SECURITY, ISSUES AND ALGORITHM AND THEIR PERFORMANCE ANALYSIS

Neelam Choubey[1], Virendra Singh[2]

[1]M. Tech Scholar Dept. Of Computer Science Engineering, Babulal Tarabai Institute of Research and Technology Sagar, M.P. India
[2]Asst. Prof. Dept. Of Computer Science Engineering, Babulal Tarabai Institute of Research and Technology Sagar, M.P. India

---***---

Abstract - *Homogeneous computing in Cloud severely limits the computational power it can potentially provide. Therefore, it is strongly desired to have new and comprehensive solutions to maintain all benefits from Cloud and suppress backsides.*

This thesis proposes three solutions to address security, computation and data issues in Cloud. Firstly, a GPU MapReduce framework specifically aims at improving performance and reducing energy consumption to data parallel problems.

In addition, the P-CP-ABE scheme overcomes not only the difficulties of data security, access control, and key management issues in Cloud, but also the overall performance is enhanced dramatically.

Finally, the multi-tenancy technology requires a strong network authentication protocols to assure authenticity and non repudiation in the Cloud.

1. INTRODUCTION

In addition, Cloud has started a new revolution on parallel and distributed computing world in late-2000s. Since Cloud provides the opportunities of resource sharing and server consolidation, the barrier of investment to get in the Internet business has been removed mostly and the average cost to overall players in the market has been reduced significantly as well.

Even though Cloud looks like having many comparative advantages over traditional infrastructures, the risks of overlapping trust domain objects may wash out all benefits. Moreover, because of resource sharing and server consolidation, the entire hardware-software stack becomes attacking surfaces to the applications in the Cloud.

To cope the backsides, cryptographic mechanisms, such as public key infrastructures, have been widely used in the Cloud. However, key management has become a critical challenge in traditional public key infrastructures. Although certificate is a general solution, we need a better and comprehensive technology. Bethencourt et al. proposed a Cipher text- Policy Attribute Based Encryption (CP-ABE) scheme in 2007.

CP-ABE is a special public key cryptography scheme that includes three natural superiorities: all users share one copy of public key; normally, one copy of plaintext is encrypted to single cipher text for different users rather than many different cipher texts in traditional cases; and expressing the access control policy in fine grained naturally. On the other hand, the main difficulty of CP-ABE comes from its complexity. Its major components such as paring and elliptic curve computations slow down the processes of key generation, encryption and decryption. But also, the existing CP-ABE system was written in a sequential algorithm, which worsens the performance.

As a result, CP-ABE seems impractical to the applications of industries. To take the advantages of CP-ABE in Cloud, we are introducing Parallelized Cipher text-Policy Attribute-Based Encryption, P-CP-ABE as abbreviation.

2. RESEARCH METHODOLGY

There are four main points related to the P-CP-ABE will be explained in this thesis as follows:

Analyze the existing CP-ABE thoroughly to identify performance bottlenecks.

Parallelize key generation and encryption/decryption processes by using multithreading technique.

Switch encryption from Cipher Block Chaining (CBC) mode to Counter (CTR) mode.

Conduct experiments to demonstrate performance gains.

There are four main points related to the P-CP-ABE will be explained in this thesis as follows:

1 Analyze the existing CP-ABE thoroughly to identify performance bottlenecks.

2 Parallelize key generation and encryption/ decryption processes by using multithreading technique.

3 Switch encryption from Cipher Block Chaining (CBC) mode to Counter (CTR) mode.

4 Conduct experiments to demonstrate performance gains.

3. RESEARCH TOOLS

There many tools available in the market but some of them used in the research are as follows:

- Cloud Sim:
- Map Reduce Algorithm
- GPU
- Nvidia GTX970
- CBC: Cipher Block Chaining etc

This algorithm was able to locate the selected file from large datasets. Essentially, keying the desired time will provide the user with the file index and its corresponding start and end time and the file name as shown in above figure. However, if the time is not found, then the algorithm locates a time that is within close proximity to the searched query, which is achieved with a nearest search algorithm.

4. RESULTS

Parallelization of Key Generation

The tested is a machine with Intel I3 4010U, which has two cores and supports Hyper-Threading technology.

