Parallel File Protecting System

Sheetal Adagale[1], Aishwarya Sawant[2] ,Pratiksha Pandagale[3],Trupti Zanje[4], Prof.Kanchan Varpe[5]

[1] Student, Computer Engineering, RMDSSOE, Maharashtra, India
[2] Student, Computer Engineering, RMDSSOE, Maharashtra, India
[3] Student, Computer Engineering, RMDSSOE, Maharashtra, India
[4] Student, Computer Engineering, RMDSSOE, Maharashtra, India

ABSTRACT

Now a days protecting outsourced data in storage databases and data warehouses against corruptions, adding fault tolerance to storage file system, along with efficient data integrity checking and recovery procedures,becomes difficult. Data Owner worry and even fear about their security problems, such as stealing, breaking, forging,and so on.Regenerating codes provide fault tolerance by striping data across multiple servers, while using less secure codes than traditional ensure codes during failure recovery. This needs secure and efficient way to protect private data from these types of issues.To tackle this problem we have proposed secure file system that remotely checks the integrity of regenerating-coded data against corruptions under a real-time file storage sytsem. In proposed system we optimized SHA3-256 and Parallel AES algorithm for security purpose and for maintaining the data integrity and confidentiality with GPU(Graphical Processing Unit) and CPU for high performance.The proposed system will use CPP(CPU Parallel Protecting) CPU parallel protecting and GPP(GPU Parallel Protecting) GPU parallel protecting ,HPP(Hybrid Parallel Protecting) and HPUP(Hybrid Parallel Unprotected) protecting algorithms.This proposed work will improves security of SEFPS(Secure and Efficient File Protecting System) in terms of integrity and confidentiality.

Keyword : - *CPU, GPU, AES Encyption, SHA,CUDA*

1. INTRODUCTION

Today we live in the era of Information Technology. We have to learn all that things which are very helpful for living a life such as how to secure our credentials from illegal usage. The highly increasing rate of new technologies in industries side by side security issue of the data is also increases. Many improvements are implemented over security of data such as encryption-decryption of data, security algorithms such as MD5 SHA2.SHA3, SHA3-256, AES etc. many security tools are developed for security, thus we have to secure our confidential file and credentials using all these things. For achieving efficiency in system performance not only security of data is important, but also efficient performance of the system using that algorithms is also important, therefore for increasing the speed of the execution of files parallel computing concept is used.

In parallel computing data execution is done in parallel manner. It means that in existing system security as well as parallel data execution is provided. For parallel computing GPU is used for parallel execution. GPUs are more suitable for efficient working and also suitable for efficient encrypting. The GPUs support larger integer computations and because of this it uses CUDA (NVIDA framework)platform for parallel programming.CUDA makes improvement for encrypting performance by using parallelism. Using CPUs it also gives the better performance. The most popular and widely used standard is used for encrypting data which is called as AES(Advanced Encrypting Standard). It encrypts/decrypts data as group of 16byte.It can be executed in parallel way on GUPs or CPUs also. In tamper-proofing technologies,the message digest algorithm MD series and SHA(Secure Hash Algorithm) series is used. In existing system only focus on improvement of AES performance by parallelism and it having some weakness in protecting files and performance is also not considered, therefore there is need to develop a file protecting system with both high performance and security.

2. PROBLEM CONTEXT

To implement a secure and efficient file protecting system using parallel AES and SHA3.In proposed system for achieving parallelism GPU is used with the help of CUDA.

2.1 FILE PROTECTING ALGORITHMS

The security of digital information contains protecting data, such as a database from stealing and destroying information from the unwanted actions of unauthorized users. Preserving the integrity, availability, and confidentiality these are the security measures achieved by parallel encryption and decryption using file protection algorithm,

- SHA3.
- Parallel AES.

The main objective of the SHA3 and parallel AES is providing security to the file system. The main key points in security are Authentication, Access Control, Confidentiality, and Integrity.

- *Authentication:*
  Communicating entity is who has claimed to be assured.

- *Access Control:*
  Prevention of resources from the unauthorized access.

- *Confidentiality:*
  Protection of information from unauthorized disclosure.

- *Integrity:*
  Checking information is same received by the authorized owner.

