Parallel Computation of Advance Encryption Standard Algorithm for Performance Improvement

Vishal H. Sathawane
M.Tech Computer Science and Engineering
Shri Ramdeobaba College of Engineering & Management
Nagpur,Maharashtra,India
Email: sathawanevh@rknec.edu

Tausif Diwan
Assistant Professor, Computer Science and Engineering
Shri Ramdeobaba College of Engineering& Management
Nagpur, Maharashtra, India
Email: tausifdiwan.tausif@gmail.com

Abstract – Information security on computer network become more essential now a day’s information confidentiality authenticity and integrity is taken care by cryptography. Cryptography has many existing algorithm for providing data security. There are so many different challenges need to be faced to implement cryptography algorithm such as execution time, memory requirement and computational power, parallel computation is promising technique to improve the speed up (performance) of Advance Encryption Standard Algorithm. This is considering as more secure algorithm in cryptography. In the parallel computation mainly two strategies are used Data Parallelism and Control Parallelism. For data parallelism mainly divide and conquer strategy is used in parallel computation. This paper presents optimized AES algorithm in parallel fashion using OpenMP. In the real time applications are required faster data processing operation like encryption and decryption. Our strategy is to use optimized approach of the algorithm which gives faster results. Parallel computation gives poor performance when the processing is very less because of parallel programming overhead where as in case of large processing overhead become negligible. Our proposed system switches algorithm as per input data size for the better performance. Proposed optimized AES algorithm is suitable to be implemented in a mulit-core environment. The proposed design exhibits improved performance over present different approaches.

Keywords*--Encryption; Decryption;AES; OpenMP; Parallel programming.*

*****

I. INTRODUCTION

Now a day’s computer network wildly used for the information and data Transmission. Highly confidential data and information need level of security at the time of transmission from one end to another end. While security comes under picture cryptography taking care of it with the help of different cryptographic algorithms. In today’s computer network lot of data is generated every day by sender and receiver. This data is generated by various domains like bank service, e-commerce website transaction, financial and legal files. These are the example of popular application responsible for data generation which requires special treatment from security point of view in terms of storage and transportation.

Cryptography provides security in transmission between sender and receiver. The aim of cryptography is to convert data into unreadable form so other cannot able to read or understand the data only authorised sender and receiver can read it. AES (Advance Encryption Algorithm) is the cryptographic algorithm provide security in sensitive data transmission.

AES is symmetric block cipher algorithm provide high level security to data by the Decryption and Encryption process. AES algorithm is algorithm which accepted as an encryption standard by US. The Rijindael algorithm (AES) was developed by Vincent Rijmen of KatholiekeUniversity at leuven and Joan Daemen of Proton.

In The real time application data generation speed is more where the data processing speeds in as comparatively low. Hence application took large time to process data from one form to another form. In the network data is shared in encryption format where receiver receives data and decrypts it. So we required fasted encryption and decryption algorithm. As we know AES is more secure cryptographic algorithm but it process only 128 bit of data at a time hence we need to process several 128 bit of data blocks parallel way for the speed up.

There are different approaches used for speedup like hardware approach pipeline method and software approach of parallelization. Data parallelization, task parallelization techniques are used for achieving parallelization between codes. In this paper we use software approach based on transformation of serial C code of AES in parallel code using OpenMP API tool. We measure speed up factor of serial and parallel code.

II. DESCRIPTION OF AES ALGORITHM

Rijndale algorithm i.e. AEs algorithm is a symmetric key algorithm which is developed in 1998. Two Belgian cryptographers, JhonDaemen and Vincent Rijmen was published AEs algorithm which is later on by NIST as the Advanced Encryption Standard.

The AES algorithm processed 128 bit of data at a time hence it require lot much time to process several data blocks. AES use three different key size as per security required like 128 bit, 192 bit and 256 bit key.where 10,12 and 14 encryption rounds will be applied for each key size respectively. While process 16 byte of data is changed to (4*4) array called as state array.

Steps:

1. Substitute Byte: non-linear bye substitution transformation taken place here, where substitution table (S-Box) which operates independently on each bytes.
2. Shift Row : A simple permutation process where state array shifting the last three rows of the state with different offset; Like row 1 is shifting circuler left or right for encryption and decryption process respectively by one place, row 2 by two place, similarly for 3 shifting by 3 place where as Row 0 remain unchanged.
3. MixColumns Step: A substitution that make use of arithmetic over GF(28).
4. Add round Key: need to just perform XOR operation of current block with the part of extended key.

