An Efficient Security Model in Cloud Computing based on Soft computing Techniques

Vijay.G.R
Phd Scholar, JNTUA, Anatapur, A.P., India

A. Rama Mohan Reddy
Professor, Department of CSE, SVU College of Engineering, Tirupati, A.P., India

ABSTRACT
In recent years, Cloud computing is one of the most attractive technological research area because of its flexibility as well as cost efficiency. Generally in a cloud the data are transferred among the client and the server. While the transferring of the data takes place, security becomes the major concern. Efficient security system must be employed in a cloud inorder to make the computing environment secure from unauthenticated users. Due to this reason, cloud securities have emerged as the recent discussion in the IT sector. Various techniques have been formulated inorder to make the cloud computing environment secure. In this paper, we presented an efficient security model in cloud computing environment with the help of Soft Computing Techniques. Here, a strong security in cloud computing is managed with the help of reputation management system to ensure the data security. Also maintaining the transaction table that contains the information related to the previous transactions like the previous transaction id of the cloud node involved, timestamp, public keys of the cloud involved, trust evaluation etc, can be very helpful to identify the relevant cloud nodes suitable of data transmission. Soft Computing Techniques utilizes fuzzy logic, neural network or genetic algorithm for processing. In the proposed method, we utilized genetic algorithm as the computing technique to identify the suitable nodes for transmission.

Keywords
Cloud Computing, Security Issues

1. INTRODUCTION
As more facets of work and personal life move online and the Internet becomes a platform for virtual human society, a new paradigm of large-scale distributed computing has emerged. Web-based companies, such as Google and Amazon, have built web infrastructure to deal with the internet-scale data storage and computation. If we consider such infrastructure as a "virtual computer", it demonstrates a possibility of new computing model, i.e., centralize the data and computation on the "super computer" with unprecedented storage and computing capability, which can be viewed as a simplest form of cloud computing [1]. Cloud Computing is a new term for a long-held dream of computing as a utility, which has recently emerged as a commercial reality [2]. Cloud computing is a model for enabling on-demand network access in order to share computing resources such as network bandwidth, storage, applications, etc , that is able to be rapidly scalable with minimal service provider management [3]. Cloud providers currently enjoy a profound opportunity in the marketplace.

The providers must ensure that they get the security aspects right, for they are the ones who will shoulder the responsibility if things go wrong. The cloud offers several benefits like fast deployment, pay-for-use, lower costs, scalability, rapid provisioning, rapid elasticity, ubiquitous network access, greater resiliency, hypervisor protection against network attacks, low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services. While the cloud offers these advantages, until some of the risks are better understood, many of the major players will be tempted to hold back [4]. Though cloud computing is targeted to provide better utilization of resources using virtualization techniques and to take up much of the work load from the client, it is fraught with security risks [5]. Because of the critical nature of the applications, it is important that clouds be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed.

This is because if one wants to exploit the benefits of using cloud computing, one must also utilize the resource allocation and scheduling provided by clouds. Therefore, we need to safeguard the data in the midst of untrusted processes [6]. Cloud computing services benefit from economies of scale achieved through versatile use of resources, specialization, and other efficiencies. However, it is an emerging form of distributed computing still in its infancy. The term itself is often used today with a range of meanings and interpretations [7]. While reducing cost is a primary motivation for moving towards a cloud provider, reducing responsibility for security or privacy should not be. Ultimately, the organization is accountable for the overall state of the outsourced service. Monitoring and addressing security and privacy issues remain in the purview of the organization, just as other important issues, such as performance, availability, and recovery [8]. The Cloud Computing model has three service delivery models and main three deployment models [9] models are: (1) Private cloud: a cloud platform is dedicated for specific organization, (2) Public cloud available to public users to register and use the available infrastructure, and (3) Hybrid cloud: a private cloud that can extend to use resources in public clouds. Public cloud most vulnerable deployment model because for public users to host their services who may be malicious users.

In providing a secure Cloud computing solution, a major decision is to decide on the type of cloud to be implemented. Currently there are three types of cloud deployment models offered, namely, a public, private and hybrid cloud.

- **Public Cloud**: A public cloud is a model which allows users' access to the cloud via interfaces using mainstream web browsers. It's typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. This helps cloud clients to better match their IT expenditure at an operational level by decreasing its capital expenditure on IT infrastructure [10].
- **Private Cloud**: A private cloud is set up within an organization's internal enterprise datacenter. It is easier to align with security, compliance, and

regulatory requirements, and provides more enterprise control over deployment and use [11].

