RESEARCH ARTICLE OPEN ACCESS

Evaluating and Improving the Performance of Cryptosystem with Low Latency Framework on Multi-Core System

Kunal Bhangale, Chaitanya Deshmukh, Shubham Jadhav, Tejas Kshirsagar
Department Of Computer Engineering, DYPIEMR, Akurdi.

Abstract:

The technique of using workload dependent dynamic power management (i.e., variable power and speed of processor cores according to the current workload) to improve system performance and to reduce energy consumption is investigated. Typically, the power supply and the core speed are increased when there are more tasks in a server, such that tasks can be processed faster and the average task response time is reduced. On the other hand, the power supply and the core speed are decreased when there are less tasks in a server, such that energy consumption can be reduced without significant performance degradation. Several speed schemes are proposed and it is demonstrated that for the same average power consumption, it is possible to design a multicore server processor with workload dependent dynamic power management, such that its average task response time is shorter than a multi-core server processor of constant speed. Information security is a challenging issue in today's technological world. There is a demand for a stronger encryption which is very hard to crack. Earlier many researchers have proposed various encryption algorithms such as AES, DES, Triple DES, RSA, Blowfish etc. Some of them are most popular in achieving data security at a great extent like AES and Blowfish. But, as security level is increased, the time and complexity of algorithm is also increased. This is the major cause of decreasing the speed and efficiency of the encryption system. In this paper we have proposed a new encryption algorithm "Byte – Rotation Encryption Algorithm (BREA)" with "Parallel Encryption Model" which enhances the security as well as speed of the encryption scheme

Keywords — **Computer System Organization, Computer Communication Networks, Distributed System, Distributed applications, Distributed databases, Network operating systems, Distributed file systems**

I. INTRODUCTION

For proposing an online resource management frame-work that maximizes profit ratio while minimizing energy expenses by exploiting the distributed task elasticity and price heterogeneity. This is done by reducing the duration during which servers need to be left ON and maximizing the monetary revenues when the charging cost for some of the inelastic tasks depends on how fast these tasks complete, while meeting all resource requirements. The power supply and the core speed are increased when there are more tasks in server, such that tasks can be processed faster and the average task response time is reduced. It is possible to design a multicore server processor with workload dependent dynamic power management, such that its average task response time is shorter than a multicore server processor of constant speed (i.e., without workload dependent dynamic power management). Byte Rotational Algorithm(BRA) provides more security and takes smallest amount of time for transfer file . This algorithm can apply on different types of files like text, image, audio, video files.

Comparative studies conducted using UCI repository data traces show the effectiveness of our proposed framework in terms of improving resource utilization, reducing energy expenses, and increasing profits ratio by calculating memory and bandwidth with increasing speed. The process elasticity is exploited on heterogeneous environment in a distributed system. Elasticity is the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current

demand as closely as possible. Various approaches are considered like serial, parallel and hybrid approaches. Accordingly, profit ratio is calculated. Process mining is taken as a task to calculate the profit ratio. Resources that are considered are CPU, Bandwidth, Time and Temperature and Memory. Tools used to calculate the profit ratio of CPU, Bandwidth, Time and Temperature and Memory is CPU-Z and HW-Monitor. The tasks involved are independent on each other. Profit ratio is calculated of factors i.se CPU, Bandwidth, Memory, Time and Temperature of systems with different processors.

II. SCOPE OF PROJECT

Project Idea: As there is a large amount of data present for data sharing fields like marketing, sales, Banks customer support, e-commerce such database having a size in GB and TB need fast processor. Serial approach can consume time and reduce performance. To solve this issue's the proposed model of parallel system to reduce time, increase performances and fast processing. For fast processing multicore processor are used. For finding useful knowledge an algorithm is required . Byte rotational algorithm is fast Cryptosystem approach Which complex to hackers In the Byte Rotation Algorithm involve twotechniques. One is key generation technique is used. And second is data processing. We plan to implement cryptosystem in single threaded approach as well as multi-threading technique.

Problem Statement: It exploits the process elasticity on heterogeneous environment proposed by the resource management framework that maximizes profit while calculating Memory, Time, Temperature and Bandwidth by taking process mining as task.

Goals :

- Reducing time of the given work.
- Reduction of the energy consumption .
- Tasks independency with multiple resources .

Objectives:

- Calculating memory and bandwidth.
- Increasing the speed of the processor.
- Maximizing the profit ratio with multiple resources.

Statement of scope :

Input File: Input can be an image, audio, video, text, pdf, application file etc.
User: At time one server and 2-3 clients can work together.
Time factor: The time for various approaches are to be calculated.
Memory: Memory calculation for various data on different approaches.
Tools: Different tools for calculating memory and bandwidth.

