Modified H-HABE and Most Common Encryption and Decryption Algorithms using Different Operating Systems

G.Narmadhai , S. Vijay Bhanu

*Abstract***:** *Cloud computing has been viewed as the cutting edge engineering of Information Technology(IT). The Cloud worldview included preferences and its potential for decreasing expenses and time for an administration that favors towards security issues. Distributed computing is a total of data technology(IT) that offered to the client dependent on renting. Despite the fact that countless security issues are tended to, in any case some are not tended to and a few calculations are proposed for security issues. This paper shows an on the diverse Operating Systems of utilizing our refreshed H-HABE calculations and contrast and the different most normal encryption instruments. A near report made on a few encryption methods are utilized in the Different Operating Systems in the cloud. At long last, the real measurements like distinctive working framework issues present in distributed computing are examined.*

Keywords: Cloud Computing, Operasting System, Encryption, Decryption, Security, Comparative Study

1. INTRODUCTION

Cloud computing is the capacity instrument for different kinds of electronic information, for example, databases, Software, Platforms, Communication Services, Commercial information stockpiles and so forth. The security is likewise an exceptionally huge issues for the substance in the capacity at cloud. Different encryption components are utilized to shield information from unapproved access just as from the misfortunes, assaults, hacks and so on. There are techniques utilized, for example, open key framework, Identity based encryption(IBE) just as fluffy character based encryption strategy. The characteristic based encryption(ABE) is likewise an another technique to encode the substance by utilizing properties as it were. This paper substance few of these strategies to verify distributed storage by utilizing property based validation and their measurements like working frameworks. Numerous touchy information can be verified by utilizing this component and this idea is additionally distributed in a Form.

II. PROBLEM STATEMENT

In previous algorithms, ABE,BH-WABE and H-HABE there are many problems, i.e., high speed during the period of encryption and decryption. These algorithms have some of the issues like different operating system that are resolved in

   G.Narmadhai, Research Scholar, Department of Computer Science, Annamalai University,Annamalai Nagar- 608 002.
   Dr. S. Vijay Bhanu, Assistant Professor, Department of Computer Science & Engineering, Annamalai University Annamalai Nagar – 608 002.

proposed algorithm. In proposed work an algorithm is developed.

III. SYSTEM PARAMETERS

The experiments are conducted in For our experiment, three laptops of 32 bit configuration are used: [1]. Intel Pentium® Dual Core with Windows XP [2]. Intel Pentium® Dual Core with Windows Vista and [3]. Intel Pentium® Dual Core with Windows 7. The size of input plaintext data varies from 1MB, 2MB,: : :,10MB. The experiments will be repeated several times and one text, audio, video and image file to ensure that results are reliable and effective to check with existing algorithms.

Hacking is the greatest problem in the Cloud Computing. Many algorithms like ABE,BH-WABE and H-HABE have been used to prevent the outside attacks to eavesdrop or to prevent the data to be transferred to the cloud. In this work, the four most popular cryptographic algorithms like ABE,BH-WABE, H-HABE and updated H-HABE have been studied and their speed with different operating systems are analysed and compared. Their efficiency for encrypting text and image across different widely used in three operating systems like Windows XP, Windows Vista and Windows 7 are compared. The simulation results show the performance of the encryption methods across the different platforms.

For our experiment, three laptops of 32 bit configuration are used:

1. Processor: Intel Core i3 4150, RAM: 4GB DDR3, Asus H81M-V3 with Windows XP

2. I Processor: Intel Core i3 4150, RAM: 4GB DDR3, Asus H81M-V3 with Windows Vista and

3. Processor: Intel Core i3 4150, RAM: 4GB DDR3, Asus H81M-V3 with Windows 7.

The tasks that will be performed are shown as below:

• A comparison is made between the results of the different encryption and decryption schemes in terms of encryption time on three different windows platforms, Windows XP, Windows Vista and Windows 7.

• The study is made for four different data types viz., text , audio, video and image

IV. EXPERIMENTAL RESULTS

The front end tools are installed in all the three laptops. This tool encrypt one text files of size nearly 500KB, one image files sized 200KB, one audio file in wav format and their files

size is 245Kb and one video file in the format MP4 and their size is 5MB. First their encryption time in ms (milliseconds)is calculated and then their mean execution speed is calculated in Mb/sec (Megabytes per second).

