A Data Security System Design for Hybrid (Cloud & Volunteer) Global Computing

Emrah Dönmez, and Akif Kutlu

***Abstract*—In this study; we aimed to develop a data security infrastructure (DSI) for a hybrid global computing system which consists of cloud and volunteer computing. This performed work has put forth potential capacity of a global computing system which is also known as network computing based method, in terms of data security. Each computer performed computing operations on network has named as "volunteer contractor". The entire computing network is named as "volunteer cloud". We obtained data security analysis on volunteer contractors via designed framework. These analyses have been examined as response time, performance loss and delay time. While global computing system's operating power is 13488 GFLOPS without DSI, it has been discovered that it loss about average 4.67% performance with operating DSI.**

***Index Terms*—Cloud computing, Data security, Global computing, Volunteer computing.**

I. Introduction

GLOBAL computing is a computing technique that provides operating of process suitable to distributed computing by utilizing computing power of computers located on the internet as a distributed or server farms manner. As computing process can be performed on one or more server in computing environment known as cloud computing, on the other hand, it can be performed on distributed computers by allocating workloads in different or similar proportions in computing environment known as volunteer computing.

Data security ensured on computing network is a quite significant element in aspect of computations performed affect total result. Especially, this situation is much more salient in mathematical models implemented with sensitive data. Thus, each computed function or other different process can be at a level where whole computation processes are affected.

In this study, since the effects of security is major concern, during the execution of computation operations such as processing of data-intensive applications in hybrid computing environment, emerging effects of the data security to the potential computing power are examined.

Manuscript received March 01, 2013.

Emrah Dönmez, Computer Engineering Department & Graduate School of Science, Engineering and Technology at İstanbul Technical University, Maslak, İstanbul, 34467 Turkey (corresponding author to provide phone: +90-542-309-9325; fax: 212-285-6169; e-mail: donmezemr@.itu.edu.tr).

Akif Kutlu, Computer Engineering Department at Süleyman Demirel University, Çünür/Central, Isparta, 32260 Turkey (e-mail: akutlu@hotmail.com).

II. Related Works

Train et al. [4] made a study upon challenges in cloud computing and security solutions. Santos et al. [6] indicated required approaches for reliable cloud computing. Chonka et al. [8] performed a study upon developed attacks against cloud architectures and counter measures. Lombardi at al. [9] implemented studies on security virtualization processes in cloud computing systems.

SETI@home [1] project is a significant implementation in terms of revealing potential power of a volunteer computing project. Bayanihan [3] is a volunteer computing project implemented by using JAVA programming language. It has allowed users to participate volunteer computing network via a web browser.

This study is the first study used volunteer and cloud computing systems as a hybrid computing network and examining changes in a global computing mechanism in terms of data security.

III. Computing Infrastructure

Volunteer Cloud Computing: It is a distributed computing network which can be participated by users to contract computation processes. At the same time, it can be used to take only computation results from servers (contractors) by using user computers without contracting any computation process.

The first definition in above paragraph refers to volunteer computing, and the second definition refers to cloud computing, by using advantages of both computing infrastructure, a flexible computing model has been obtained.

A. Volunteer Cloud Model

Structure of computation network working with respect to volunteer computing fundamentals, is demonstrated in figure 3. In this figure, contractor computers consist of singular volunteer hosts and server farms including multiple numbers of computers.

Server farms connect to computation environment through proxy host. This situation reveals apparent distinction of these host communities from singular volunteer contractors. Hosts which employ only computation processes without taking any workload on computing network are named as computation clients. The structure that consists of all contractor hosts constitutes global computing itself.

IV. Computing System Resources

The performance and major QoS (Quality of Service) requirements of computing cloud has been measured according to hardware resources via designed application and Dhrystone synthetic benchmark micro-software by operating them at different time intervals.

A. Data Processing Power

68% of the total participant hosts that are located as volunteer contractors and server farms have constituted the multicore single processor computers in the volunteer cloud computation environment. 27% of the total participant hosts, located on the computing network, has actualized participation as single-core single processor computers. A method resembling to the one used in [12] study has been used to compute data processing power as following.

$$C_P = H_{eff} * N_{eff} * C_{back} * H_{shr} * C_{flops} * C_{life} * C_{ncpu} \quad (1)$$

In this formula, C_p stands for computing power, H_{eff} hardware resources efficiency, N_{eff}; average performance of network efficiency, C_{back}; average exhausted resources by back-up unit, H_{shr}; average shared hardware resources, C_{flops}; average floating point operations per CPU, C_{life}; average life time of contractors and C_{ncpu}; average number of CPU per contractor host.