III. BYTE ROTATION ALGORITH

Features :

1. Block Size - 128 bit (16 byte).
2. Key Size - 128 bit (16 byte)..
3. Support all file type.

Steps :

1. Take ASCII value of 16 byte of file in block matrix of dimension 4 by 4 denoted by M. M={v1,v2,v3,....,v16}.
2. Take transpose of block matrix and represent is by Mt.
3. Create key matrix of 4 by 4 matrix with value of each cell is generated randomly in range of 0 to 255. Matrix denoted by K.
   K = {k1,k2,k3,...,k16}.kn = Random(0,255). Where n is element number.
   Random(integer,integer) is function to generate random number.
4. Add key matrix to transpose.
   Condition for addition -
   i. if sum exceeds 255 then subtract sum by 256.
   ii. if sum is negative then add 255 to sum.

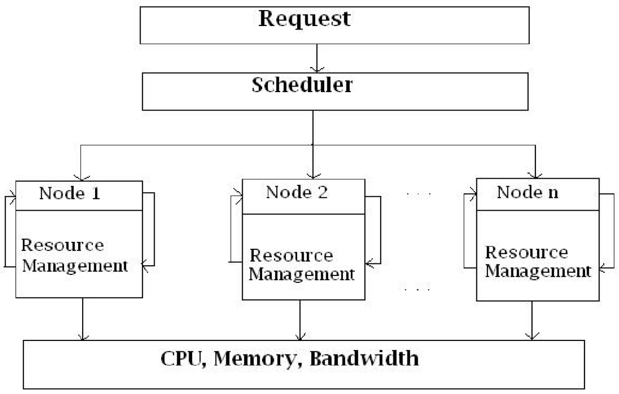
```
  vn = vn + kn
 if vn<0  then vn = vn + 256
 if vn>255  then vn = vn -256
 n = 1,2,3,.....,16.
```

5. Rotate Matrix Me Horizontally such that first row by one byte to left, second row two byte to left and third row three byte to left.
6. Simillary rotate Me Vertically such that first column by one in upward(left) direction , second column two byte in upward direction , and third column by three byte in upward direction.

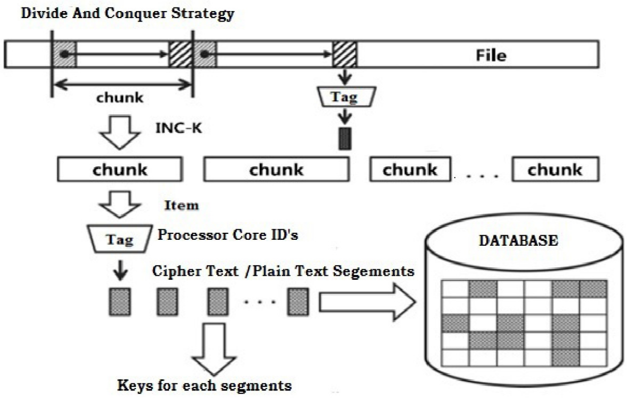
Note :

- One byte left rotation is equivalent to three byte right rotation, two byte left rotation is equivalent to two byte right rotation, three byte left rotation is equivalent to one byte right rotation
- To decrypt data use above step in reverse order.

IV. ARCHITECTURAL MODEL



Fig[1] Task Scheduler Modular Approach



Fig[2] Architecture diagram

LIMITATIONS OF PROJECT

- Multi-core System Required For Execution.
- Achieve Cryptosystem Profit Gains Only.
- Internal Based Parallelism Execution Only.

V. CONCLUSION

A profit driven online resource allocation framework for elastic task requests is proposed. The framework exploits the elasticity and the varying charging costs among the submitted requests and decides where to place the heterogeneous submitted task requests, and how much resources should be allocated to the elastic ones such that the cloud profits are maximized while meeting all tasks demand. The various algorithms like chunking algorithm, byte rotational algorithm and TTTD algorithms are discussed. TTTD algorithm, not only successfully achieves the significant improvements in running time and average chunk-size, but also obtains the better controls on the variations of chunk-size by reducing the large-sized chunks. Byte rotational algorithm is fast encryption algorithm. Byte Rotational Algorithm is complex to hackers but it's a strong algorithm in case of security.

REFERENCES

[1] O. J. Bedrij, “Carry-select adder,” *IRE Trans. Electron. Comput,* pp. 340–344, 1962.

[2] B. Ramkumar, H.M. Kittur, and P. M. Kannan, “ASIC implementation of modified faster carry save adder,” *Eur. J. Sci. Res.*, vol. 42, no. 1, pp.53–58, 2010.

[3] T. Y. Ceiang and M. J. Hsiao, “Carry-select adder using single ripple carry adder,” *Electron. Lett.*, vol. 34, no. 22, pp. 2101–2103, Oct. 1998.

[4] J. M. Rabaey, *Digtal Integrated Circuits— A Design Perspective* Upper Saddle River, NJ: Prentice-Hall, 2001

[5] J. M. Rabaey, *Digtal Integrated Circuits— A Design Perspective* Upper Saddle River, NJ: Prentice-Hall, 2001.

[6] Y. He, C. H. Chang, and J. Gu, “An area efficient 64-bit square root carry-select adder for lowpower applications,” in *Proc. IEEE Int. Symp. Circuits Syst.*, 2005, vol. 4, pp. 4082–4085.

[7] Cadence, “Encounter user guide,” Version 6.2.4, March 2008