Current P-CP-ABE adopts multithreading for shared memory parallelization. Thus, choosing a correct number of threads will be critical. Once more threads are selected than the physical core or hyper-core supported by Hyper Threading technology, extra threads will cause the penalty for creation, maintenance and synchronization.

In Linux systems, sysconf might provide a good sense about the actually available computing units for P-CP-ABE. We can simply use sysconf (_SC_NPROCESSOR_ONLN) as the actual number of the created threads to distribute input data to all threads as evenly as possible. However, this might fit in all cases.

If the number of input data items is a multiple of sysconf(_SC_NPROCESSOR_ONLN), the number of threads equals to sysconf (_SC_NPROCESSOR_ONLN). Otherwise, one more thread will be created to handlethe leftovers. Thus, the number of threads will be sysconf (_SC_NPROCESSOR_ONLN)+1.

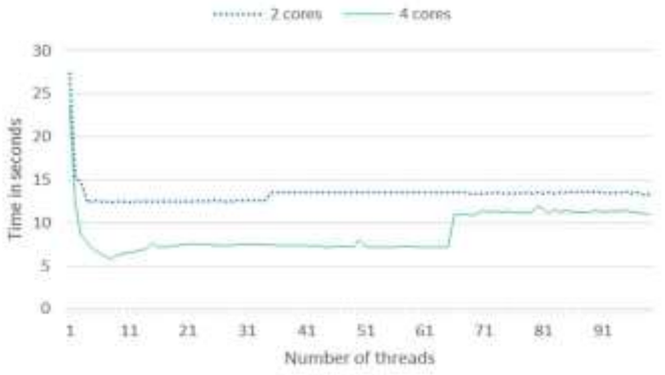

Figure 1 Performance of generating private keys in 50 attributes

In Figure 1 above, for example, we are generating private keys with constantly50 numerical policies by creating different quantities of threads to do so. The differences are obvious. In our environment that Intel I3 4010U, which has two cores with Hyper-Threading technology, there is a speeding up about 2.38 times when parallelization was used and at least 5 attributes inputted.

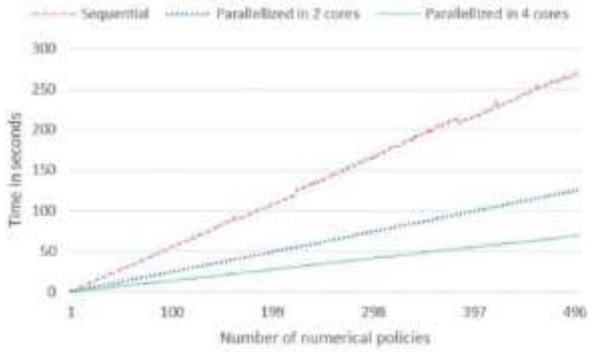

Figure 2 Speedups and efficiencies of private key key generation

Based on Figure 2, our construction has a significant performance gain comparing to the original CP-ABE. We have tested 500 times from only one numerical policy to 500 numerical policies. We can see that there are at least 2 times speedup in 2cores platform and about 4 times speedup in 4 cores platform. Moreover, we knew that only an ideal parallel system containing p processing elements can deliver speedup equal to p and efficiency could be equal to one. Hyper threading is the main reason that superliner speedup has been created, which causes the speedup beyond processing elements and efficiency excesses one. According to the efficiency showed in Figure 26 above, parallelization on key generation might not be very good in scalability because its efficiency is asymptotically greater than (1). This is where we are going to keep working on.