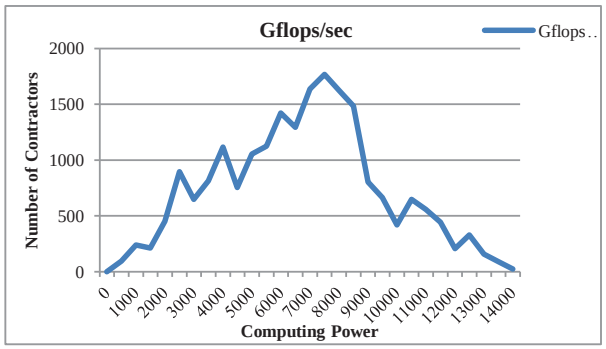

Fig. 1. Floating point operations power (Number of contractors-Gflops/sec).

Total CPU performance values have been obtained with data taken from global computing network periodically. Results make possible observations to be interpreted CPU performance as number of contractor host against floating point operations, figure 1. Given values belong to average performance values in total execution time.

Average processing power per host in GFLOPS for each CPU type of total 1762 pcs hosts demonstrating participation to the cloud have been compared in table 1. Number of CPU core situation has been given for only hosts which have Intel or AMD architecture. Total processing power has been specified approximately 13488 GFOLPS.

At the same time, 63% of contractor hosts have consisted of two processor node and 5% of contractor hosts have consisted of three or more processor nodes.

TABLE I
CPU Types

CPU Type	Number of hosts	GFLOPS per host	Total GFLOPS
Intel	1137	8.504	9668.5
-Multi-core	*853*	*9.885*	*8432*
-Single-core + HT	*284*	*4.354*	*1236.5*
AMD	532	6.647	3536.2
-Multi-core	*351*	*8.079*	*2835.7*
- Single-core	*181*	*3.870*	*700.5*
Power PC	53	3.212	170.2
Others	40	2.837	113.5
TOTAL	1762	7.656	13488.4

B. Network Bandwidth

Average network communication speed has been measured as 352 Kbps in tests actualized by taking into account whole computation cloud. This speed has been measured at higher values than average in some contractors; on the other hand, it has been measured at lower values than average because of their locations. File download speeds in network against number of contractors have been demonstrated in figure 2.

Average network speed rates have been identified between 0 and 32 Mbps in communication that occurs between contractors, clients and contractor-clients. Though the increase in number of contractor hosts, it has been identified that reflection of increase in computing power to the computation network can be possible with increase in bandwidth in parallel manner. It can be said that bandwidth is a restrictive factor by looking this determination in computation power.

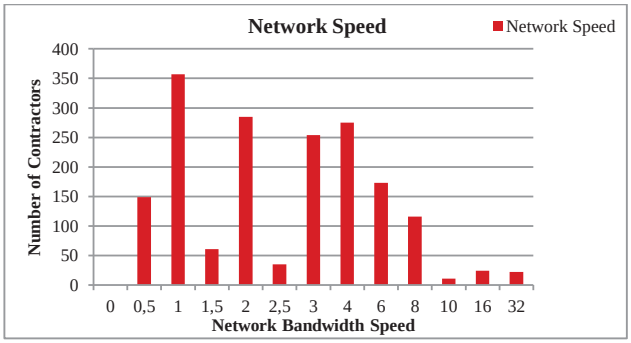

Fig. 2. File download speed distribution in network graph

V. Environmental Design And Findings

A. Dataset

Data used through computation processes have been sent or taken as encrypted on client-server network communication line with starting-up DSI. To be able to synthesize effect of the used data better, it is aimed to obtain a result that is closer to real-world by giving place to different data types. Data have been chosen arbitrarily and any proportion has been not overseen between data types which constitute total amount. It has been minded that data size values are between 1KB-1GB.

Security is a significant element in a computation network designed with respect to global computing structure, since

results obtained from data computation of each contractor host, effects total computation result. Consumption of system resources is desired at a minimum cost level while security is provided at the same time. An optimized data security reduces cost in computation network comparing to a non-optimized data security. Therefore, different security algorithms and designs should be tried by choosing different data types.

