Utilization Of Multicore System For Security Framework Gate

Diksha Aher[1], Kirti Nayakwadi[2], Vidya Bhakare[3],Priyanka Jadhav [4]

Department of Computer Engineering

[1,2,3,4] Siddhant college of engineering

Abstract- *In today's system, speed of CPU is not beneficial for fast processing. The approach that they use to execute task not utilizes the CPU better. We proposes a multicore hardware platform that will enhance the efficiency of system and will also provide more security. Hybrid AES-BRA algorithm is used. It could be used to measure performance impact from different p-states. Energy management can be performed at many levels of granularity and through various techniques. Comparing our approach to sequential shows gains in compute energy efficiency. In this way dynamic management scheme saves energy consumption.*

Keywords- Parallel processing, data security, BRA algorithm,high performance computing.

I. INTRODUCTION

As processors have increase in performance and speed, processor power & energy consumption have become key challenges in the design of future high- performance systems. the maximum utilization of cpu in present system is 32-40%.task is executed using sequential operation & that sequential execution cannot utilize cpu time efficiently. thus,increases time complexity of executing task.

In proposed system, we are changing the approach of task execution. To increase efficiency of system, we proposes software platform. We present a multicore architecture where all cores execute the same instruction set, but have different capabilities & also performance levels. At run time, system software evaluates the resource requirements of an application and further chooses the core that can best meet these requirements while minimizing energy consumption. The motivation behind this is to reduce power consumption, and release s reserved resources for other applications.

The dynamic power management approach balances utilized processor resources against current work- load at runtime. The power management observes the processor statistics ie utilization, and evaluates the amount of required resources, i.e. the number of active processors. We have implemented software platform and evaluated various operation on a range of platforms, from embedded processors typical for mobile phones up to high-end server platforms.Important reasons about the extremely high energy consumption in cloud data centers can attributed to the low utilization of computing resources that incurs a higher volume of energy consumption as compared with efficient utilization of resources. The resources with a low utilization consume an unacceptable amount of energy & time. According to recent studies, the average resource utilization in various data centers is lower than 30% and the energy consumption of idle resources is more than 70% .We are providing security mechanism to information in serial & parallel way for existing & proposed system. We will consider power and computational factor of processor. Three levels of security are provided Authentication level security, Data level security, Network level security. BRA & AES top 2 security algorithms by combining will give higher level security. This algorithm is providing more security, because it is harder to crack the message. Result shows that, if this project is run in serial way, then utilization of CPU is 30-40%.If same project is run by proposed approach, CPU utilization will be upto 100%.

II. LITERATURE SURVEY

Recent survey of green data centers and energy-efficient cloud computing systems found in [1], [2]. Overview of energy and time efficiency techniques in cluster computing systems was provided in [3]. In [4], the authors proposed a method to route a request to the data center that is nearest in terms of geographical distance, results in least electricity, and emits the smallest amount of carbon. In [5] the authors studied the problem of scheduling batch jobs for multiple geographically distributed data centers, and proposed a provably efficient online scheduling algorithm, which optimizes the energy cost and fairness among different organizations, subject to queueing delay constraints, which satisfy the maximum server inlet temperature constraints.s.

III. SYSTEM DESIGN

a. System Architecture

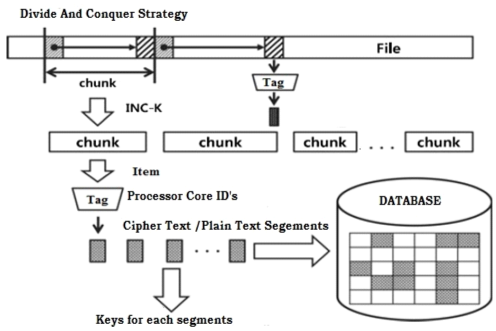


FIGURE1.System Architecture

A description of the program architecture is presented. Subsystem design or Block diagram, Package Diagram, Deployment diagram with description is to be presented. file, office file, PDF file, .txt file, etc. These files are divided into different chunks using divide conquer strategy.Divide and conquer strategy means given file is divided into chunks.Different operations are performed on that chunk and results of this chunk are combined to get final result.