Table 1: Encryption Speed (in Mb/sec) for the Algorithms on Different OS for Text File

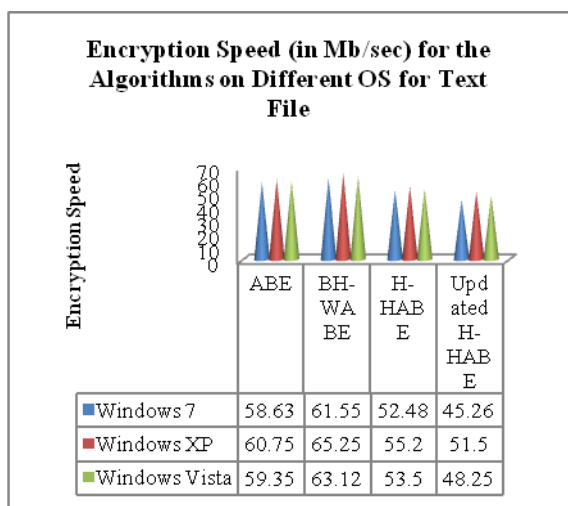| Encryption\OS	Windows 7	Windows XP	Windows Vista
ABE	58.63	60.75	59.35
BH-WABE	61.55	65.25	63.12
H-HABE	52.48	55.20	53.50
Updated H-HABE	45.26	51.50	48.25

Figure 1: Encryption Speed (in Mb/sec) for the Algorithms on Different OS for Text File

In this work, the four most common and popular symmetric cryptographic algorithms like ABE,BH-WABE, H-HABE and updated H-HABE have been studied and their efficiency are analysed and compared. Their efficiency for encrypting text and image across different widely used operating systems like Windows XP, Windows Vista and Windows 7 are compared. The simulation results show the performance of the most common encryption methods across the different platforms.

Table 2: Encryption Speed (in KB/sec) of Most Common Algorithms on Different OS for Image Data

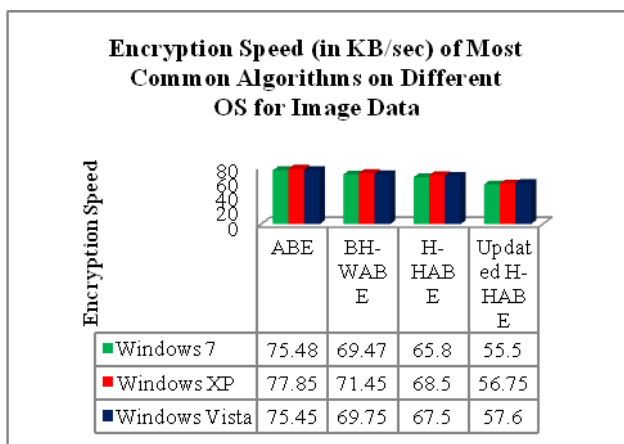| Encryption\OS	Windows 7	Windows XP	Windows Vista
ABE	75.48	77.85	75.45
BH-WABE	69.47	71.45	69.75
H-HABE	65.80	68.50	67.50
Updated H-HABE	55.50	56.75	57.60

Figure 2: Encryption Speed (in KB/sec) of Most Common Algorithms on Different OS for Image Data

But, The simulation results show the performance of the most common encryption methods across the different platforms using Image. Here in this research work Updated H-HABE is better in Windows 7 operating System compared with other operating systems like Windows XP, and Windows Vista.

Table 3: Encryption Speed (in KB/sec) of Most Common Algorithms on Different OS for Audio Data

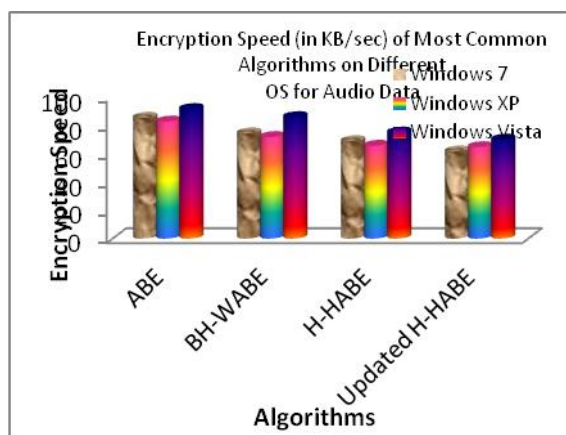| Encryption\OS	Windows 7	Windows XP	Windows Vista
ABE	85.25	82.55	91.35
BH-WABE	74.20	71.65	85.70
H-HABE	68.75	65.51	74.80
Updated H-HABE	61.50	64.55	69.80

Figure 3: Encryption Speed (in KB/sec) of Most Common Algorithms on Different OS for Audio Data

But, The simulation results show the performance of the most common encryption methods across the different platforms using audio data. Here in this research work Updated H-HABE is better in Windows 7 operating System compared with other operating systems like Windows XP, and Windows Vista.

Table 4: Encryption Speed (in KB/sec) of Most Common Algorithms on Different OS for Video Data

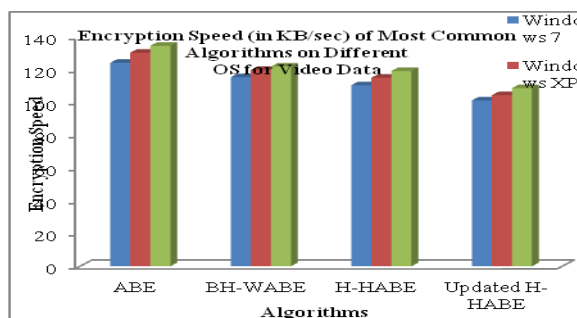| Encryption\OS	Windows 7	Windows XP	Windows Vista
ABE	124.25	130.45	134.65
BH-WABE	115.40	119.85	121.90
H-HABE	110.55	115.10	119.25
Updated H-HABE	101.25	104.50	108.75

Figure 4: Encryption Speed (in KB/sec) of Most Common Algorithms on Different OS for Video Data

The simulation results show the performance of the most common encryption methods across the different platforms using video data. Here in this research work Updated H-HABE is better in Windows 7 operating System compared with other operating systems like Windows XP, and Windows Vista.