Let computation power is expressed with CP (the computation of CP is given section 3) in implemented hybrid global computing cloud and contractors which will operate threaded data are expressed with c1, c2, …, cn. Let computation power of each contractor is denoted with CP_{c1}, CP_{c2}, …, CP_{cn}. Passing time when making only computations without making any encryption, is denoted for each contractor with t_1, t_2, ..., t_n. Let periods passing to encrypt computation data for each contractor while RC6 is using are denoted as t_{r1}, t_{r2}, ..., t_{rn}, while AES is using are denoted as t_{a1}, t_{a2}, ..., t_{an} and while Blowfish using are denoted as t_{b1}, t_{b2}, ..., t_{bn}. In that case, the emerged computing power with actuating DSI on computation cloud;

For RC6;

$$CP_R = CP_{c1}\frac{t_1}{t_{r1}} * CP_{c2}\frac{t_2}{t_{r2}} * \cdots * CP_{cn}\frac{t_n}{t_{rn}} \quad (2)$$

For AES;

$$CP_A = CP_{c1}\frac{t_1}{t_{a1}} * CP_{c2}\frac{t_2}{t_{a2}} * \cdots * CP_{cn}\frac{t_n}{t_{an}} \quad (3)$$

For Blowfish;

$$CP_B = CP_{c1}\frac{t_1}{t_{b1}} * CP_{c2}\frac{t_2}{t_{b2}} * \cdots * CP_{cn}\frac{t_n}{t_{bn}} \quad (4)$$

can be calculated by using these formulas. Average computation power while DSI is used with encryption,

For CP_A;

$$CP_A = \frac{CP_R + CP_A + CP_B}{3} \quad (5)$$

can be calculated with above formula.

The components of the designed hybrid global computation network are demonstrated in figure 3. Workloads actualized in cloud, have been shared between server farms named as sub-cloud and volunteer contractors. The whole network composed of sub-cloud and volunteer contractors named as main hybrid cloud. The computers which stayed out of the main cloud can connect to the computation network to make only calculation together to be able to participating to the cloud.

The management of intercommunication between sub-cloud and volunteer contractors in main cloud and between clients and main cloud in whole network are implemented by main server named Central Computation Management Unit (CCMU). In addition, sub-clouds access to the CCMU located in the main cloud through proxy hosts.

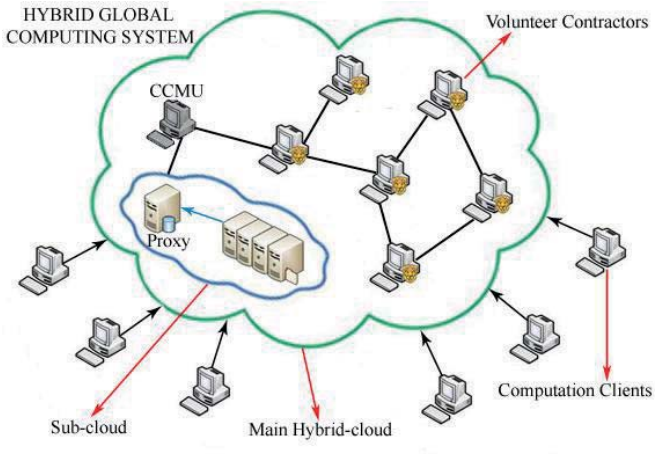

Figure 3. Simplified details of computation environment.

The general name of the process including data encryption methods that are used to prevent accessing, reading and writing the data by other environments, except environments that already use the related data when data security is needed, are called cryptography.

Data Encryption Algorithms

RC6: It is a symmetric switching based encryption technique. It is worked as block based, block size is chosen as 128 bit generally. Generally, suitable to work with 128, 192 and 256 bit switch size. It provides fast and strong encryption.

AES: Advanced Encryption Standard is optimal for 128 – 192 – 256 bit switching sizes. Generally, operates on 128 bit blocks.

Blowfish: It is a symmetric encryption technique operated as block based. Switches between 32 bit and 448 bit are suitable to this encryption technique. Suitable to operate on 64 bit blocks or can be modified to operate on larger blocks.

The comparisons pointing to the speed of algorithms implemented for multi file group (.txt, .jpeg, .png, .avi, .wmv, .mp3, .pdf etc.) about average of three months and occurred changes in performance of global computation cloud in encryption processes are located in the table 2.