Chunking:

Chunking in psychology is a process by which individual pieces of information are bounded together into a meaningful whole. A chunk is defined as a familiar collection of more elementary units that have been inter associated and stored in memory repeatedly and acting as coherence and integrated group when retrived. Chunks can be fix or in variable size.

Inc-k:

It is module which increments the chunk

Tags:

Tag is nothing but processors core id. Each chunk has assign some id. That id describe on which processor that chunk should execute.

Encoding:

If the given file is in plain text, encoding operation is performed on that file.Its associated ciphertext get generated. That ciphertext is stored into database.

Decoding:

If the given file is in cipher text, ,decoding operation is performed on that file. Its associated plain text get generated. That plain text is stored into database.

Database:

When user does registration, he fills up different information that information is stored into database.

b. Modular framework

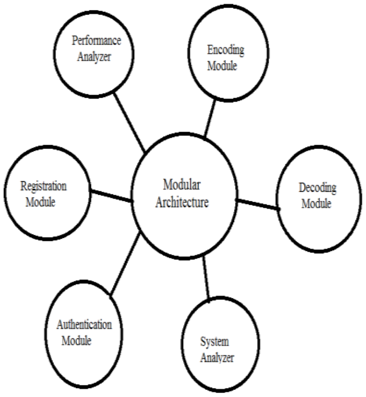


FIGURE2.Modular Architecture

Registration: User does registration.Fills all his information and unique information like mobile number is validated.

Authentication: Users login information is authenticated and it is stored into database.It depends on registration.

System Analyzer: Analyse the system.

Encoding Module: Encoding is done in two steps i.e Serial and Parallel encoding.

Hybrid BRA - AES Encoder: If user sends file it is encoded using this algorithm.

Decoding Module:

Decoding is done in two steps i.e Serial and Parallel decoding.

Hybrid BRA - AES Decoder: Intended user decodes this file using this algorithm.

Performance Analyzer: In this model we compare the time or the result.

c. High Performance computing

“Multicore System of HPC framework”technique increase the performance of data security algorithm which uses sequential processing they are modified using the theory of parallel processing. Still there is a chance of performance improvement of hybrid AES-BRA algorithm by using Parallel Processing. HPC systems popularly known as Supercomputers, generally capitalize on aggregating computing power in a way that delivers much higher performance than one could get out of a typical single desktop computer or workstation in order to solve large problems in engineering, or business. They are used for a wide range of computationally indepth tasks in various fields such as, comprise quantum mechanics, weather forecasting, climate research, oil and gas exploration, molecular modeling and or physical simulations. HPC systems have been shifting from expensive massively parallel architectures to clusters of commodity computers in order to take advantage of cost and performance benefits.

d. Single core vs Multicore

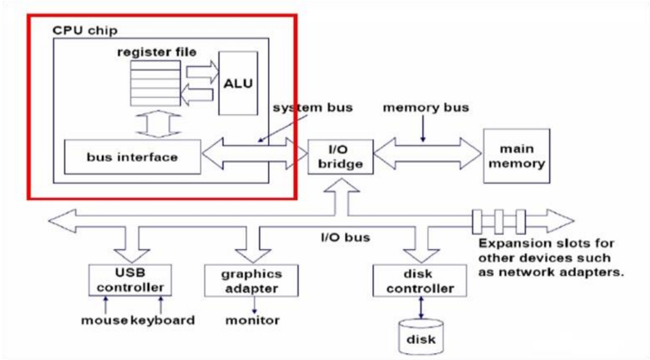


FIGURE3.Single core architecture

A single core processor is a microprocessor with a single core on a chip, running a single thread at certain time. The term became common after the emergence of multicore processors to distinguish non multi core designs. Most microprocessors prior to the multi core era are single core. The class of many core, in a processors follows on from multicore in a progression showing increasing parallelism over time.Processors remained single core unit it was impossible to achieve performance gains from the increased clock speed and transistor count allowed by Moore’s law.

