International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Power Consumption using Cryptography Algorithms in Cloud Computing

G.Narmadhai, S. Vijay Bhanu

Abstract*: Cloud Computing has been viewed as the cutting edge design of Information Technology. The Cloud worldview included points of interest and its potential for diminishing expenses and time for an administration that favors towards security issues. Distributed computing is an accumulation of data technology(IT) that offered to the client dependent on renting. In spite of 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 Power Consumption of utilizing our refreshed H-HABE calculations and contrast and the different encryption systems. A similar report made on a few encryption systems are utilized for power utilization in the cloud. At long last, the significant measurements like Power Consumption issues present in distributed computing are examined.

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

I. 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 on. The security is additionally an exceptionally huge issues for the substance in the capacity at cloud. Different encryption instruments 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 personality based encryption strategy. The property based encryption(ABE) is additionally an another strategy to encode the substance by utilizing traits as it were. This paper substance few of these strategies to verify distributed storage by utilizing property based confirmation and their measurements like power utilization. Numerous touchy information can be verified by utilizing this component and this idea is additionally distributed in a journal.

Manuscript published on 30 September 2019
* Correspondence Author
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.

II. PROBLEM STATEMENT

In past experiments, ABE,BH-WABE and H-HABE there are numerous issues, i.e., high power utilization during the time of encryption and unscrambling. These calculations have a portion of the issues like power utilization that are settled in proposed calculation. In proposed work a calculation is created.

III. SYSTEM PARAMETERS

The experiments are conducted in IntelR CoreTM i5-4440 CPU @ 3.10GHz processor, 8GB RAM, Windows 10, 64-bit Operating systems. The simulation environment was developed by default settings of Java 1.8. The size of input plaintext data varies from 1MB, 2MB,: : : ,10MB. The experiments will be repeated several times and one text file to ensure that results are reliable and effective to check with existing algorithms.

IV. COMPARISON

In this manner by security perspective all the ABE,BH-WABE and H-HABE existing frameworks isn't that much solid. Here it is contrasted our proposed calculation and other existing calculations based on certain parameters like power utilization. So as to legitimize that our proposed work is more effective than others, here it is presented new encryption system which diminishes control utilization for encryption and unscrambling. It additionally gives high throughput and low power utilization with expanded security. In this part here it contrasted our work and other existing procedures. It is spoken to our outcome with regards to various parameters like ascertaining Throughput and Power Consumption for different calculations.

A. Power Consumption

Larger key size/number of rounds, produce higher levels of security at the cost of additional power consumption. For example, Figure 1.2 shows a general trends in the trade-off between vulnerability and power consumption with different number of encryption rounds. Therefore, in order to design power-efficient encryption algorithms for cloud networks, there is an inherent need to understand the relationships between power consumption and encryption parameters. Once these relationships are well understood, then it is possible to optimize power consumption with respect to a security requirement or vice versa. Energy consumption for encryption and decryption can be measured in many ways. These methods are as follows:

The first method used to measure energy consumption is to assume that an average amount of energy is consumed by normal operations and to test the extra energy consumed by an encryption algorithms. This method simply monitors the level of the percentage of remaining battery that can be computed by equations (1) and (2),

$$\text{Change in battery life} = \frac{\text{The battery life consumed in percentage for one run}}{\text{the number of runs}} \quad (1)$$

$$\text{Average battery consumed per iteration} = \sum_{1}^{N}\left(\frac{\text{Battery Consumed per Iteration}}{N}\right)$$

The second method of security primitives can also be measured by counting the amount of computing cycles which are used in computations related cryptographic operations. For computation of the energy cost of encryption, it uses the same techniques as described and using the following equations.

$B_{cost\_encryption}$(ampere-cycle)= τ * I :

T_{energy_cost}(ampere-seconds) :

E_{cost}(Joule)=T_{energy_cost}(ampere-seconds) * V Where

$B_{cost\text{-}encryption}$: basic cost of encryption(ampere-cycle)

τ: the total number of clock cycles.

I : the average current drawn by each CPU clock cycle.

T_{energy_cost}: the total energy cost(ampere-seconds)

F : Clock frequency(cycles/sec) E_{cost}(joule) : the energy consumed cost

This section presents a basic cost of encryption represented by the product of the total number of clock cycles taken by the encryption and the average current drawn by each CPU clock cycle. The basic encryption cost is in unit of ampere-cycle. To calculate the total energy cost, it is divided by the ampere-cycles by the clock frequency in cycles/second of a processor; Here obtain the energy cost of encryption in ampere-seconds. Then, this is multiplied by the ampere-seconds with the processor‘s operating voltage, and the energy cost in, joule can be obtained.