- **Hybrid Cloud**: A hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [12]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Clouds provide more secure control of the data and applications and allows various parties to access information over the Internet [11].

Also, there are 5 major technical characteristics of cloud computing: (i) large scale computing resources (ii) high scalability & elastic (iii)shared resource pool (virtualized and physical resource) (iv) dynamic resource scheduling and (v) general purpose. Specifically, cloud computing provides computing resources as on demand services that are hosted remotely, accessed over the Internet, and generally billed on a per-use basis.

For cloud computing, the data are stored in "data center", the security and confidentiality of user data is even more important. The so-called integrity of data in any state is not subject to the need to guarantee unauthorized deletion, modification or damage. The availability of data means that users can have the expectations of the use of data by the use of capacity [13]. To ensure data confidentiality, integrity, and availability (CIA), the storage provider must offer capabilities that, at a minimum, include

- Tested encryption schema to ensure that the shared storage environment safeguards all data.
- Stringent access controls to prevent unauthorized access to the data.
- Scheduled data backup and safe storage of the backup media [14].

Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing [15]. In cloud computing, security applies to two layers in the software stack. First, users' workloads have to be run isolated from each other, so that one (malicious) user cannot affect or spy on another user's workload. Second, each user is also concerned with the security of their own workload, especially if it is exposed to the Internet (as in the case of a web service or Internet application) [16].

2. REVIEW OF RECENT RESEARCHES

A numerous researches have been presented in the literature for cloud computing and its security issues. A brief review of some recent researches is presented here.

Cloud computing was a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns were beginning to grow about just how safe an environment it was. Despite of all the hype surrounding the cloud, enterprise customers were still reluctant to deploy their business in the cloud. Security was one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. The advent of an advanced model should not negotiate with the required functionalities and capabilities present in the current model. A new model targeting at improving features of an existing model must not risk or threaten other important features of the current model. The architecture of cloud poses such a threat to the security of the existing technologies when deployed in a cloud environment. Cloud service users need to be vigilant in understanding the risks of data breaches in that new environment. S. Subashini *et al*., [17] proposed a survey of the different security risks that pose a threat to the cloud.

Cloud computing has become one of the most significant information security issues in recent years. That was due to the dramatically emerging applications and required services of cloud computing. However, in order to safely utilize and enjoy the benefit of cloud computing through wired/wireless networking, sufficient assurance of information security such as confidentiality, authentication, non repudiation, and integrity was the most critical factor for adoption. In order to well understand the security of cloud computing, experimental platform based on kernel-based virtual machine has established. Besides, a dynamic intrusion detection system for strengthening the security application of cloud computing was implemented. In their mechanism, numbers of intrusion detectors were dispatched on the whole topology of the networking system through multi-layers and multi-stages deployment. Those information security issues related with the application and service of cloud computing would be experimented and discussed. The experiments included the equipment security of the client side termination, the threats of web site and webpage, the detection and diagnosis and surveillance of intrusion, the access and security of database in the cloud side, the detection of system leakage and the monitor of real-time repairing process, the management of server system, the management of mobile e-commerce processing, and the integrated analysis of associated security information and issues. Chang-Lung Tsai *et al*., [18] proposed a mechanism that was not only focused on find out some solutions, but also focused on develop some feasible information security techniques or products for the application and service of cloud computing.

Cloud computing technology was a new concept of providing dramatically scalable and virtualized resources, bandwidth, software and hardware on demand to consumers. Consumers could typically requests cloud services via a web browser or web service. Using cloud computing, consumers could safe cost of hardware deployment, software licenses and system maintenance. On the other hand, it also has a few security issues. Danish Jamil *et al*., [19] introduced four cloud security problems, which are XML Signature Element Wrapping, Browser Security, Cloud Malware Injection Attack and Flooding Attacks, and also gives the possible countermeasures.

Cloud computing moved away from personal computers and the individual enterprise application server to services provided by the cloud of computers. The emergence of cloud computing has made a tremendous impact on the Information Technology (IT) industry over the past few years. Currently IT industry needs Cloud computing services to provide best opportunities to real world. Cloud computing was in initial stages, with many issues still to be addressed. The objective of that was to explore the different issues of cloud computing and identify important research opportunities in this increasingly important area. V. Krishna Reddy *et al*. [20] presented different design challenges categorized under security challenges, Data Challenges, Performance challenges and other Design Challenges.

