"Smart Secure System using Parallel AES"

Ankit Khedlekar [#1],

[#] Computer Engineering, RMD Sinhgad School of Engineering
ankitkhedlekar71@gmail.com

Tejas Shelke[#2],

[#] *Computer Engineering, RMD Sinhgad School of Engineering*
teja.shelke@gmail.com

Shraddha Walhekar [#3],

[#] *Computer Engineering, RMD Sinhgad School of Engineering*
shraddha.walhekar27@gmail.com

Nikhita Nerkar [#4],

[#] *Computer Engineering, RMD Sinhgad School of Engineering*
nerkar.nikhita@sinhgad.edu

Abstract: - **Today, computer networks are becoming more important for exchanging information. One of the most important requirements of these networks is to provide secure transmission of information from one place to another. Cryptography is one of the techniques which provide the most secure way to transfer the sensitive information from sender to intended receiver. Advanced Encryption Standard (AES) algorithm is one of the most important cryptography algorithms for hiding the sensitive information, but AES algorithm has many performance limitations such as memory requirement and execution time. One of the solutions to reduce the execution time of AES algorithm is by using parallel computation. Our application is to store confidential files in an encrypted format in our storage devices. This will give us security to carry any documents without worry. The application will read a file, encrypt and store it back into the file system by over writing the file. To encrypt the file content we will use the parallel AES algorithm.**

Keywords:- ***AES, Cryptography, Security, MongoDB, GridFS, Parallel Computation.***

I. INTRODUCTION

In today's high technology environment, organizations are becoming more and more dependent on their information systems. The public is increasingly concerned about the proper use of information, particularly personal data. The threats to information systems from criminals and terrorists are increasing. Many organizations will identify information as an area of their operation that needs to be protected as part of their system of internal control. Therefore there is a need to provide secure transmission of information from one place to another. Security in networking is based on the Cryptography. Cryptography, a word simply means "secret writing". It is nothing but the science and art of transforming messages to make them secure and immune to attacks. Cryptography can provide confidentiality, integrity, authentication and non repudiation of messages. Cryptographic algorithms can divide into two groups: Symmetric key cryptography (secret-key) and asymmetric key cryptography (public key) algorithms. AES was designed because Data Encryption Standard's key was too small. AES is the Symmetric key cryptography algorithm. AES uses the same key to encrypt and to decrypt the messages. The key is shared between the sender and the user. But AES has many performance limitations. Therefore much more time required for encryption and decryption of information. Due to the time limitations we use the parallel AES algorithm. Parallel AES algorithm helps to divide the information in small chunks and these chunks are given to the threads to perform encryption and decryption. This complete process is done in parallel. In our proposed system we used MongoDB for data storage. It is open-source databases which can uses various documents vary in structure. MongoDB uses collections instead of tables for data storage. Organizations of all sizes are adopting MongoDB because it enables them to build applications faster, handle highly diverse data types, and manage applications more efficiently at scale. We have also used the concept of GridFS to store the data into small chunks for parallel computation. GridFS is a simple file system abstraction on top of MongoDB. When a file is uploaded to GridFS, the file is split into chunks of 256k and stored separately. So when you need to read only a certain range of bytes of the file, only those chunks are brought into memory and not the whole file. This is extremely useful when dealing with large media content that needs to be

selectively read or edited. By default MongoDB document size is capped at 16MB. So if you have documents that are greater than 16MB you can use store those using GridFS.

II. LITERATURE SURVEY

In this year, Vandan Pendli, Mokshitha Pathuri, Subhakar Yandrathi, Abdul Razaque all these authors described the concept of parallel programming by using a multicore processor with the help of AES [1].

In this year, Xiongwei Fei, Kenli Li,Wangdong Yang, Keqin Li presented a secure and high efficient file protecting system based on SHA3 and parallel AES [2].

In 2015, Puneet Kumar, Shashi B. Rana, observed that by increasing number rounds of AES algorithm the security is improved. They also stated that how AES algorithm is better than other modern algorithms for security [3].

In 2014, M.Sambasiva Reddy, P.James Vijay, B.Murali Krishna, presented 4 different AES cipher implementations with both on offline key expansion on a fine grained many-core system. Each implementation exploits different levels of data and task parallelism [4].

In 2013, Bin Liu, Student Member, IEEE, and Bevan M. Baas, presented 16 different AES cipher implementations with both online and offline key expansion on a fine-grained many-core system [5].

In 2011, Nhat-Phuong Tran, Myungho Lee, Sugwon Hong, Seung-Jae Lee, proposed a new parallelization approach for data encryption/decryption application, AES- CTR. The proposed approach parallelizes the AES-CTR by extending the data block size encrypted at one time [6].

In 2010, Fei Shao, Zinan Chang, Yi Zhang, measured the speed of these CPU-based encryptions on the same test machine, and we got results using the same AES algorithm [7].