In contrast, these services are achieved by the security mechanism. Security mechanisms are design to identify secure and recover from the attacks. In SEFPS work flows contains file protection and unprotecting.
Message Digest is the fixed-size hash or a unique code contains MD5 series and SHA3 series. A hash function H maps bit-strings of some length from a domain D to strings of fixed length (n) in range R with H: D→R and |D| > |R|. Particular message or hash values considered as a fingerprint of the message. Cryptographic hashing function may be different to a certain degree stronger security requirements.

Compression function:

It’s a function H which associates the fixed-length input to a fixed-length output i.e.

$$H :\{0, 1\}b□n\ □\{0,1\}n$$

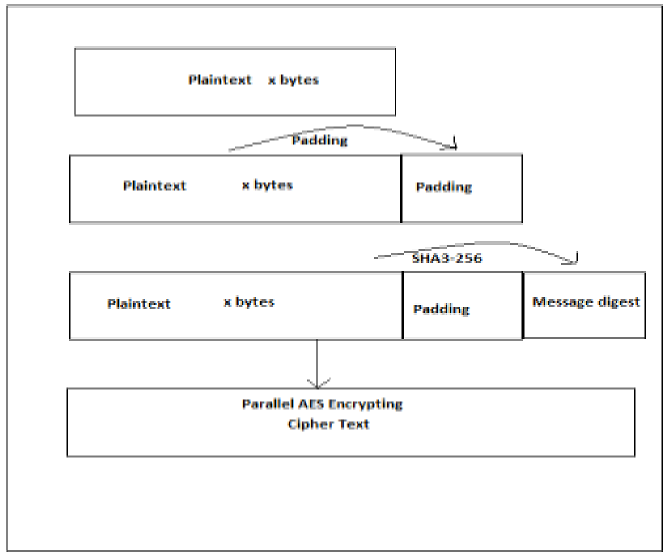
Where, H maps b + n bits to *n* bits

In this file protecting system we first use SHA and use parallel AES encryption for the file protection. SHA3 used in pidgin of the data tamper proofing. Parallel AES algorithm not only for security but used also for great speed. Both hardware and software implementation are faster still, proposed by encryption standard recommended by NIST to Encrypts data blocks of 128 bits in 10, 12 and 14 round It can be implemented on various platforms especially in small devices. It is carefully tested for much security applications.

2.FLOW

2.1 Encryption

While protecting file, first padding the some bit in the length 16-bytes. Padded bits then hashed by the SHA algorithm and then attach message with the file. After message digested in the file the file secured and tamper-proofing encrypting by AES algorithm will stored on the internet or on the file system.

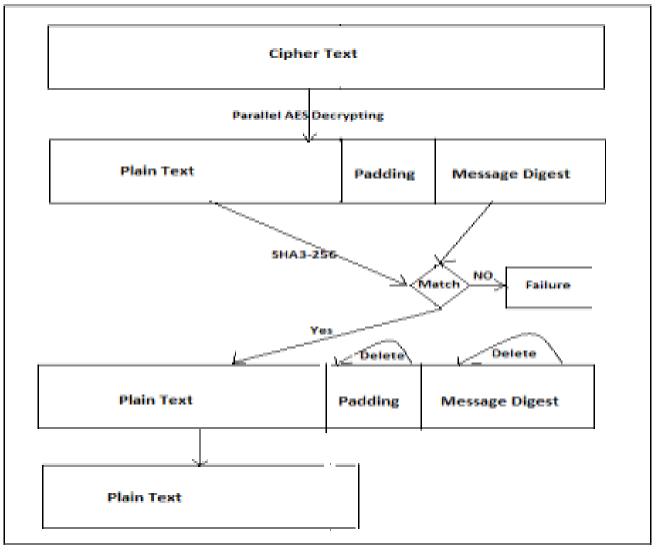


[Xiongwei Fei a, 2016]

Fig -1: **Encryption by using SHA3 and parallel AES**

2.2Decryption:

Decryption is the process of unprotecting data. This process backs the encrypted data in original form. Data is decrypted by the parallel AEs algorithm. Then data retrieved from the file hashed by the SHA3 algorithm. Then recovered digested message will be compared with the original digested message if they both are same then file is the original file. And if both messages are different then alert will be sent to data owner about data alter may happen.



[Xiongwei Fei a, 2016]

Fig -2: **Decryption by using SHA3 and parallel AES**

2.3 Overview of GPU and CPU:

2.3.1 GPU:

GPU (Graphic Processing Unit) has higher data transfer bandwidth and better parallelism and its high-performance computing capability. Parallel AES algorithm performance improved by using GPU's high computation capability.