Krishna Chaitanya *et al*., [21] provided the basic idea on Cloud Computing. It also deals with the Security Issue mainly faced in the Industry where Cloud Computing is implemented and

necessary steps which could solve these problems to certain extent.

The prominence of the place of cloud computing in future converged networks was incontestable. That was due to the obvious advantages of the cloud as a medium of storage with ubiquity of access platforms and minimal hardware requirements on the user end. Secure delivery of data to and from the cloud is however a serious issue that needs to be addressed. Aderemi A. Atayero *et al.,* [22] presented the security issues affecting cloud computing and proposed the use of homomorphic encryption as a panacea for dealing with these serious security concerns vis-à-vis the access to cloud data.

Cloud computing was a set of IT services that were provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services were delivered by a third party provider who owns the infrastructure. It advantages to mention but a few include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offered an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations were slow in accepting it due to security issues and challenges associated with it. Security was one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company was worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in that new environment. Kuyoro S. O *et al.,* [23] introduced a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.

3. PROPOSED METHODOLOGY

The proposed scheme for security model in cloud computing using soft computing technique comes across with the usage of reputation management system which is a proficient reputation collection scheme from multiple cloud nodes to ensure the data security. For enhancing the security, trust and reputation verification technique is used which is more efficient. The nodes for data transmission are identified with the usage of transaction table that contain the information related to the previous transactions like the previous transaction id of the cloud node involved, timestamp, public keys of the cloud involved, trust evaluation etc. Genetic Algorithm, an efficient soft computing technique is utilized here inorder to identify the suitable nodes for transmission. The proposed method is detailed in the following sections,

3.1. Reputation Management System

Reputation management system, in general, is the strategies made to provide any network or system from negative impacts. The major function of reputation management system is to estimate the quality of the nodes behavior, to differentiate well behaving and misbehaving nodes and its reaction to such nodes. These evaluation, detection and reaction are considered to be the major fact in using reputation management system. The reputation management system has proved to be an effective system which is unfavorable to misbehavior [24]. The system can also target security problems in decentralized and unstructured networks due to internal misbehavior attacks.

In reputation management system two metrics are considered to be the factor for data security,

- Reputation Effectiveness and
- Reputation Efficiency

3.1.1 Reputation Effectiveness

The reputation management effectiveness further consists of various metrics which are explained below,

3.1.1.1 Misbehavior Impact

The misbehavior impact metrics usually measures the influence of the node misbehavior in the network. This measures the negative impact of the misbehavior on the network performance. It is calculated in terms of proportion of packets dropped due to misbehavior. For a given p_d^j, the number of dropped packets by a node j, is given by

$$p_d = \frac{\sum_{j \in T} p_d^j}{\sum_{j \in R} p_d^j} \quad Where \quad \sum_{j \in R} p_d^j \neq 0 \tag{1}$$

3.1.1.2 Behavior Classification

The behavior classification metrics measures the effectiveness of the detection functionality of the reputation management system.

3.1.1.3 Quality of Reaction

This metrics measure the effectiveness of the function of reputation management system in isolating misbehaving nodes.

3.1.2 Reputation Efficiency

The reputation efficiency measures the communication overhead, computation overhead and storage overhead of Reputation management system.

- Communication overhead: This measures the communication overhead employed by the reputation management system. For a number of data packets p_d^j from the source node and p_r^j,the number of packets sent by reputation management system, the overhead is given by,

$$p_{over} = \frac{\sum_{j \in N} p_r^j}{\sum_{j \in N} \left(p_d^j + p_r^j \right)}, \text{ where } \sum_{j \in N} \left(p_d^j + p_r^j \right) \neq 0 \tag{2}$$

- Computation overhead: The computational overhead is defined in a similar way as that of the communication over head with the exception that the amounts of the CPU resources ' μ 'and data packets ' λ ' are considered here.

$$p_{c-over} = \frac{\sum_{j \in N} p_r^j * \mu}{\sum_{j \in N} \left(p_d^j * \lambda + p_r^j * \mu \right)}, \quad where \quad \sum_{j \in N} \left(p_d^j * \lambda + p_r^j * \mu \right) \neq 0 \tag{3}$$

- Storage overhead: In storage overhead, the storage required per reputation management system ' μ_s ' and data packets ' λ_s ' are also considered.