In 2009, Mohammad Ahmed Alomari, Khairulmizam Samsudin, Abdul, Rahman Ramli, evaluated the performance of encryption algorithms and modes of operation that are suitable for storage encryption [8].

III. PROPOSED SYSTEM

In Smart Secure System, the parallel AES algorithm is used for encryption and decryption process. Data security is a major issue for businesses and organizations today. Ensuring that your data is secure is becoming more important every day and vital to business operations. So this system provides a way of better security to the client's vital and credentials files. Client can store their data on a server which is totally secure and confidential. The data or file which are stored on the server are completely in encrypted form. The database is also in secured form in system. Multiple clients can use this system at a time without any interference. They should register with unique user name and password. User's password will be considered as a key to encrypt and decrypt the file. For encryption and decryption process we use the AES algorithm.

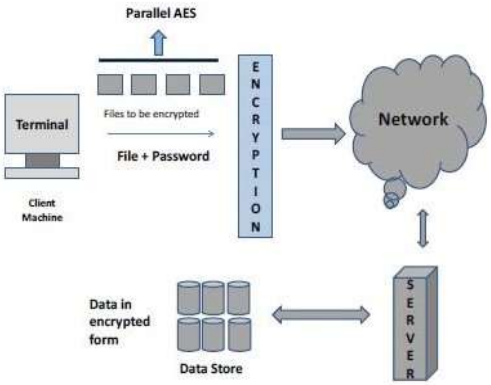

Fig.1 System Architecture (Encryption)

In above Fig.1, the process of encryption is described. Client should register himself using unique user name and password. The password is the key for encryption and decryption. Then he can upload the files on server, download the files which are stored on a server, delete the files which are not necessary, and also search the files. Suppose client wants to upload/store the files on server then while uploading the files through network parallel AES does its work. Using client's password files get encrypted and distributed into the chunks (threads). This process of distribution is done by the GridFS in a MongoDB. Here we uses the concept of JavaThreads. Java threads do the encryption of data in parallel and after that they merge it into a single file and send it to the particular receiver through IP address of that receiver. Suppose file size is 5 Mb then the file is distributed to the java threads with a respected size of 256k, and then encryption process done in parallel. Each thread do its encryption and finally all threads get merged and we get final original file. In our scenario the receiver is nothing but the server on which we want to store the files. On a server side the files are stored in encrypted format and also in database the files are in a cipher text. Hence in our system the database is also secured. No one can halt the data by attacking, because it is in encrypted form.

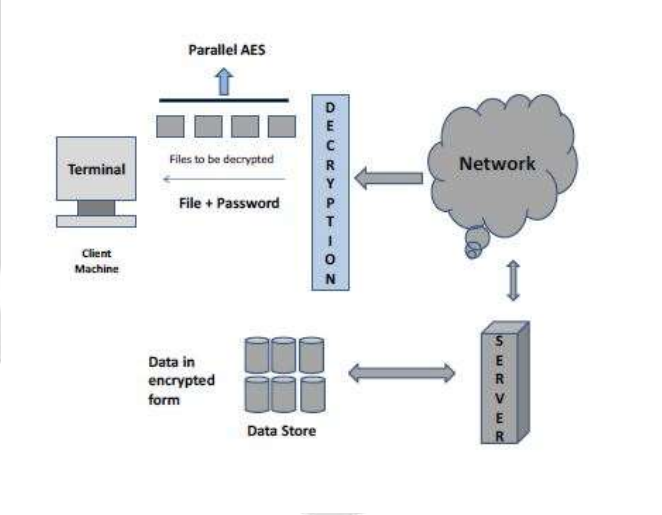

Fig.2 System Architecture (Decryption)

In above Fig.2, it explains the process of decryption. The process of decryption is as same as an encryption process. Consider client wants to download some files which are stored on server. For this process also, client authenticates himself using username and password. When he requests for specific file then server acknowledges through the requested file which is in encrypted form. While transmitting through the network the files get decrypted using client's unique password.

IV. RESULTS AND PERFORMANCE ANALYSIS

Results mentioned here are based on the different files using Parallel AES algorithm.
Hardware Description: Intel Dual Core, 2GB RAM with Ubuntu Operating system.
IDE: NetBeans.

Programming Language: JAVA
Database: MongoDB

Table.1: Comparative results

Input File (Size in MB)	Sequential execution result	Parallel execution result
1	2010ms	1089ms
10	3125ms	1578ms
150	7829ms	3252ms

The implementation results reported in this section make the comparison between the sequential and parallel implementation of AES block cipher. The graphical representation of time for encryption and decryption process explained in next scenario. In this graph, the blue line shows the execution time for sequential implementation and the orange line shows the execution time for parallel implementation. The graph shows the difference in execution time for sequential and parallel implementation for both encryption and decryption process.