In this test, 256 bit switches have been used for all encryption algorithms. While 128 bit blocks have being used for RC6 and AES, 64 bit blocks have being used for Blowfish. Let t denotes the passing time for the calculations made without DSI, t_g denotes the passing time for the same calculations made by using DSI, and t_s denotes encryption time generated by algorithms in system;

$$t_s = t - t_g \quad (6)$$

TABLE II
COMPARISON OF ENCRYPTION ALGORITHMS

Encryption Type	Encryption Time (sec)	Computation Power (GFLOPS)
Blowfish/CTR	0.0064	13263
RC6	0.0112	13125
AES/ECB	0.0081	13087

The time periods identified above, have been obtained from performance report created by using integrated performance measurement tool in ide where the middleware software executed on CCMU is programmed.

Distinct file group has been distributed to the whole computation cloud through CCMU in order to pre-test the available network throughout. Then, each contractor taken these files has sent the data (by assuming that data is processed and ready to sending) to CCMU with encryption modules integrated to the middleware software. The hardware resources of CCMU have been given the following table 3.

TABLE III
CCMU PROPERTIES

	Type	Model	Speed	Other
Mainboard	Intel Ser.	S2600GL	X2 Proc.	I/O Exp.
Processor	Xeon	E5-2643	3.3 GHz	10Mb Ch
Memory	Kingston	HyperX	1600Mhz	64GB
Hard disk	WD SSD	64S-7150	3Gb	8x64GB
GPU	Nvidia	Q-5000	120Gb/s	GDDR5

SSD hard disks have been arranged as x2 RAID5 (2 pcs x 4 unit storage fields) scheme in specified manager workstation (CCMU). Memories have been in the format of x8 8GB. 8 distinct threads can be executed on 4 discrete cores. There are 352 CUDA cores on GPGPU processor and it has 320 bit memory interface.

While network communication is provided through the Internet services, DSI is optimized for only selected data and each message packet including these selected data are subjected to encryption process. This feature has been integrated to the middleware software against the occurrence of the data operated are partially consist of sensitive data in case. User can prevent redundant performance loss that actualized by other general files by encrypting only desired files (.dll, class etc.) in computation environment.

B. Contractor Host Security

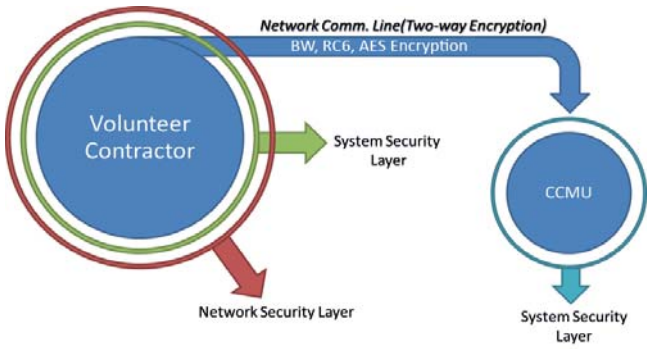

Figure 4. Volunteer contractor security diagram in designed global cloud

Two-way encryption has been implemented in data transfer processes occurred on network communication line between volunteer contractors and CCMU on computation network as shown in figure 4. Three different encryption algorithms; RC6, AES and Blowfish known as prevalent, have been used in two-way encryption processes. Workload occurred by each of them in computation cloud, has been calculated by taking into account parameters of performance criterions (response time, encryption duration and latency duration).

Data security in volunteer contractors has been ensured with a double layer structure designed with respect to a new approach. These layers are system security layer and network security layer respectively.

System security layer: Security modules operating in this layer not only responsible for encryption of data but also responsible for backup to the computer. The general aim is, providing limited accessing authority (such as only reading) or totally preventing accessing to these data from outside by providing data security for users setting calculations with special data in volunteer cloud.

Network security layer: Instead of sending data directly and vulnerably during communication, they have been sent to the CCMU by encrypting with cryptographic encryption modules in this second layer.