AES algorithm is non-feistel cipher which differ in encryption and decryption process.

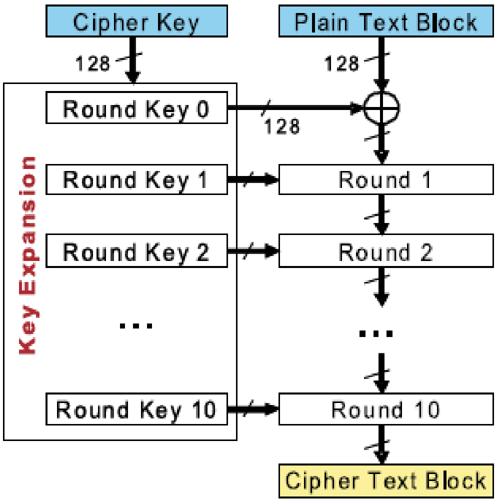

Figure 1: AES Algorithm structure

III. DESCRIPTION OF OpenMP API

OpenMp is the tool which support Multi-Processing. Open Multi-processing Application programming interface (OpenMP API) is defined by the group of computer software and hardware vendor. OpenMP API is scalable and portable model help for any input data size. OpenMP supports different programming languages like FORTRAN, C, C++ on several architecture like windows and Unix .OpenMP uses fork-join model for the execution of the program .OpenMp star execution of the program with single thread as parallel construct appear OpenMP divide task into different number of threads. The statement which lies between parallel region construct are execute in parallel among various threads. After parallel region light weighted parallel threads are terminated and master thread is continue its execution

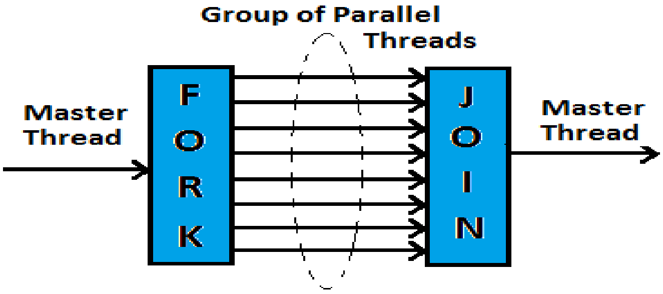

Figure 2: Fork-join Model

IV. REVIEW OF LITERATURE

Different Strategies are used for the optimizing the performance of AES algorithm. Optimizing the performance with the help of hardware and software following are reference paper we refer for the optimizing the performance.

- Paper by Gunjan Ansari,Vishal Panchori,,Neha Chaudhary in this paper author use the JPPF i.e. JAVA Parallel Programming Framework. Title of this paper is “Improved Performance of Advance encryption Standard using Parallel Computing”. JPPF provide flexibility and performance improvement in term of speed-up. Two main approaches are used like data parallelism and control parallelism. In data parallelism several data blocks are processed at a time. .
- Paper by Francisco Rodriguez-Henriquez ,Nazar A. Saqib, and Arturo Diaz-Perez in this paper an efficient implementation of AES on FPGAs. In this paper the present both approach of sequential and pipeline architecture and compare the result.title of this paper is “AES Algorithm Implementation- An efficient approach for sequential and Pipeline Architecture”. In sequential architecture design occupies 2744 CLB slices and achieved a throughput of 258.5 Mbits/s and there is no use of extra memory resources. In pipelined design occupies a total of 2136 CLB slices and achieved a

throughput of 2868 Mbits/s. The performance achieved by this pipelined system is not only efficient in terms of throughput but also area efficient.

- Paper by S.S. Navalgund, Akshay Desai, Krishna Ankalgi and Harish Yamanur this paper explain the parallelization tool that were utilized. Title of this paper is “Parallelization of AES algorithm Using OpenMP”. Some applications are required faster data processing means data encryption and decryption process required to be done faster to match data generation data Rate. In this paper they proposed parallel algorithm which process several data at a time.
- Paper by M. Vanitha, J. SairaBanu, Dr. J. Vaideeswaran, Dr. S. Subha In this paper they focused on the increase the throughput of AES algorithm using software and hardware technique. Various optimization techniques are used in this paper like pipelining, loop unrolling and iterative technique. They use pipelining technique between various rounds in the AES algorithm where out of 4 functions 2 functions are processed by one core while other core process next two functions. Title of this Paper is “Loop Parallelization and Pipelining Implementation of AES Algorithm Using OpenMP and FPGA”