Multi Core:

Multi core assign two or multiple processors. But they are different from independent parallel processors as they are integrated on the similar chip circuit .A multi core processor implement message passing or shared memory inter core communication methods in multiprocessing. If the number of threads are less than or equal to the number of cores, separate core is provided to each thread and threads run independently on these multiple cores. If the number of threads are more than the number of cores, the cores are distributed among the threads. Any application that can be threaded can be mapped effortlessly to multi-core, but the improvement in performance gained by the usage of multi core processors depends on the portion of the program that can be parallelized.

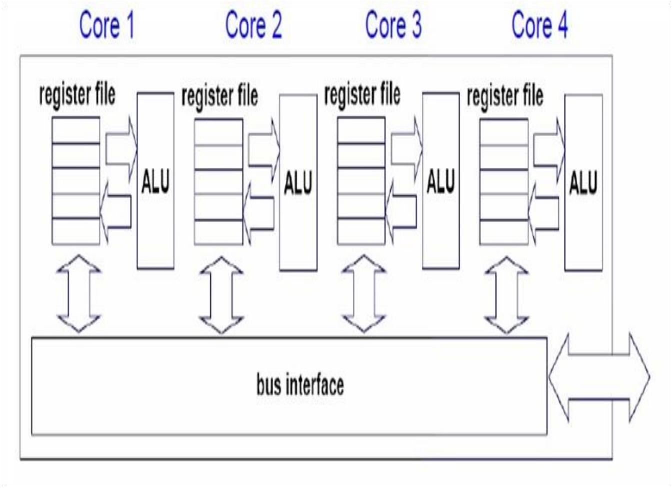


FIGURE4.Multicore Architecture

IV.SCHEDULING ALGORITHM

a) BRA Algorithm

- BRA provides high security to users during communication.
- In Architecture diagram shows the plain text divided into small blocks of data and BRA parallel encryption technique apply on small block of data.
- Parallel decryption technique decrypts the data and combine the divided block.

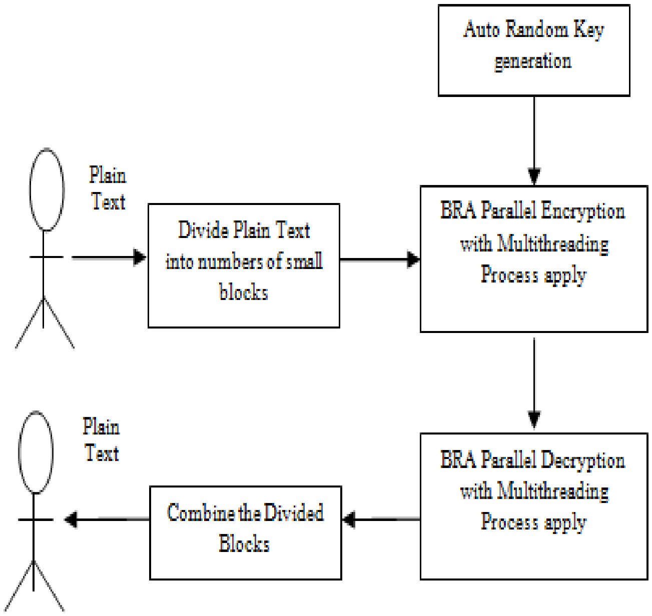

Auto Random Key generation
Plain Text
Divide Plain Text into numbers of small blocks
BRA Parallel Encryption with Multithreading Process apply
Plain Text
Combine the Divided Blocks
BRA Parallel Decryption with Multithreading Process apply

FIGURE5. Arichtecture of BRA algorithm.