By using the cycles, the operating voltage of the CPU, and the average current drawn for each cycle can be calculated by the energy consumption of cryptographic functions. For example, each cycle consumes approximately 270mA on an IntelR CoreTM i5-4440 CPU@3.10GHz processor, 8GB RAM, Windows 10, 64-bit Operating systems or 180 mA on Intel Strong ARM. For a sample calculation, with a 3.10GHz, CPU operates at 1.35 volt, an encryption with 20,000 cycles would consume about $5.71X10^{-3}$ mA second or 7.7μJoule. So, the amount of energy consumed by program P to achieve its goal (encryption or decryption) is given by $E= VCC \times I \times N \times \tau$ ––––––––––(1)

where N – Number of clock cycles

VCC – The supply voltage of the system

I – the average current in amperes drawn from the power source for T seconds.

Since for a given hardware, both VCC and τ are fixed, $E \alpha I \times N$. However, at the application level, it is more meaningful to talk about T than N, and therefore, here it is express energy as $E \alpha I \times T$. Since for a given hardware VCC are fixed. The second and third methods have been used in this work.

The second method used to measure energy consumption is to assume that an average amount of energy is consumed by normal operations and to test the extra energy consumed by an encryption algorithms like ABE,BH-WABE and our updated H-HABE. This method simply monitors the level of the percentage of remaining battery. The experiments note the number of iterations or runs over the file and the battery life. The change in battery life divided by the number of runs gives the battery life consumed in percentage, for one run.

B. Encryption Power consumption of Different Text files

Encryption time is used to calculate the power consumption of an encryption scheme. In this section, to encrypt the text files, calculate it consumes power by using two different methods (μJoule/Byte, and Average Battery Consumed Per Iteration) are calculated for encrypting text files (.doc or .docx files).

The first method used to measure energy consumption is to assume that an average amount of energy is consumed by normal operations and to test the extra energy consumed by ABE,BH-WABE and our updated H-HABE algorithms. This method simply monitors the level of percentage of the remaining battery. The experiments note the number of iteration or runs over the file and battery life. Change in battery life divided by the number of runs gives the battery life consumed in percentage for one run. Figure 1.1 shows the performance of ABE,BH-WABE and our updated H-HABE algorithms in terms of power consumption for encryption.

The CPU process time is the time that a CPU is committed only to the particular process of calculations. It reflects the load of the CPU. The more CPU time is used in the encryption process, the higher is the load of the CPU. The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while operating on encryption operations. Each cycle of CPU will consume a small amount of energy.

Battery power consumption is directly dependent on the CPU execution time; if execution time is high then battery consumption will be high and if execution time is low then battery consumption will be low. So here our updated H-HABE algorithms is producing low battery consumption due to its less execution time as compared to ABE,BH-WABE and H-HABE algorithms.

In Figure 1.1, here it is calculated power consumption (in msec) for one text file sized 899 kbytes. After analyzing this output 10 times for each input size of data, we calculated average time for each input size. Then it is calculated average of time for all input size data, which is our power consumption in (msec) for decryption.

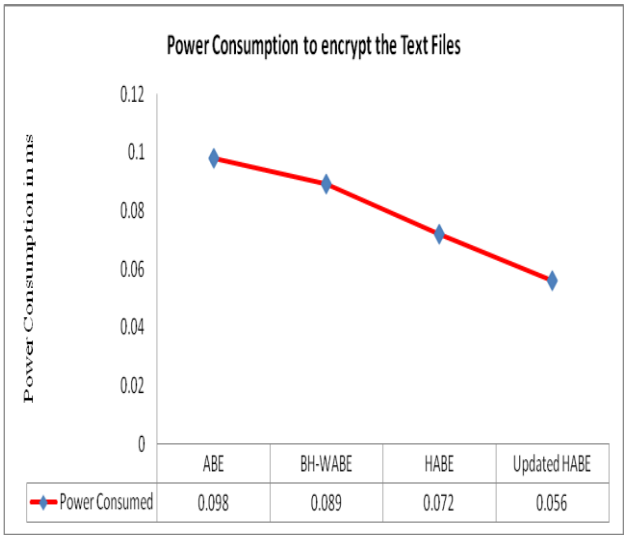

Figure 1.1: Calculate power consumption for Encryption

- The results show the superiority of updated H-HABE algorithm over the other algorithms in terms of the power consumption.
- The results show the superiority of our updated H-HABE algorithm over the other algorithms in terms of the power consumption.
- When it encrypts the same data by using our proposed updated H-HABE algorithm, it is found that Proposed requires approximately 14% of the power which is consumed for ABE.
- H–HABE require less power than all other algorithms except updated H-HABE(when it encrypts the same data by using ABE and BH-WABE, it is found that ABE requires approximately 52% of the power which is consumed for BH-WABE).
- H–HABE has an advantage over other ABE and BH-WABE in terms of power consumption.
- Finally, it is found that BH-WABE has low performance in term of Power Consumption and low throughput when compared with the other algorithms.