C. Server Farms Security

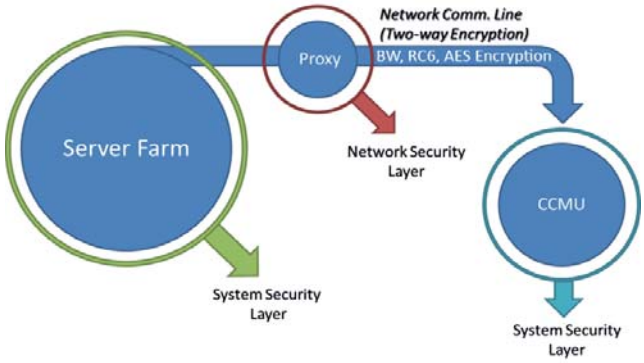

Figure 5. Server farm security diagram in designed global cloud

There is data security structure which is similar to the data security structure of volunteer contractors with a little difference in server farms that are another significant part of computer community in network. The security structure provided for server farms located in computation network has been demonstrated in figure 5. Similarly, two-way encryption structure has been implemented on network communication line. Unlike the security structure of contractor computers, security in server farms has been actualized with operating the double layer structure separately from each of these layer. System security layer has been operated at contractor computers located in server farms. Network security layer has been operated at proxy computer which is the gate of the internet for server farm.

Acquiring performance gain lies at the basic of separately operating security layers from each other. Only the system security layer that is the first layer of security modules has been worked in contractor computers generated server farm. As a result, it has been provided that contractor computers which are already deal with computation processes; have not to enter under the additional workloads. Since, network security layer which is second layer of security has been operated on proxy computer. Providing control of the single flow point of the network is more cleverly method than providing control of the network communication lines on every computer separately.

D. Computation Clients Security

These hosts have only client role. They send requests by entering their own data to make requested computation operations and then take results of these computations as response from network where contractors serve at the end of the period that it was carried out. While defined operations

are executed, the DSI controls all over the communication lines and local files to protect and back-up raw or non-raw data through operations as set-up. Security of network communication lines is ensured as a precaution of data loss in this request-response loop as seen in figure 6. Clients have not any effect on data security in performed computation loop from sending data to the global computation cloud. This operating structure resembles to the classic cloud computing structure in terms of its operating mechanism.

Client-side security is on the carpet only while the data which will be calculated is entered to the computation middleware. Since, security of client data wanted to be processed is ensured by DSI after the related data is entered computation environment via middleware. Ultimately, accurate results can be expected from computation processes by transferring these data to the contractors correctly.

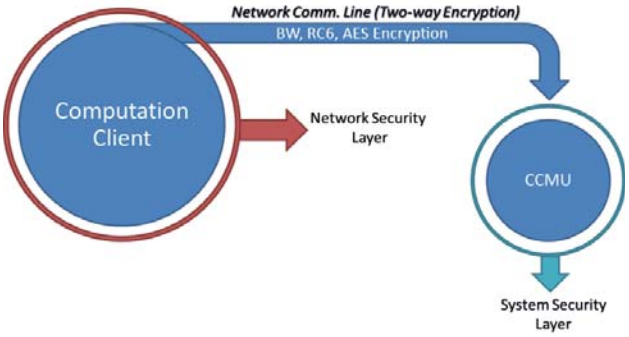

Figure 6. Computation client security diagram in designed global cloud

After the client host entered its own data to the form with desktop application interface, the data are demonstrated to the client user one more time to take approval of user. Before the data transfer processes are performed, the data that were entered at client-side are subjected to the encryption process completely by starting-up of the cryptographic security algorithms as soon as client gives approval for verification process. After encryption processes have done, the data is ready to be sent through DSI.

E. Security Gains

DSI has been created with a triple layered security protocol with regard to other developed or being developed security unit of computation environments. These layers are network security layer, system security layer and client security layer respectively.

Data have been transmitted on both CCMU-Client and CCMU-Contractor communication line by encrypting related data in the first layer defined as network security layer. The data reached to the hybrid computing environment have been protected through system security layer defined as second layer during computations.

The security of data entered to the computation environment from client is ensured in client security layer that is third and last layer. Each data has been subjected to the encryption process through security protocols designed with encryption algorithms which are generated by middleware software.

Performance test has been implemented with three different encryption algorithms in design of security protocols. Analyses have been made on the performance of designed computation cloud from the strongest one to the fastest one in terms of security. The data showing latency time of RC6, AES and Blowfish encryption algorithms against gradual reduction in power of volunteer-cloud computation environment are exhibited in figure 7. The least latency time occurred with Blowfish encryption algorithm as it can be understood from figure. The most latency time occurred with AES. The main reason of faster performing of Blowfish than other algorithms is its block size and *f* function. The other two algorithm; AES and RC6 operates as block-based. 256 bit key (cipher) size is chosen for implementation of general tests.