V. COMPARISON

Consequently by security perspective all the ABE,BH-WABE and H-HABE existing frameworks isn't that much dependable. Here it is thought about our proposed algorithm(updated H-HABE) with other existing calculations based on certain parameters like proficiency in the various stages. So as to legitimize that our proposed work is more effective than others, here it is presented new encryption procedure which high effectiveness in the various stages for encryption and unscrambling.

In this part here it contrasted our work and other existing strategies. It is spoken to our outcome with regards to various parameters like ascertaining effectiveness in the various stages for different calculations.

VI. CONCLUSION

There are more necessities to verify the information transmitted over various cloud utilizing various administrations. To give the security to the cloud and information distinctive encryption strategies with various working frameworks are utilized. In this paper, an overview on the current chips away at the encryption methods utilizing diverse working frameworks has been finished. As indicated by research done and writing overview it tends to be discovered that our proposed calculation like refreshed H-HABE is most effective as far as three distinctive working frameworks with various document sizes.

REFERENCE

1. Waleed, AL-Museelem, and Li Chunlin. "Client Privacy and Security in Cloud Computing." International Journal of Security and Its Applications 10.2 (2016): 341-352.
2. Wu, Jiehong, Ilia Detchenkov, and Yang Cao. "An investigation on the power utilization of utilizing cryptography calculations in cell phones." Software Engineering and Service Science (ICSESS), 2016 seventh IEEE International Conference on. IEEE, 2016.
3. Bhandari, Akshita, Ashutosh Gupta, and Debasis Das. "Secure calculation for distributed computing and its applications." Cloud System and Big Data Engineering (Confluence), 2016 sixth International Conference. IEEE, 2016.
4. Jakimoski, Kire, "Security Techniques for Data Protection in Cloud Computing." International Journal of Grid and Distributed Computing(2016): 49-56.
5. Vanya Diwan, Shubhra Malhotra, Rachna Jain. (2014, April 4) "Cloud Security Solutions: Comparison among Various Cryptographic Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering
6. Bokefode Jayant.D, Ubale Swapnaja A, Pingale Subhash V., Karane Kailash J. , Apate Sulabha S. ,"Creating Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role bases Access Control Model", International Journal of Computer Applications, Volume 118-No.12, May 2015.
7. Karun Handa, Uma Singh," Data Security in Cloud Computing utilizing Encryption and Steganography", International Journal of Computer Science and Mobile Computing", Vol.4 Issue.5, May-2015, pg.786-791.
8. Manzoor Hussain Dar, Pardeep Mittal and Vinod Kumar, 'A Comparative Study of Cryptographic Algorithms', International Journal of Computer Science and Network. June (2014) ISSN(Online):Volume 3, Issue 3.
9. R.Gowthami Saranya and A.Kousalya,"A Comparative Analysis of Security Algorithms Using Cryptographic Techniques in Cloud Computing", International Journal of Computer Science and Information Technologies, ISSN: 0975-9646, Vol. 8 (2), 2017, 306-310.
10. Diaa Salama Abdul.Elminaam, Hatem Mohamed Abdul kader, Mohie Mohamed Hadhoud," Studying the Effects of Most Common Encryption Algorithms" , International Arab Journal of e-Technology(IAJeT),Vol.2,No.1,PP:1-10, January 2011.
11. J. Raigoza and K. Jituri, "Assessing Performance of Symmetric Encryption Algorithms," in Proceedings - 2016 International Conference on Computational Science and Computational Intelligence, 2017, pp. 1378–1379.
12. M.A.Bahnasawi, K.Ibrahim, A. Mohamed, M. K. Mohamed, A. Moustafa, K. Abdelmonem, Y. Ismail, and H. Mostafa, "ASIC Oriented Comparative Review of Hardware Security Algorithms for Internet of Things Applications," in Proceedings of the International Conference on Microelectronics, ICM, 2017, pp. 285–288.
13. M. Ebrahim, S. Khan, and U. B. Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," International Journal of Computer Applications, Vol.61, No.20, 2013.
14. G.Narmadhai, Dr.S.Vijay Bhanu,"Comparative Study of Hybrid Attribute Based Encryption for Cloud Computing System", International Journal of Computer Sciences and Engineering, Vol.- 6, Issue-10, Oct 2018.
15. G.Narmadhai, Dr.S.Vijay Bhanu,"A Survey on Hierarchical Attribute set based Encryption Access Control Method for Mobile Cloud Computing", International Journal for Science and Advance Research in Technology, Volume 4, Issue 1 in January 2018 E-ISSN: 2347-.2693