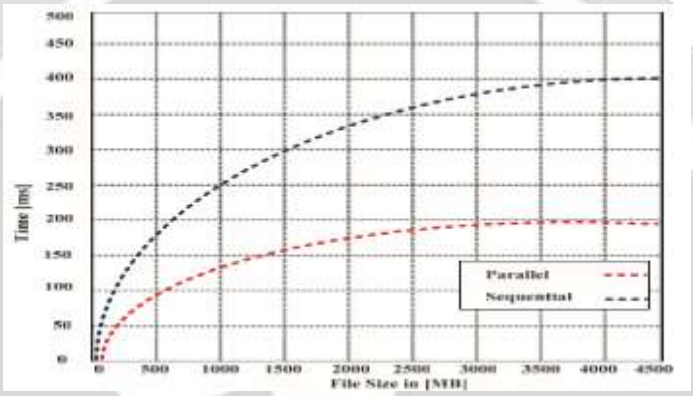

Fig.3 Comparison between Serial and Parallel execution.

V. EXECUTION

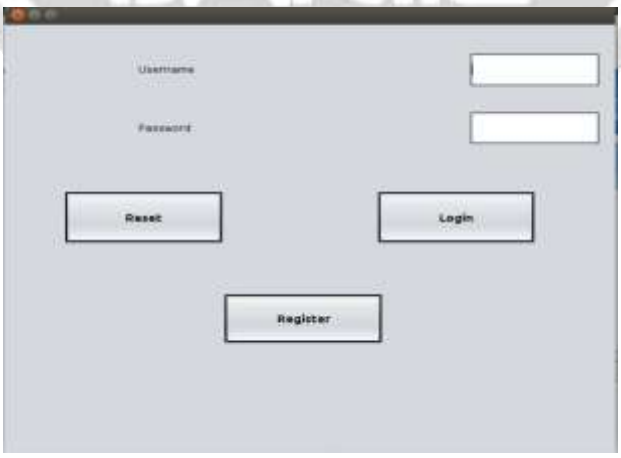

Fig. 4 Login Form

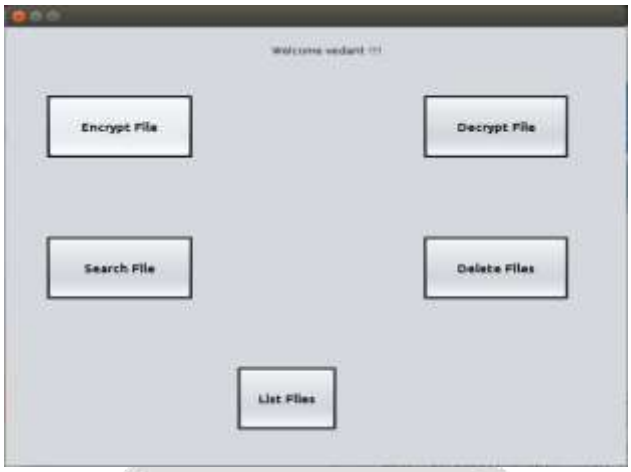

Fig. 5 Home Form

Fig. 6 Encryption

Fig. 7 Decryption

VI. CONCLUSION

In this paper, shows the parallel implementation of AES algorithm and using this algorithm we implement a secure smart system which is used to store the files on a server which is totally confidential and secure.

VII. REFERENCES

[1] VandanPendli, MokshithaPathuri, SubhakarYandrathi, Abdul Razaque (2016)"Improvising performance of Advanced EncryptionStandard Algorithm," *Department of Electrical Engineering, Department of Electrical Engineering, Department of Electrical Engineering,Cleveland State University, Cleveland State University, Cleveland State University,Cleveland, Ohio*

[2] XiongweiFei, KenliLi,Wangdong Yang, Keqin Li(2016) "A secure and efficient file protecting system based on SHA3 and parallel AES", Hunan University, China

[3] Puneet Kumar, Shashi B. Rana (2015) "Development of modified AES algorithm for data security", Guru Nanak Dev University, India

[4] M.Sambasiva Reddy, P.James Vijay, B.Murali Krishna (2014) "Design and Implementation of Parallel AES Encryption Engines for Multi-Core Processor Arrays.," , India

[5] Bin Liu, Student Member, IEEE, and Bevan M. Baas (2013) "Parallel AES Encryption Engines for Many Core Processor Arrays.,"

[6] Nhat-Phuong Tran, Myungho Lee, Sugwon Hong, Seung-Jae Lee (2011) "Parallel Execution of AES-CTR Algorithm Using Extended Block Size."

[7] Fei Shao, Zinan Chang, Yi Zhang, (2010)"AES Encryption Algorithm bsed on the High Performance Computing of GPU.," in China.