GPU parallel protecting for parallelism used in protecting the file. GPU has two algorithms GPP and GPUP used in protecting and unprotecting the file. These algorithms use file name as keys which is used in protecting and unprotecting the file. . NVIDIA first proposed GPU has stronger performance and a more perfect programmable construction

2.3.2 CPU

CPU (Central Processing Unit) correspondingly used with GPU, parallely achieving the high performance of the encryption and decryption in secured and highly efficient file protecting system. CPU parallel protecting used for the protection of file and CPUP is used for unprotecting the file.

3. Architecture

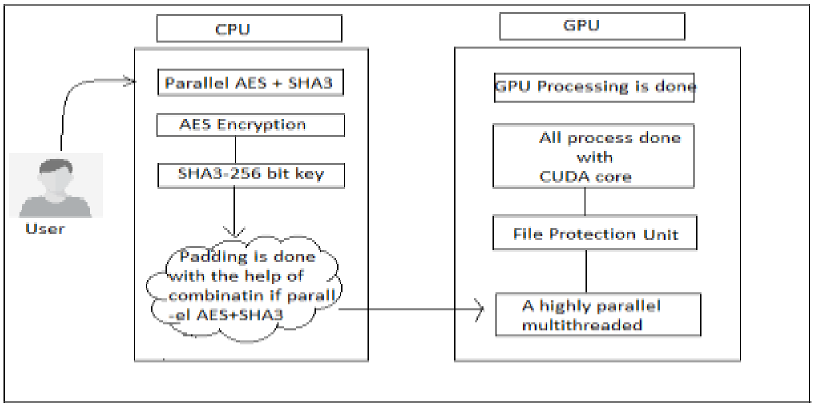

CPU
GPU
Parallel AES + SHA3
AES Encryption
SHA3-256 bit key
User
Padding is done with the help of combinatin if parall -el AES+SHA3
GPU Processing is done
All process done with CUDA core
File Protection Unit
A highly parallel multithreaded

Fig 3.System Archtecture

Secure file and efficient file protecting system uses parallel AES and SHA3-256 algorithms. User given file input to the system. File is x byte length then in that file some bytes will be added to make sure that file is in multiple of 16 bytes. All bits are padded by using SHA3-256. Then message digested in file or attaché the digested message with the file.

AES encryption algorithm encrypts all data in cipher text for securing data and tamper-proofing. In all we use CPU and GPU with AES and SHA3 for achieving high performance. Efficient CUDA implementation to perform on the GPU using atomic operation. CUDA-enabled GPUs support for atomic summation operation of double precision floating-point numbers. GPU processing is done with core CUDA unit.

4 . MATHEMATICAL EVOLUTIONS

Integrated mathematical steps necessary for implementation. The first expression to final all includes input of our system with the help of mathematical parameter. In this section we design mathematical expressions with the help of our existing and proposed system of our system.

Algorithms:

AES Algorithm Psuedocode

```
Cipher(byte in[16], byte out[16], key_array round_key[Nr+1])
begin
byte state[16];
state = in;
AddRoundKey(state, round_key[0]);
for i = 1 to Nr-1 stepsize 1 do
```

```
SubBytes(state);
ShiftRows(state);
MixColumns(state);
AddRoundKey(state, round_key[i]);
end for
SubBytes(state);
ShiftRows(state);
AddRoundKey(state, round_key[Nr]);
end
```

SHA3 Algorithm:

```
SHA3:=proc(message::string , messagetype::name:=text)
local n,m,l;
if type(procname,'indexed')then
        n:=op(procname)
else
        error"output length not specified"
end if;
if not  n in {224,256,384,512}then
error"%1 is not a valid output length",n
end if;
m:= messagetobytes(message,messagetype);
l:=keccak(m,1600,1600-2.n,n,hash);
bytestohexstring(l)
End proc;
```

Above algorithms such as AES and SHA3-256 are used for parallel encryption and decryption and key generation respectively.

5. CONCLUSIONS

The proposed system presents secure and efficient file protecting system by using multi-core processor, CUDA programming, SHA3-256 and parallel AES .This system used for the protection of the users file in a network. This system helps to maintain confidentiality and integrity of the data. In proposed system for encryption and decryption parallelism is required so that CUDA is used for parallel encryption and decryption process. These system implements six algorithms of SEFPS CPP, GPP, CPUP, GPUP, HPP, and HPUP. This system trying to achieve better performance in case protecting and unprotecting file encryption, decryption speed. Proposed system provides security to the users file using parallel AES and optimizing SHA3-256 algorithm. In future it works with blake2-b algorithm. It achieves high speed computing power than existing system.