While computing power is about 13350 GFLOPS on volunteer computation cloud and speed of data exchange (or bandwidth) is about 634.7 Mbps (79.34 MB per second) on network communication line of CCMU, the average latency time of Blowfish algorithm has been actualized approximately 0.1 s (0.098 s), the average latency time of RC6 algorithm has been actualized approximately 0.19 s and lastly, the average latency time of AES algorithm has been actualized approximately 0.21 s according to output of middleware software. This latency is the period occurring only during the communication on between network and CCMU, namely the latencies occurring on the contractors don't fall under to this period. The main reason of lower latency occurred by Blowfish algorithm is that it use smaller block size (64 bit) than others block size (128 – 256 bit), instead of stream it operates as block-based, and accelerated and simple structure of algorithm that is distinctive to itself can be indicated.

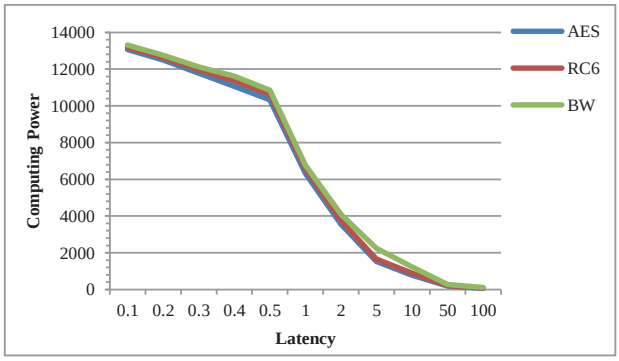

Figure 7. Computing power vs. latency for encryption algorithms

Performance gain is focused factor thus data security in each unit of computation cloud has been handled with distinct principles. Aim approach in here, provide an optimized security with flexibility. In other words; by setting forth from these principles, it is said that the main reason of different design of security in computation units is minimum performance loss while ensuring maximum security.

Both general performance changing and memory performance changing occurred throughout computation cloud against increasing size of the key used for encryption algorithms are illustrated for each algorithm in figure 8. Decreasing is actualized in computation performance (processor, memory, disk unit etc.) while size of the switching increases as it can be understood from figures. Especially starting with use of 256 bit and above keys, decreasing in performance emerges as more significantly. While processor performance is being evaluated in terms of Gflops (floating-point processor power), read – write time and memory frequency is taken into consideration for

memory. During the computations, computing power is observed at level of 13382 Gflops as average while 32 bit switching has been applied. Computation power drops back to level of 12565 Gflops with a loss of 7.86% by 32-fold increasing in the size of switching from 32 bit to 1024 bit. Increasing of switching size at this scale decreases the memory performance from 96.5% to 80.2% with a loss of 16.3%.

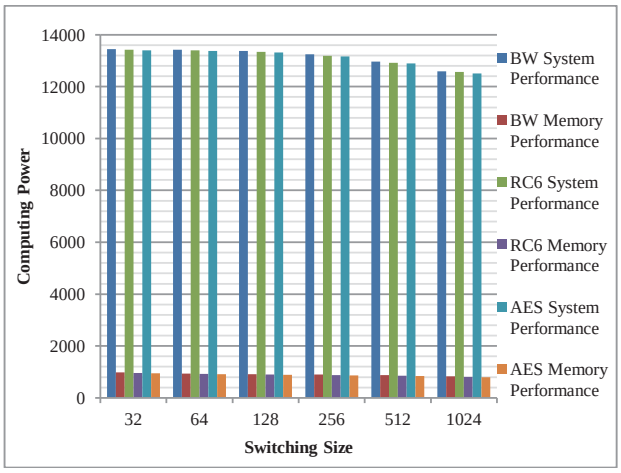

Figure 8. System and memory performance while encryption is being used.

Similarly, effect of encryption block size which is another factor of performance changing in volunteer cloud are illustrated for each encryption algorithm in figure 9. Noticeable declines have been observed when size of block increases. Especially, this decreasing can be observable from 64 bit blocks more clearly. While 32 bit blocks have being used for data during computations, computation power have been about 13389 Gflops. Computation power drops back to level of 12865 Gflops with a loss of 4.62% by 8-fold increasing in the size of switching from 32 bit to 256 bit. Similarly, memory performance is also in a decreasing proclivity. Since, increasing of block size at this scale decreases the memory performance from 96.5% to 74.4% with a loss of 22.1%, approximately. It can be said that block size effects the memory performance more than key size.

