. Else i. Continue

- Key calculations require both the sender and the beneficiary of a message to have a similar master key. All early cryptographic frameworks required either the sender or the beneficiary to by one way or another get a duplicate of that mysterious key over a truly secure channel.

- Practically all advanced cryptographic frameworks actually utilize symmetric-key calculations inside to encode the heft of the messages, yet they wipe out the requirement for a truly secure channel by utilizing Diffie–Hellman key trade or some other public-key convention to safely come to concurrence on a new mystery key for each message.

- Secondly, the encryption algorithm is furnished here.

• Algorithm - II: Virtual Machine Encryption using Adaptive Master Key (VME-AMK) Algorithm
• Input: VM[], Virtual machine image data and MS, Master Key • Output: VMS, Encrypted Virtual machine image data
• Process: • Load VM[] • For each element in the VM as VM[i] • Separate data header, DH and data block DB from VM[i] • Encrypt DH as DHS[i] = DH XOR MS[0..n/2] and DB as DBS = DB XOR MS[n/2..n] • Merge the VM blocks as VMX[i] = Merge (DHS[i], DBS[i]) • Apply final encryption as VMS[i] = VMX XOR MS • Return the encrypted VM file as VMS[]

- Encryption is a sort of encryption where just one key (a mysterious key) is utilized to both scramble and decode electronic data. The substances conveying by means of symmetric encryption should trade the key with the goal that it tends to be utilized in the unscrambling cycle. This encryption strategy contrasts from topsy-turvy encryption where a couple of keys, one public and one private, is utilized to scramble and unscramble messages.

- Distributed computing can be considered as service supplier that includes conveying facilitated services over the Web. It doesn't mean treatment of the application utilizing nearby or individual assets nor utilizing the devoted organization to offer support like office or home organization. Purchasers and suppliers both need to confront a few difficulties disregarding getting to numerous utilities as an interaction in distributed computing. Service level agreement (SLA) is a typical authoritative record where both the gathering needs to consent to the agreements for provisioning and burning-through the service. Henceforth, SLA assumes a significant part in distributed computing to get to service true to form with a couple of practical limits. The target of this paper is to clarify momentarily the significance of SLA in distributed computing alongside periods of its lifecycle, format, and boundaries. This paper likewise proposes test SLA format on which premise service provisioning and checking being done effectively.

Finally, the decryption algorithm is furnished.

Algorithm - III: Virtual Machine Decryption using Adaptive Master Key (VMD-AMK) Algorithm
Input: VMS, Encrypted Virtual machine image data

and MS, Master Key Output: VM, Decrypted Virtual machine image data
Process: Step - 1. Load VMS Step - 2. Separate data header, DH and data block DB from VMS Step - 3. Decrypt DH as DHD = DH XOR MS[0..n/2] and DB as DBD = DB XOR MS[n/2..n] Step - 4. Merge the VM blocks as VMX = Merge (DHD, DBD) Step - 5. Apply final decrypt as VM = VMX XOR MS Step - 6. Return the decrypted VM file as VM

Key cryptography depends on a common key between two gatherings. Uneven key cryptography utilizes a public-private key pair where one key is utilized to encode and the other to decode. Symmetric cryptography is more effective and subsequently more appropriate for encoding/unscrambling enormous volumes of information. Uneven cryptography isn't proficient and along these lines utilized uniquely for trading a common key, after which the symmetric key is utilized to scramble/unscramble information.

Henceforth, in the next section of this work, the obtained results are furnished and discussed.

5. Obtained Results and Discussions

After the detailed discussions on the proposed algorithms, in this section of the work, the obtained results are furnished and discussed. The obtained results are highly satisfactory and demonstrated significant improvements over the existing methods.

The work is simulated on CloudSim with the CloudLab dataset. The current CloudLab organization comprises of in excess of 25,000 centers appropriated across three locales at the College of Wisconsin, Clemson College, and the College of Utah. CloudLab interoperates with existing testbeds including GENI and Emulab, to exploit equipment at many destinations all throughout the planet.

Firstly, the size of the virtual machine images is analysed during 5 trials [Table – 1].

Table. 1 VM File Size Analysis

Trial #	Min VM File Size (GB)	Avg VM File Size (GB)	Max VM File Size (GB)	Total number of VM Files
1	4	47.4	88	40
2	4	49.15	97	15
3	4	51.6	99	45
4	4	52.45	99	23
5	4	51.64	99	46

Considering the average size of the virtual machine files, it is natural to observe that, the generic encryption methods cannot handle such extensive files and shall increase the time complexity to a greater extend. Thus, the fundamental claim made in this work is proven. The results are also visualized graphically here [Fig – 4].

