IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

An Optimized Parallel Computation of Advanced Encryption Algorithm using Open MP -A Review

Vishal Sathawane[1], Tausif Diwan[2]

M.Tech Computer science and Engineering, RCOEM Nagpur, Maharashtra, India[1]

Assistant Professor, Computer Science and Engineering, RCOEM Nagpur, India[2]

Abstract: To protect electronic data, an approved cryptographic algorithm AES (Advanced Encryption Standard) is used. AES is a block oriented complex algorithm which have large amount of mathematical computations. For the large real time data requires a considerable amount of execution time for encryption and decryption, which may or may not be feasible for real time applications. This paper presents optimized AES algorithm in parallel fashion using OpenMP. Real time application requires faster encryption and decryption of data flows. Our approach used optimized strategy to process input data and gives faster results. Parallel computation gives better result if input data is large because parallel programming directive overhead is negligible in that case but it affects when data size is small. Our proposed system switches algorithm as per input data size for improved 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: AES, OpenMP, Encryption, Decryption, Parallel programming.

I. INTRODUCTION

Computer Networks are becoming more important for data and information transmission now days. We need secure transmission line for the security requirement for transmission from one end to another. large amount of data is generated every day billions of user send and receive data via computer networks. Various fields are involved in large volume of data generation such as bank service, e-commerce website transaction, financial and legal files. These are the example of application which requires special treatment from security point of view in term of storage and transportation.

Cryptography is one of the way to provide security in transmission between sender and receiver. The main aim of cryptography is to make data unreadable form so other cannot able to read other than authorised sender and receiver. AES (Advance Encryption Algorithm) is one of cryptographic algorithm provide secure data transmission which hide sensitive data.

AES is also known as ‘Rijndal’which is block cipher accepted as an encryption standard by US. The Rijindael algorithm was developed by Vincent Rijmen of Katholieke university at leuven and Joan Daemen of Proton World International submitted to the AES selection process under the name ‘Rijndael’.it is a symmetric block cipher algorithm provide high level security to electronic data by encrypt and decrypt process.

In addition to security the speed of algorithm plays an important role in real time application where we need faster encryption and decryption process. 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

The National Institute of Standard and Technology (NIST) was announced The Advanced encryption standard (AES) in November 2001. AES is alternative for DES which is cannot consider as safe because of short key where DES use on 56 bit key. There are different key sizes used in AES with fixed block size of 128 bit key. It allows 128 ,192 and 256 bit key as per the security required. This allows different number of round functions 10, 12 and 14 rounds respectively.

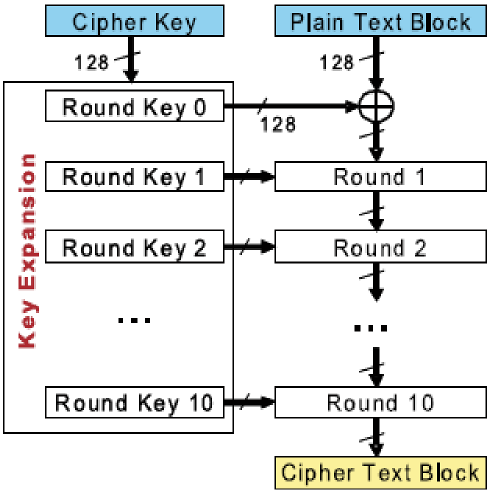

Figure 1: AES Algorithm structure

During encryption and decryption process 16 bytes of data (128 bit) given as input to the block in form of array (4*4) called as state array. In the encryption process the state

DOI 10.17148/IJARCCE.2016.5283

array consist the input data and array will change as per rounds until reaching the final enciphered data. In the decryption process state array consist enciphered text as input and keep changing until retrieving original data.

AES is non-feistel cipher where encryption and decryption process is slightly differing from each other.

III. DESCRIPTION OF OPENMP API

OpenMP API (Open Multi-processing application programming interface) is a tool which support Multi-processing. It is defined by a group of computer software and hardware vendors. OpenMP is scalable and portable model for developers of shared memory parallel application. OpenMP supports different programming languages like C,C++ and FORTRAN on several architectures like Unix and windows platform. All the OpenMP program start execution with single thread called it as Master thread. Master thread execute the region till parallel construct is encountered. After parallel construct is encountered master thread get divided into number of light weight parallel threads. OpenMP uses fork-join model for the execution of program. Figure shows the architecture of Fork and join model. The statements which lies between parallel region construct are execute in parallel among various threads. After execution of parallel region group of light weighted parallel threads are terminated and master thread continues its execution.

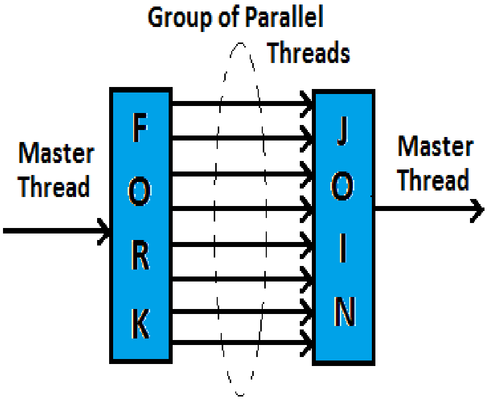

Figure 2: Fork-join Model

IV. REVIEW OF LITERATURE

There are many different strategies are used for optimize the performance of AES algorithm. Optimization taken place at hardware level or software level. Ultimate aim is to improve efficiency of data processing.