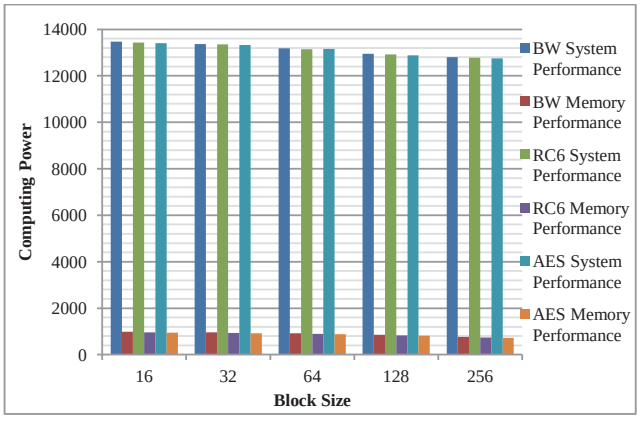

Figure 9. System and memory performance while encryption is being used.

VI. Analyses and Experimental Results

The most important reason of incorporating the data security infrastructure to the global computing cloud is that volunteer contractors and clients are not trustable because of anonym communication is allowed to the computation network. Therefore, security in units (contractor, server farm and client) and back-up modules are used to reduce the worse effect of the malicious and defective hosts to the computation environment performing as volunteer-based. Each task (workload) has been operated on three different contractors with back-up module. If results of these tasks run in with application-defined tolerance values, these results are accepted. Otherwise, a second instance is executed and process continues in this way.

There will be occurred much more data traffic in data secured (means defined encryption algorithms and security modules are worked) volunteer-cloud computing environment according to the pure unsecured computing environment. This situation can cause saturation in network connection of a great number of contractors. If these connections are saturated, computer network connections (shared etc.) opened to the outside can become incapable of working.

Three different encryption techniques known commonly have been used on data security layer designed for volunteer cloud (Data properties have been given in section 5.1). Performance situations are identified when data security is provided or not provided in computation network with these encryption techniques (Table 4). Outputs have been examined as data encryption time, performance loss, and delay time. Average results have been obtained through tests made during approximate time of the entity of computation environment. Network saturation is actualized about average 436,6 Mbps in daytime and 271,3 Mbps in night in tests (daytime, with Turkey time: 08:00 – 17:00, night: 17:00 – 08:00). Saturation is actualized about 43.7% in daytime and 27.1% in night as percentage, if 1000 Mbps data transfer capacity of available CCMU network card is considered. These proportions are found as average values on computation network. Normally, network communication has occurred in a fluctuating course. Encryption time for 1MB granular data have been identified as average 0,0015 sec with AES algorithm, average 0,0012 sec with RC6 algorithm, and average 0,0010 sec with Blowfish in computation network. Performance losses have been identified as average 6,077% with RC6 algorithm, average 4,148% with AES algorithm, and lastly average 3,775% with Blowfish algorithm for particle data (sound, video, text, picture etc.) in computation network. While Blowfish algorithm was being used, the fastest response time has been observed as delay time. Since the least delay time has been identified as average 0,0015 sec with Blowfish. Delay time has been identified as average 0,0018 sec with RC6 and lastly this delay time has been identified as 0,0022 sec with AES which has the latest response time with this value. Computation powers occurred in volunteer-cloud for each encryption algorithm, have been found as in the following table.

TABLE IV
ENCRYPTION TIME OF ALGORITHMS

Encryption type	Average encryption time (sec)	Comparing computing power (GFLOPS)			Delay Time (sec)
		Normal computing power	Encrypted computing power	Difference (%)	
Blow./CT	0.0010	13488	12964	3.775	0.0015
RC6	0.0012	13488	12919	4.148	0.0018
AES/ECB	0.0015	13488	12668	6.077	0.0022

VII. CONCLUSION AND FUTURE WORKS

Computations made as secure as possible and getting results in a fast manner (local + network parallelism) reveal the power of volunteer-cloud hybrid design. The main focusing point is utilizing unused system resources to implement available computations. In this way, unused resources losses are prevented thus cost of computations will be able to be decreased. On the other hand, security mechanisms of computation units are one of the most significant topics in volunteer-cloud computation network. Performance loss has been observed while data security is ensured in a network holding high capacity computing power and employing DSI.