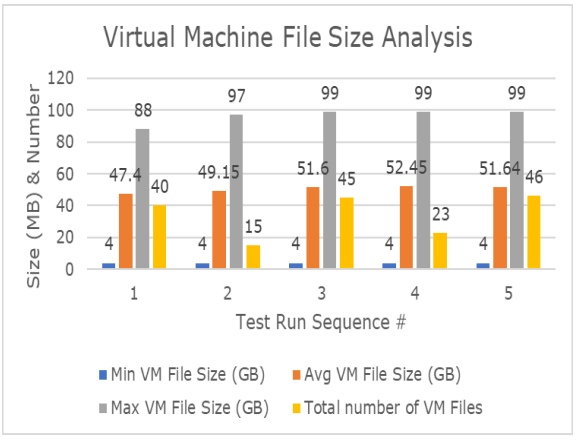

Figure 4: Virtual Machine File Size Analysis

Secondly, based on the proposed encryption algorithm, the encryption and decryption key generation times are analysis [Table – 2].

TABLE. 2 KEY GENERATION TIME ANALYSIS

Trial #	Min Key Generation Time (ms)	Avg Key Generation Time (ms)	Max Key Generation Time (ms)
1	0.00	961.50	1599.00
2	0.00	1522.30	2474.00
3	0.00	2050.87	3590.00
4	0.00	2577.78	4573.00
5	0.00	3129.76	5816.00

It is significant to observe the time complexity reduction for key generation as well. The proposed algorithm for key generation relies on a multi-order adaptive iteration. In spite of the higher complexity of the proposed algorithm, due to the progressive adaptation of the key values from the previous steps, during iteration, the actual time complexity is less. The results are visualized graphically here [Fig – 5] and the key generation demonstrates a nearly linear trend.

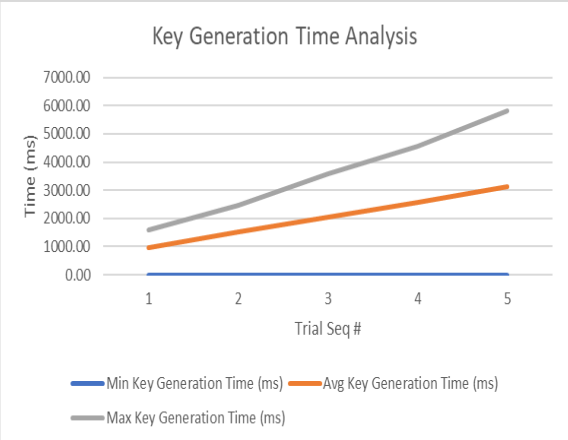

Figure 4: Key Generation Time Complexity Analysis

Thirdly, the encryption time complexity is analysed here [Table – 3].

TABLE. 3 VM FILE ENCRYPTION TIME ANALYSIS

Trial #	Min Encryption Time (ms)	Avg Encryption Time (ms)	Max Encryption Time (ms)
1	0.00	48.70	481.00
2	0.00	24.80	481.00
3	0.00	16.73	481.00
4	0.00	12.75	481.00
5	0.00	10.38	481.00

The encryption time, during the trials, are found to be significantly low as the average of average time complexity out of 5 trials are observed as 22.67 ms. Regardless to mention, considering the size of the virtual machine file sizes, the observed encryption time is significantly low. The results are visualized graphically here [Fig –6].