Parallelization of Encryption and Decryption

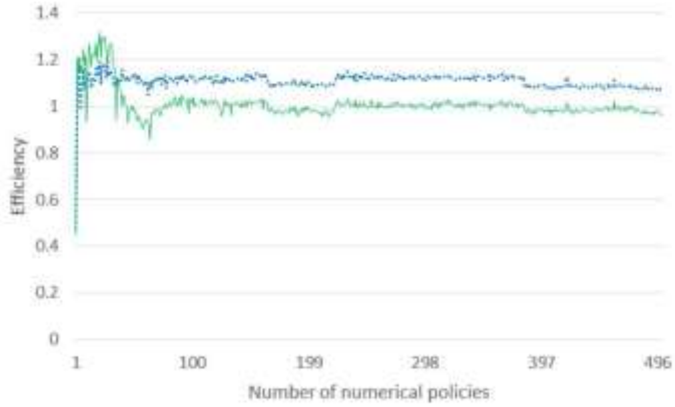

Figure 3 Speedups and efficiencies of encryption

According to Figure 3 that we have tested the encryption on 1000 different input sizes from one megabyte to 1000 megabytes, we can see that parallelization on encryption and decryption of our system is cost-optimal and very scalable due to it has the ability to maintain efficiency at a relatively fixed value by simultaneously increasing the number of processing elements and the size of data. In the first graph of Figure 28 above, we only included 100 results for showing that even though the problem size is relatively small, our system still has at least the same or better performance to the original CP-ABE system.

5. CONCLUSION

In this thesis, new solutions to the security, computation, and data issues in Cloud have been presented: the GPU MapReduce framework enhances the performance of data parallel problems in Cloud; the P-CP-ABE aims at the issues of data security and access control in Cloud; and, the strong network authentication protocol suite targets at the difficulties of authenticity and repudiation in Cloud, which is built on top of multi tenancy and service oriented architecture. According to the experimental results, solutions have been proved to be relatively better than traditional mechanisms in the given scenarios.

The designing purposes of the GPU MapReduce framework are illustrated as follows: taking advantages of GPU architecture as much as possible; reducing communication overhead and making threads independent to each other as much as possible; hiding memory latency by launching a large number of threads with a large enough problem size; decomposing the inputs as even as possible; and reducing both local and global synchronizations as much as possible.

Traditional encryption algorithms (both symmetric and asymmetric ones) fail to support Cloud well due to their severe issues such as complex key management and heavy redundancy. CP-ABE scheme overcomes the aforementioned issues and provides fine-grained access control as well as reduplication features. But, its high complexity has prevented it from being widely adopted. On the other hand, P-CPABEscheme addresses the performance issues by parallelizing CP-ABE and porting it to multi-core architecture machines. Major performance bottlenecks such as key management and encryption/decryption processes are identified and accelerated.

Moreover, New AES encryption operation mode is adopted for further performance gains as well.

The strong network authentication protocol suite includes three identities: central authenticator (CA), servers, and users. In addition, the protocol suite assumes neither user nor server trusts each by communicating on top of the insecure network; and, both the user and server have CA's public key. Because of P-CP-ABE, CA, users, and servers share only one copy of public key, all public keys in the infrastructure will be certified if CA's public key is certified. Consequently, the burden of key management in the infrastructure is relieved.

REFERENCES

[1] L. Li, X. Chen, H. Jiang, Z. Li, and K. C. Li. P-cp-abe: "Parallelizing ciphertextpolicy attribute-based encryption for clouds." In 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pages 575–580, May 2016.

[2] Jonathan Katz and Yehuda Lindell, &quot; Number Theory and Cryptographic Hardness Assumptions, & quot; Introduction to Modern Cryptography Second Edition, 2015.

[3] M. Zaharia et al. Resilient distributed datasets: a fault-tolerant abstraction for in-memory cluster computing. NSDI, 2012.

[4] S. Davis Z. Qiao, S. Liang and H. Jiang. "Survey of attribute based encryption." SNPD 2014, 2014.

[5] Brent Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," Public Key Cryptography—PKC 2011, pp. 53--70, 2011.

[6] Allison Lewko and Brent Waters, "Decentralizing attribute-based encryption," Advances in Cryptology--EUROCRYPT 2011, pp. 568--588, 2011.

[7] A. Lewko and B. Waters. "Decentralizing attribute based encryption. Advances in Cryptology" - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2011.

[8] R. Steinwandt V. Bozovic, D. Socek and V. Villanyi. "Multi-authority attribute based encryption with honest-but-curious central authority." IACR Cryptology ePrint Archive, 2009.

[9] M. Chase. “Multi-authority attribute-based encryption.” The Fourth Theory of Cryptography Conference, 2007.

[10] L. Cheung and C. Newport. “Provably secure ciphertext policy abe.” In ACM conference on Computer and Communications Security (ACM CCS), 2007.

BIOGRAPHIES

Neelam Choubey is an M.Tech Scholar & currently researching on SECURITY, ISSUES AND ALGORITHM AND THEIR PERFORMANCE ANALYSIS.