C. Decryption Power consumption of Different Text file Sizes

The higher the value of power consumption is less the efficiency of decrypting any text with an encryption algorithm. Figure 1.2 shows a graph for comparison on power consumption of ABE,BH-WABE and our updated H-HABE algorithms with different input file sizes. It is clear from the below figure that power consumption is higher for ABE,BH-WABE and H-HABE algorithms as compared to updated H-HABE algorithms algorithm.

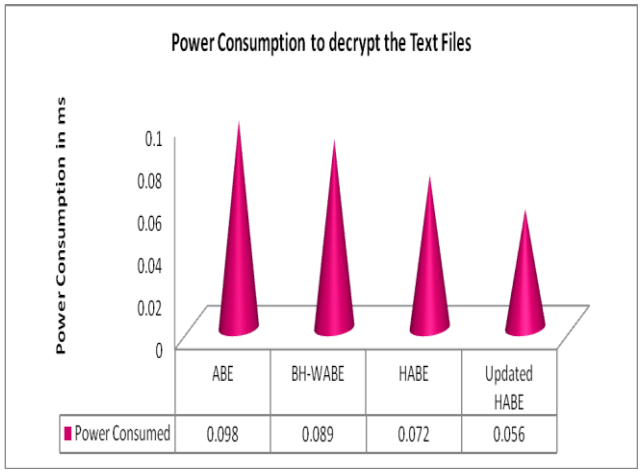

Figure 1.2: Calculate power consumption for decryption

- The results show the superiority of updated H-HABE algorithm over the other algorithms in terms of the power consumption.
- The results show the superiority of our updated H-HABE algorithm over the other algorithms in terms of the power consumption.
- When it decrypts the same data by using our proposed updated H-HABE algorithm, it is found that Proposed requires approximately 14% of the power which is consumed for ABE.
- H–HABE require less power than all other algorithms except updated H-HABE(when it encrypts the same data by using ABE and BH-WABE, it is found that ABE requires approximately 52% of the power which is consumed for BH-WABE).
- H–HABE has an advantage over other ABE and BH-WABE in terms of power consumption.
- Finally, it is found that BH-WABE has low performance in term of power consumption when compared with the other algorithms.

V. CONCLUSION & FUTURE WORK

A. Conclusion

There are more requirements to secure the data transmitted over different cloud using different services. To provide the security to the cloud and data different encryption methods are used. In this paper, a survey on the existing works on the encryption techniques using power consumption has been done. According to research done and literature survey it can be found that our proposed algorithm like updated H-HABE is most efficient in terms of Power Consumption with different file sizes.

B. Future Work

The present work deals with plain text being represented in numerical and characters of English alphabet. This work can be improved so that it can support the characters of not only English but also of other languages as well. This work can also be improved to support not only text but also other forms of message transmission like audio, video and images.

REFERENCE

1. 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.
2. 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.
3. Wu, Jiehong, Ilia Detchenkov, and Yang Cao. "A Study on the Power Consumption of Using Cryptography Algorithms in Mobile Devices." Software Engineering and Service Science (ICSESS), 2016 7th IEEE International Conference on. IEEE, 2016.
4. Y. Kumar R. Munjal and H. Sharma "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", International Journal of Computer Science and Management Studies, Vol. 11 No. 3 Oct 2011.
5. P. Mahajan and A. Sachdeva "A Study of Encryption Algorithms AES DES and RSA for Security" ,Global Journal of Computer Science and Technology Network Web & Security,Vol. 13 No. 15 2013.
6. S. Chandra, S. Bhattacharyya, S. Paira and S. S. Alam, "A Study and Analysis on Symmetric Cryptography," Science Engineering and Management Research (ICSEMR), 2014 International Conference on, Chennai, 2014, Pp. 1-8.
7. P. Liu H. Chang and C. Lee "A True Random-based Differential Power Analysis Countermeasure Circuit for an AES Engine", IEEE Transactions on Circuits and Systems-II: Express Briefs,Vol. 59 No. 2 pp. 103-107 2012.
8. H. Hayouni, M. Hamdi and T. H. Kim, "A Survey on Encryption Schemes in Wireless Sensor Networks," Advanced Software Engineering and Its Applications (ASEA), 2014 7th International Conference on, Haikou, 2014, pp. 39-43.
9. J. Raigoza and K. Jituri, "Evaluating Performance of Symmetric Encryption Algorithms," in Proceedings - 2016 International Conference on Computational Science and Computational Intelligence, CSCI 2016, 2017, pp. 1378–1379.
10. 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.
11. M. Ebrahim, S. Khan, and U. B. Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," International Journal of Computer Applications, Vol. 61, No. 20, pp. 975–8887, 2013.
12. 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.
13. 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 2018ct 2018 E-ISSN: 2347-.2693