6. REFERENCES

[1]. Xiongwei Fei , Kenli Li , Wangdong Yang , Keqin Li,A secure and efficient file protecting system based on SHA3 and parallel AES,Parallel Computing 52(2016)106-132

[2]. A. Pousa, V. Sanz, A. de Giusti, Performance analysis of a symmetric cryptographic algorithm on multicore architectures, in: Computer Science & Technology Series-XVII Argentine Congress of Computer Science-Selected Papers, Edulp, 2012, pp. 57–66.

[3]. W. Yang, K. Li, Z. Mo, Performance optimization using partitioned SPMV on GPUs and multicore CPUs, IEEE Trans. Comput. 64 (9) (2015) 2623–2636.

[4]. H.-V. Dang, B. Schmidt, Cuda-enabled sparse matrix–vector multiplication on GPUs using atomic operations, Parallel Comput. 39 (11) (2013) 737–750.

[5] M. Krotkiewski, M. Dabrowski, Efficient 3d stencil computations using cuda, Parallel Comput. 39 (10) (2013) 533–548.

[6] -L. Duta, G. Michiu, S. Stoica, L. Gheorghe, Accelerating encryption algorithms using parallelism, in: 2013 19th International Conference on Control Systems and Computer Science (CSCS), IEEE, 2013, pp. 549–554.

[7] H. Chen, P. Lee, Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation, IEEE Trans. Parallel Distrib. Syst. 25 (2) (2014) 407–416.

[8] L. Tan, S.L. Song, P. Wu, Z. Chen, R. Ge, D.J. Kerbyson, Investigating the interplay between energy efficiency and resilience in high performance computing, in: Proceedings of the 29th IEEE International Parallel and Distributed Processing Symposium, IEEE, 2015, pp. 786–796

[9] K. Li, J. Liu, L. Wan, S. Yin, K. Li, A cost-optimal parallel algorithm for the 0–1 knapsack problem and its performance on multicore cpu and gpu implementations, Parallel Comput. 43 (2015) 27–42.

[10] X. Shi, F. Park, L. Wang, J. Xin, Y. Qi, Parallelization of a color-entropy preprocessed chan-vese model for face contour detection on multi-core cpu and gpu, Parallel Comput. 49 (2015) 28–49.

[11] M. Nagendra, M.C. Sekhar, Performance improvement of Advanced Encryption Algorithm using parallel computation, Int. J. Softw. Eng. Appl. 8 (2) (2014) 287–296.

[12] Attacks on and Advances in secure Hash Algorithm. Neha Kishore Member IAENG and Bhanu Kapoor.

[13] B. Liu, B.M. Baas, Parallel aes encryption engines for many-core processor arrays, IEEE Trans. Comput. 62 (3) (2013) 536547.

[14] J. Diaz, C. Munoz-Caro, A. Nino, A survey of parallel programming models and tools in the multi and many-core era, IEEE Trans. Parallel Distrib. Syst.23 (8) (2012) 13691386.

[16] T. Nhat-Phuong, L. Myungho, H. Sugwon, L. Seung-Jae, High throughput parallelization of AES-CTR algorithm, IEICE Trans. Inform. Syst. 96 (8) (2013)16851695

[17] Q. Dong, J. Zhang, L. Wei, A sha-3 based rfid mutual authentication protocol and its implementation, in: 2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC), IEEE, 2013, pp. 15

[18] N. Moreira, A. Astarloa, U. Kretzschmar, Sha-3 based message authentication codes to secure IEEE 1588 synchronization systems, in: 39th Annual Conference of the IEEE on Industrial Electronics Society (IECON13), IEEE, 2013, pp. 23232328.

[19] X. Shi, F. Park, L. Wang, J. Xin, Y. Qi, Parallelization of a color-entropy preprocessed chan-vese model for face contour detection on multi-core cpu and gpu, Parallel Comput. 49 (2015) 2849.

[20] C. JunLi, Q. Dinghu, Y. Haifeng, Z. Hao, M. Nie, Email encryption system based on hybrid aes and ecc, in: IET International Communication Conference on Wireless,Mobile and Computing (CCWMC11), IET, 2011, pp. 347350