V. PROPOSED WORK

In this project we implement parallel algorithm for AES algorithm. Using OpenMP we process several data blocks in parallel to achieve data parallelization.OpenMP provide flexibility and performance improvement in term of speed up. Here we present parallel encryption and decryption algorithm by making use of OpenMP Directives to reduce execution time. Parallel algorithm fail to give better performance when task is small hence it is efficient way to use the parallel approach when task is big to process. Hence in our switch between the algorithms as per input file size. If file size is small we processed it in serial where as we use parallel approach when input data is big. For that we need to find threshold value. Threshold value is calculated by checking algorithm on different input file size.

VI. RESULT AND OBSERVATIONS

Following are the result of serial and parallel algorithm on different file size

Sr. No .	File Size (No. of Blocks)	Serial (Time)	Parallel(4-core)	Speed Up
1	100000	11.655	9.862	1.187
2	10000	1.145	0.936	1.222
3	1000	0.130	0.122	1.062
4	900	0.104	0.096	1.085
5	800	0.092	0.089	1.038
6	700	0.086	0.075	1.143
7	600	0.070	0.072	0.975
8	500	0.057	0.074	0.771
9	400	0.048	0.059	0.811

Figure 3: Observation Table

Computing Threshold Value by plotting graph of time verses file size on x axis we plot file size whereas y axis represent y axis

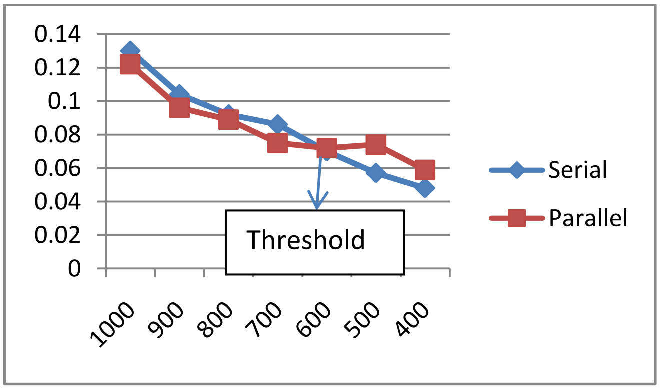

Figure 2: Graph time vs File size

From the above graph we can easily conclude the on 600 blocks of file size has threshold value which decides the mode of execution or the algorithm of execution.

VII. CONCLUSION

In this paper we present best possible method to increase the AES algorithm. Here we find best path to process AES algorithm according to the input data size.

REFERENCES

[1] Multi -core implementation of the symmetric cryptography algorithms in the measurement system, Piotr Bilski , Wiesław Winiecki, 2010 Measurement 43 (2010) 1049–1060, Elsevier. 10. 1016/j. measurement. 2010. 03. 002.

[2] Vishal Pachori, Gunjan Ansari, Neha Chaudhary,Improved Performance of Advance Encryption Standard using Parallel Computing / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www. ijera. com Vol. 2, Issue 1,Jan-Feb 2012, pp. 967-971.

[3] M. Nagendra and M. Chandra Sekhar,Performance Improvement of Advanced Encryption Algorithm using Parallel Computation , International Journal of Software Engineering and Its Applications Vol. 8, No. 2 (2014), pp. 287-296.

[4] Ghada F. Elkabbany, HebaK. Aslan and Mohamed N. Rasslan ,“A Design of A Fast Parallel-Pipelined Implementation of AES: Advanced Encryption Standard” International Journal of Computer Science & Information Technology (IJCSIT) Vol 6, No 6, December 2014.

[5] S. S. Navalgund, Akshay Desai, Krishna Ankalgi, and Harish Yamanur. “Parallelization of AES Algorithm Using OpenMP” ,Lecture Notes on Information Theory Vol. 1, No. 4, December 2013.

[6] J. Saira Banu, M. Vanitha, Dr. J. Vaideeswaran, Dr. S. Subha, “Loop Parallelization And Pipelining Implementation Of AES Algorithm Using OpenMP” , IEEE 2013 International conference on Emerging Trends in computing , communication and Nanotechnology (ICECCN2013).