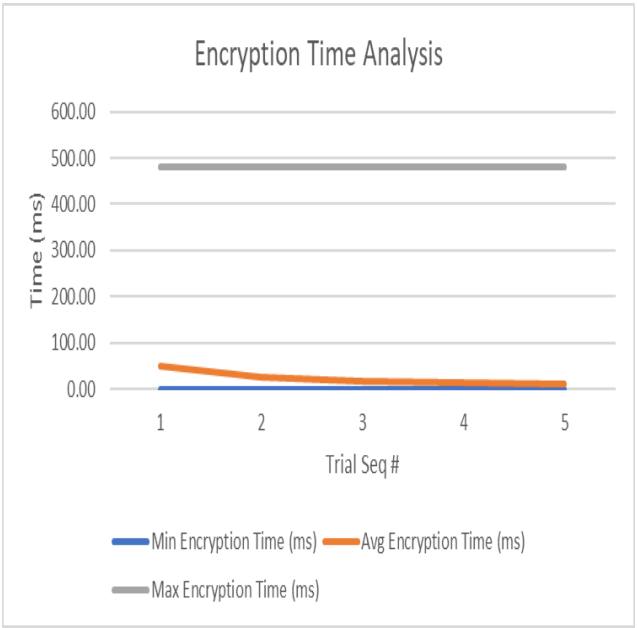

Figure 6: VM File Encryption Time Complexity Analysis

It is to be clearly observed that, the worst-case time complexity or the maximum time complexity during all test runs are same, which significantly indicates the higher stability of the proposed algorithm.

Fourthly, the decryption time complexity analysis is carried out here [Table – 4].

TABLE. 4 VM FILE DECRYPTION TIME ANALYSIS

Trial #	Min Decryption Time (ms)	Avg Decryption Time (ms)	Max Decryption Time (ms)
1	0.00	0.10	1.00
2	0.00	0.05	1.00
3	0.00	0.07	1.00
4	0.00	0.05	1.00
5	0.00	0.18	7.00

The results are visualized graphically here [Fig – 7].

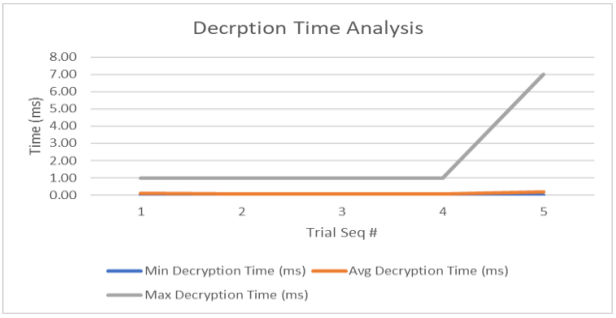

Figure 5: VM Vile Decryption Time Complexity Analysis

Finally, the SLA violation during the encryption and decryption is analysed here [Table – 5]. A total of 20 trail results are furnished here to realize the possibilities of the violation of the SLA due to the added security services.

TABLE. 5 SLA VIOLATION ANALYSIS

Trial #	SLA Violation (%)
1	0.45
2	0.74
3	0.54
4	0.16
5	0.31
6	0.79
7	0.83
8	0.13
9	0.62
10	0.43
11	0.53
12	0.43
13	0.24
14	0.32
15	0.71
16	0.27
17	0.41
18	0.96
19	0.55
20	0.13

The results are visualized graphically here [Fig – 8].

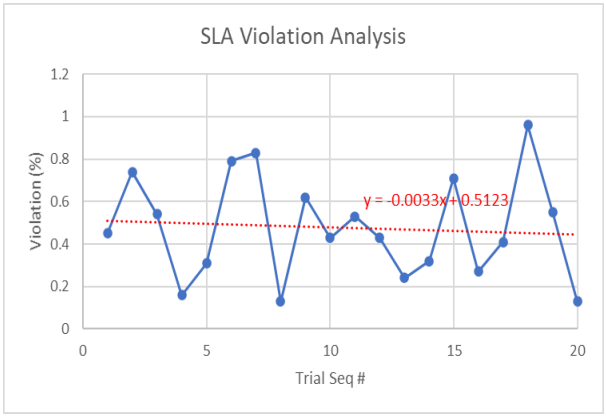

Figure 6: VM Vile Decryption Time Complexity Analysis

It is significantly to observe that, the SLA violation have never reached near to 1% also and this can conclusively prove the effectiveness of the proposed algorithms. The dotted line in the above graph demonstrates the possibilities of predicting the SLA violation (%) in the future as well, which is again derived automatically using the linear regression standard formulation.

Henceforth, in the next section of this work, the comparative analysis is carried out.

6. Comparative Analysis

After the detailed analysis of the obtained results, in this section of the work, the proposed system is compared with the parallel benchmarked research outcomes. The parameters for comparison are adopted from the work by M. Aiash et al. [19] and furnished here [Table – 6].

TABLE. 6 COMPARATIVE ANALYSIS [16]

Comparative Parameters	The CoM Framework	The vTPM	The LMDF	Proposed Method
Access Control	Yes	No	No	Yes
Data Confidentiality	Yes	Yes	No	Yes
Communication	No	Yes	Yes	Yes
Data Integrity	No	Yes	Yes	Yes
Availability	Yes	No	No	Yes

Henceforth, it is natural to realize that, the proposed method has outperformed the parallel research outcomes on all possible aspects.