- **Paper by Vishal Panchori,Gunjan Ansari,Neha Chaudhary titled "Improved Performance of Advance encryption Standard using Parallel Computing ".**

In this paper they present parallel implementation of AES algorithm using JPPF i.e. JAVA Parallel Programming Framework. most of the research is on improving performance of AES on hardware implementation . JPPF provides flexibility and performance improvement in terms of speed-up. In this paper there are two approaches are used i.e. data parallelism and control parallelism. In data parallelism, 128 bit data blocks are taken. Different data blocks are taken and each part will be send independently processing unit.

- **Paper by Ghada F. Elkabbany, Heba K.Aslan and Mohamad N. Rasslen from Informatics Department ,Electronics Research Institute,Cairo,Egypt titled "A Design of a fast parallel-pipelined implementation of AES: Advanced Encryption Standard ".**

In this paper design of parallel AES on the multiprocessor platform is presented. Most of the previous designs either use pipelined parallelization or take advantage of the Mix_Column parallelization, this design based on combining pipelining of rounds and parallelization of Mix_Column and Add_Round_Key transformations. Basically this model is divided into two levels the first level is to pipelining different rounds and second method is through parallelization of both the Add_Round_Key and the Mix_Column transformations. In the previous models pipelining is achieved in nine stages of AES algorithm whereas this method introduce eleven level of pipelining which includes both initial and final round of AES. This system enhance the system performance compared to previous designs. Using two level of parallelization which is useful for independency of Add_Round_Key and Mix_Column / Inv_Mix_Column transformations.

- **Paper by Nazar A. Saqib, Francisco Rodríguez-Henríquez and Arturo Díaz-Pérez titled "AES Algorithm Implementation- An efficient approach for sequential and Pipeline Architectures".**

In this paper they present an efficient implementation of Rijndal cryptographic algorithm on FPGAs, they implement AES algorithm both in sequential and pipeline architecture and compare the results as area time trade-off. 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 titled "Parallelization of AEs Algorithm Using OpenMP".**

This paper gives a brief description of the Parallelization tools that were utilized. Followed by brief explanation of the parallelization process of the AEs algorithm. Lastly experimental result is given regarding efficiency of parallel algorithm which is presented.

Some applications are required faster data encryption and decryption process to match faster data rate. For that we need to process multiple data simultaneously. This paper proposed an optimal parallel architecture of AES algorithm at both data and control level which is suitable to be implemented on multicore architecture. AEs algorithm is implemented in C programming language and parallelized using OpenMP standard.

- **Paper by J.Saira Banu, M.Vanitha, Dr. J.Vaideeswaran, Dr. S.Subha titled "Loop**

DOI 10.17148/IJARCCE.2016.5283

Parallelization And Pipelining Implementation of AES Algorithm Using OpenMP and FPGA".
The main focus of this paper work is to increase throughput of AES algorithm through hardware and software technique. In this paper many optimization techniques are used like pipelining, Loop unrolling and iterative design.Here they adopted pipelining technique to to increase the speed of the algorithm by performing multiple rounds simultaneously. OpenMP is tool to achieve software parallelization to increase the speedup of the algorithm compared to its sequential version.A pipelined architecture AES-128 is implemented using Xilinx xc5vlx110t-1 device achieve a throughput of 31.25 Gbps which is more effective than previous ASIC implementations. By using OpenMP they achive speed up of 1.08 in the dual core.

V. PROPOSED WORK

This project presents the implementation of Advance encryption algorithm using parallel computing. This paper presents the parallel implementation of AES using openMP which provides flexibility and performance improvement in terms of speed up factor. Here we have parallelized the encryption and decryption process of AES algorithm by making use of openMP directives to reduce execution time. Due to openMP directives overhead it fails to give optimal result while input size is small or processing is small at that time sequential algorithm gives better performance than parallel algorithm. After particular amount of input data sequential algorithm fail to give optimal speed up than parallel algorithm. We find out threshold value in terms of input data size from where we take decision which algorithm need to take care of that input data. If data size smaller than calculated threshold then input is processed sequentially otherwise if data size is greater than threshold value it going to be processed parallel algorithm.

Threshold value is calculated by trial and error method.

VI. CONCLUSION

In real time application large amount of data is generated and it is necessary to encrypt and decrypt it in real time to match data generation speed and processing speed. Hance it is necessary to increase speed up of encryption and decryption algorithm. Our proposed work is able to take decision on real time date and processed it with best available speedup.

REFERENCES

[1] Piotr Bilski , Wiesław Winiecki, 2010 ,Multi -core implementation of the symmetric cryptography algorithms in the measurement system, Measurement 43 (2010) 1049–1060, Elsevier.10.1016/j.measurement.2010.03.002.

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

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

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

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

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

BIOGRAPHY

Vishal Sathawane was born on 16th June 1991. He is currently pursuing Post graduation studies in the final year of Master of technology (2014-2016) in Computer Science and Engineering at Shri Ramdeobaba College of Engineering and Management, Nagpur under Rashtrasant Tukadoji Maharaj Nagpur University,Nagpur, Maharashtra State, INDIA. He is graduate from Rajiv Gandhi College of Engineering, Nagpur.

DOI 10.17148/IJARCCE.2016.5283