b) AES Algorithm

- The AES algorithm has implemented by modifying old AES 128 algorithm. This modified algorithm used different methods like byte substitution using S-box, shifting row and mix column.
- The key size of AES algorithm is 512 bits and input also 512 bits. Security, throughput, efficient utilization of processer, memory are the advantages of this algorithm.
- The AES algorithm has implemented by using inter-round and intra round pipeline design. Different key size of this algorithm is like 128,192, and 256 bits. The bock size of AES algorithm is 128 bits.
- AES algorithms includes two modes. One is cipher feedback mode and second is an output feedback mode. This algorithm is reduce the use of hardware in encryption and decryption process

c) Partition Algorithm

The name "divide and conquer" is sometimes applied also to algorithms that reduce each problem to only one sub-problem.These algorithms can be implemented more efficiently than general divide-and-conquer algorithms; in particular, they can be converted into simple loops.Under this broad definition, however, every algorithm that uses recursion or loops could be regarded as a "divide and conquer algorithm". Therefore, some authors consider that the name "divide and conquer" should be used only when each problem may generate two or more subproblems. The name decrease and conquer has been proposed instead for the single-subproblem class.

An important application of divide and conquer is in optimization, where if the search space is reduced ("pruned") by a constant factor at each step, the overall algorithm has the same asymptotic complexity as the pruning step, with the constant depending on the pruning factor .

V.RESULT

a.System Enviroment

For our project evaluation, we consider system consisting of Dual core processor and above having speed 1.1GHz. Hard disk used is 20GB. RAM of our system is 1GB.We used standard windows keyboard with monitor SVG/TFT. Database used is MYSQL with java version J2SDK1.5 and above

b.Performance Analysis

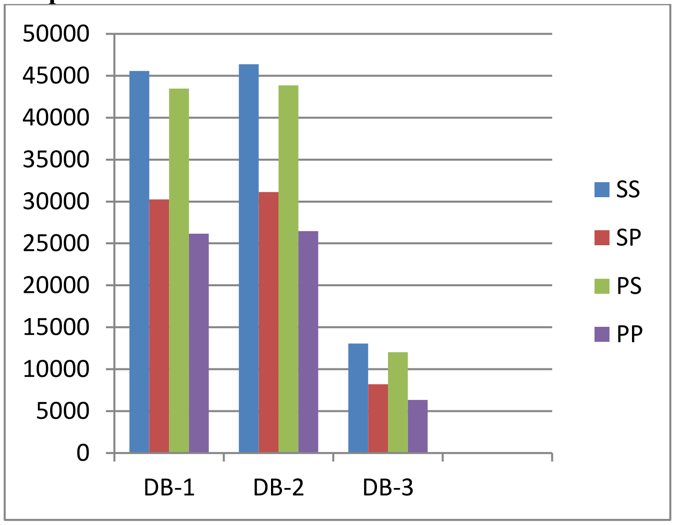
1.Experimental Result:

H/W and S/W	Description
Processor	Intel® Core™ i3 CPU
Speed	2.20 GHZ
RAM	8 GB
Cores	4
O.S.	Windows 7 (64-bit)

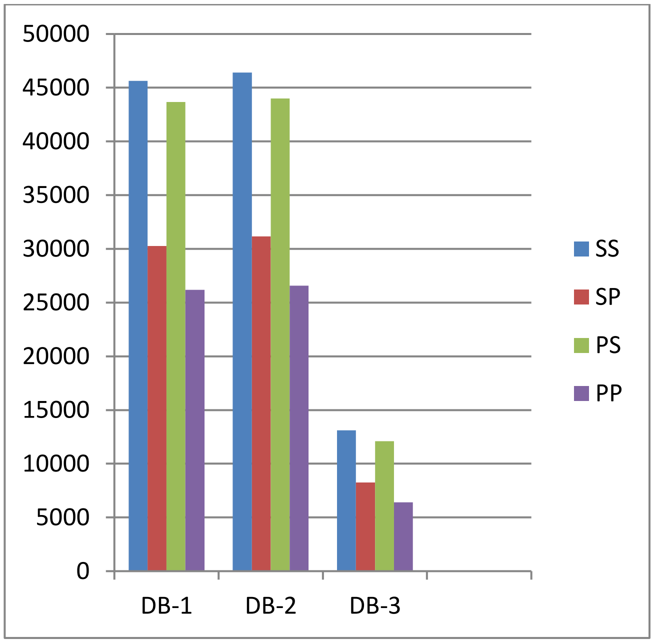
2.Experimental Result:

H/W and S/W	Description
Processor	Intel® Core™ i5 CPU
Speed	2.40 GHZ
RAM	4 GB
Cores	4
O.S.	Windows 7 (64-bit)

Graph:



Encode Mechanism



Decode Mechanism

VI. CONCLUSION

Energy consumption can be reduced for multicore processors using hardware platform of parallel operation. Using hybrid BRA-AES algorithm are taking 13% less time for text, image, pdf, application, etc for their encryption and decryption as compare to AES algorithm. Performance analysis of hybrid BRA-AES Algorithm for file encryption and decryption process is done

ACKNOWLEDGEMENT

We sincerely thank the reviewers for their comments and suggestions that helped us improve our work. This research has been supported by our Faculty members especially our project guide Prof. Kamal Reddy and the International Journal For Science And Advance Research In Technology.

REFERENCES

[1] Beloglazov, R. Buyya, Y. C. Lee, and A. Zomaya, "A taxonomy and survey of energy-efficient data centers and cloud computing systems,"Advances in computer,vol.82

[2] L. Wang and S. U. Khan, "Review of performance metrics for green data centers: a taxonomy study," Journal of Supercomputing, vol. 63, no. 3, pp. 639-656, 2013.

[3] G. L. Valentini, W. Lassonde, S. U. Khan, N. Min-Allah, S. A.Madani, J. Li, L. Zhang, L. Wang, N. Ghani, J. Kolodziej, H.Li, A. Y. Zomaya, C.-Z. Xu, P. Balaji, A. Vishnu, F. Pinel, J. E.Pecero, D. Kliazovich, and P. Bouvry, "An overview of energy efficiency techniques in cluster computing systems," Cluster Computing, vol. 16, no. 1, pp. 3-15, 2013.

[4] J. Doyle, R. Shorten, and D. O'Mahony, "Stratus: load balancing the cloud for carbon emissions control", IEEE Transactions on Cloud Computing, vol. 1, no. 1, pp. 116-128, 2013.

[5] M. Polverini, A. Cianfrani, S. Ren, and A. V. Vasilakos,"Thermal-aware scheduling of batch jobs in geographically distributed data centers," IEEE Transactions on Cloud Computing,vol. 2, no. 1, pp. 71-84, 2014.

[6] P. Kukkala, T. Arpinen, M. Set¨al¨a, M. H¨annik¨ainen, and T. D.H¨am¨al¨ainen, "Dynamic power management for UML modeled applications on multiprocessor SoC," Proceedings of the IS&T/SPIE 19th Annual Symposium on Electronic Imaging, 2007.

[7] R. Kumar, K. Farkas, N. P. Jouppi, P. Ranganathan, and D.M. Tullsen, "Processor power reduction via single-ISA heterogeneous multi-core architectures," IEEE Computer Architecture Letters, vol. 1, no. 1, pp. 5-8, 2002.

[8] S. J. Lee, H.-K. Lee, and P.-C. Yew, "Runtime performance projection model for dynamic power management," Proceedings of 12th Asia-Pacific Computer Systems Architecture Conference,LNCS 4697, pp. 186-197, 2007.

[9] D. C. Snowdon, E. Le Sueur, S. M. Petters, and G. Heiser,"Koala a platform for OS-level power management," Proceedings of the 4th ACM European Conference on Computer Systems,pp. 289-302, 2009.