Further, in the next section of this work, the final research conclusion is presented.

7. Research Conclusion

The security of the virtual machine is one of the highest priorities of cloud security. Thus, realizing the demand of the recent research, this work formulates three novel key generation and encryption & decryption algorithms for large scale files such as virtual machine images. During the course of the research, firstly this work proposes a novel adaptive security key generation algorithm using the interim key and master key concepts. This proposed algorithm demonstrates a very low time complexity and during testing records as low as 900 ms for key generation. Further, this work also proposes two adaptive algorithms for virtual machine encryption and decryption using the separation of the files into two blocks as file descriptor and file data contents. This strategy is significant in establishing the ground-breaking innovation for making the auditing of the files highly secure and removes the risk of potential data breeches during the auditing processes. The proposes encryption and decryption method records as low as 22 ms and 10 ms of time complexity during testing.

REFERENCES

[1] Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., Warfield, A.: Xen and the art of virtualization. In: Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles (SOSP19), pp. 164–177. ACM Press (2003)

[2] Clark, C., Fraser, K., Hand, S., Hansen, J.G., Jul, E., Limpach, C., Pratt, I., Warfield, A.: Live migration of virtual machines. In: Proceedings of NSDI, pp. 273–286. USENIX Association, Berkely (2005)

[3] Padala, P., Zhu, X., Wang, Z., et al.: Performance evaluation of virtualization technologies for server consolidation. Virtualiz. VMware ESX Serv. 9, 161–196 (2007)

[4] Murugesan, S.: Harnessing green IT: principles and practices. In: Proceeding of IT Professional, vol. 10, pp. 24–33. IEEE Computer Society (2008)

[5] Djenna, A., Batouche, M.: Security problems in cloud infrastructure. In: The 2014 International Symposium on Networks, Computers and Communications, pp. 1–6. IEEE (2014)

[6] Ristenpart, T., Tromer, E., Shacham, H., et al.: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: CCS Conference, pp. 199–212 (2009)

[7] Fan, W., Kong, B., Zhang, Z.J., Wang, T.T., Zhang, J., Huang, W.Q.: Security protection model on live migration for KVM virtualization. J. Softw. 27(6), 1402–1416 (2016). (in Chinese)

[8] Oberheide, J., Cooke, E., Jahanian, F.: Empirical exploitation of live migration of virtual machines. In: Black Hat DC Briefings, Westin Washington DC City Center (2008)

[9] Yamunadevi, L., Aruna, P., Sudha, D.D., et al.: Security in virtual machine live migration for KVM. In: 2011 International Conference on Process Automation, Control and Computing (PACC), pp. 1–6. IEEE (2011)

[10] Fan, W., Huang, W.Q., Jiang, F., Liu, C., Lv, B., Wang, R.R.: Research on security of memory leakage in live migration based virtualization. In: Twenty-Fourth National Conference on Information Security (IS 2014), vol. 09, pp. 12–17 (2014)

[11] Dawoud, W., Takouna, I., Meinel, C.: Infrastructure as a service security: challenges and solutions. In: The 7th International Conference on Informatics and Systems (INFOS), pp. 1–8 (2010)

[12] Anala, M.R., Shetty, J., Shobha, G.: A framework for secure live migration of virtual machines. In: 2013 International Conference on IEEE Advances in Computing, Communications and Informatics (ICACCI), pp. 243–248 (2013)

[13] S. Biedermann, M. Zittel and S. Katzenbeisser. Improving Security of Virtual Machines during Live Migrations. Eleventh Annual Conference on Privacy, Security and Trust (PST). 2013.

[14] A. Back, U. Mller, and A. Stiglic. Traffic Analysis Attacks and Trade-Offs in Anonymity Providing Systems. Information Hiding, volume 2137 of Lecture Notes in Computer Science, page 245-257. Springer, 2001.

[15] J. Oberheide, E. Cooke, F. Jahanian.Empirical Exploitation of live migration of virtual machines. Proc of Black Hat DC, March 24, 2008.

[16] M. Aiash, G. Mapp and O. Gemikonakli, "Secure Live Virtual Machines Migration: Issues and Solutions," 2014 28th International Conference on Advanced Information Networking and Applications Workshops, Victoria, BC, Canada, 2014.