In the future, all user interactive applications will be able to be developed as suitable to the global computing, cloud computing, or hybrid computing systems with the development of applications and the arrival of high-speed network bandwidth through new communication technologies and different techniques. The most important factor will be network bandwidth in development of these kinds of computing technologies. Since when such systems are switched with available ones the reachable speed in reciprocal communication lines will be a determining factor as well as the data processing speed in network elements. Data processed or non-processed may affect the total computation result if these data are changed by external interventions. Thus, security in these communication lines and local environments emerges as an area which should be studied as distinctly in terms of effects on computing performance.

ACKNOWLEDGMENT

We are grateful to volunteer people who allow middleware software to perform tests in their computers, firstly**.** We thank especially cloud service providers allowing integration of volunteer hosts to their platforms. We especially exhibit our thanks to Computer Science Department laboratory at SDU Technology Faculty and CS Department @ITU.

REFERENCES

[1] D.P. Anderson, J. Cobb, E. Korpela, M. Lebofsky, D. Werthimer, "SETI@home: An Experiment in Public-Resource Computing". *Communications of the ACM,45(11)*, Nov. 2002, pp. 56-61.

[2] D.P. Anderson. "BOINC: A System for Public-Resource Computing and Storage". *5th IEEE/ACM International Workshop on Grid Computing*, Pittsburgh, PA, Nov. 8 2004, pp. 365-372.

[3] L.F.G. Sarmenta, "Bayanihan: Web-Based Volunteer Computing Using Java". *Lecture Notes in Computer Science 1368, Springer-Verlag*, 1998. pp. 444-461.

[4] A. Traian, "Cloud Computing Challenges and Related Security Issues". *A project report written under the guidance of Prof. Raj Jain*, 22(6), 2009, pp. 1-10. Available: http://www.cse.wustl.edu/~jain/cse571-09/ftp/cloud/index.html

[5] B. Reingold, R. Mrazik, "Cloud computing: the intersection of massive scalability, data security and privacy". *Cyberspace Law*, 14(5), 2009, pp. 1-5.

[6] N. Santos, K. P. Gummadi, R. Rodrigues, "Towards Trusted Cloud Computing". *MPI-SWS*, 11(6), 2009, pp. 1-5.

[7] Z. Dimitrios, L. Dimitrios, "Addressing cloud computing security issues". *Future Generation Computer Systems (Science Direct)*, 10.1016, 2010, pp. 1-10.

[8] A. Chonka, Y. Xiang, W. Zhou, A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks". *Journal of Network and Computer Applications (Science Direct)*, 09-06(004), 2009, pp. 1-11.

[9] F. Lombardi, R. Di Pietro, "Secure virtualization for cloud computing". Journal of Network and Computer Applications (Science Direct), 10-06(008), 2010, pp. 1-10.

[10] R. P. Weicker, "Dhrystone: A Synthetic Systems Programming Benchmark". *Communications of the ACM 27 (10)*, Oct. 1984, pp. 1013-1030.

[11] D. P. Anderson, G. Fedak, "The Computional and Storage Potential of Volunteer Computing". *Seti@HOME, U.C. Berkeley*, Space Science Laboratory, 24(10), 2008, pp. 1-8.

[12] L.F.G. Sarmenta, S. Hirano, S. A. Ward, "Towards Bayanihan: Building an Extensible Framework for Volunteer Computing Using Java". *in Proc. of ACM 1998 Workshop on Java for High-Performance Network Computing, Feb./Mar. 1998.* Also published in Concurrency: Practice and Experience, 1998, pp. 10(11-13).

Emrah Dönmez is a Ph.D. student in the Computer Engineering Department at the İstanbul Technical University. His research areas are: security of cloud computing, data mining with HPC systems, performance optimization in HPC systems, GPGPU acceleration and communication optimization, distributed operating systems, global, grid, volunteer and hybrid computing; problems & solutions. He graduated from the Süleyman Demirel University in 2009 with a B.Sc. in computer science under supervising T. Aydoğan and then he graduated from the Süleyman Demirel University in 2011 with M.Sc. in computer science under supervising of A. Kutlu. He is a student member of IEEE.

Akif Kutlu is a professor in the Computer Engineering Department at the Süleyman Demirel University. His research areas are: microcontrollers, computer networks, microprocessors, industrial control, industrial networks, CAN (Control Area Network), embedded systems, firmware, and engineering education. He graduated from the Sussex University, England in 1998 with a Ph.D. in computer science. His Ph.D. thesis topic is industrial network protocols. He has already published a number of qualified publications as national and international. He is a member of IEEE and IEEE Communication Society. He gives lectures in computer engineering department at SDU nowadays.