$$p_{st-over} = \frac{\sum_{j \in N} p_r^j * \mu_s}{\sum_{j \in N} \left(p_d^j * \lambda_s + p_r^j * \mu_s \right)}, \text{ where}$$

$$\sum_{j \in N} \left(p_d^j * \lambda_s + p_r^j * \mu_s \right) \neq 0 \quad (4)$$

3.2 Genetic Algorithm

Genetic algorithms are adaptive methods which may be used to solve search and optimization problems. They are based on the genetic processes of biological organisms [25]. According to the principles of natural selection and survival of the fittest; natural populations are evolved in many generations. By simulating this process, genetic algorithms are able to use solutions to real world problems, if they have been suitably encoded [26, 27].

The genetic algorithm usually works as given below,

3.2.1. Selection

In genetic algorithm, a population is created with a group of individuals or chromosomes. The selection process decides which of the chromosomes from the population will be selected for crossover to create new chromosomes. This new chromosome will now included with the population to determine the next selection. The individuals with more fitness value will be selected. The selection is based on the fitness of the individuals.

3.2.2 Crossover

After selecting the individuals the next step is the crossover where two parents are made to mate each other. In crossover there are various types in which two point crossover is more commonly used method. Here the offspring is produced by selecting two crossover point and the genes in between these two points are interchanged from the parents to form new offspring's.

3.2.3 Mutation

After crossover, new set of populations are produced .Inorder to provide individuality to each chromosome, mutation operation is performed where we replace any value with a new value to form a new individual.

3.2.4 Fitness Function

After mutation the fitness of each individual is founded and the individual with high Fitness values are selected as the final solution.

3.3 Genetic Algorithm for the Proposed Method

In our proposed method, the genetic algorithm is used to find out the suitable node for transmission. Here the node is represented as the bit of chromosome. The Fig.1 shows flow diagram of genetic algorithm for our proposed method. Initially generate 'N' number of chromosomes (nodes).Next fitness for each of the individuals are calculated. In our proposed method the fitness value is calculated in relation to the distance between the nodes. The nodes with less distance are selected. Here a Euclidean distance from each node to the next closest nodes is calculated. It is given by the expression,

$$Fitness(F) = \frac{1}{\min} \left(E_d(m,n) \right) \quad (5)$$

Where m and n are the source and the destination nodes respectively.

Once fitness of the nodes is calculated we proceed to next step in the genetic algorithm. Next is the selection process where the two chromosomes for crossover and mutation are selected. This selection is based on the fitness of the chromosome.

More fit the chromosomes are more the chance for selection. There are various methods of selection in genetic algorithm. In our proposed method we use the roulette wheel selection method. The roulette wheel selection is used for selecting potentially useful solutions for recombination.

In roulette wheel selection the chromosome with higher fitness value when compared to others are selected to form the new offspring's.

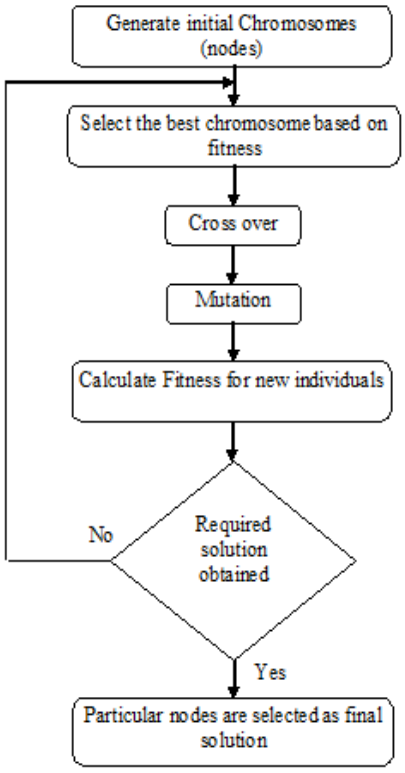

Fig 1. Proposed Genetic Algorithm Flow Diagram.

The probability of selecting the 'k'th node is given by, where N is the total number of nodes, P_k is the probability of the 'k'th node and F_k is the fitness of the 'k'th node.

$$P_k = \frac{F_k}{\sum_{t=1}^{N} F_t} \quad (6)$$

After selecting the solutions crossover and mutation are performed. In the proposed method we utilized two-point crossover method. Two points are selected in the parent chromosomes as R1 and R2 and the genes in between these two points are interchanged to form new offsprings. After the crossover operation, mutation is applied to the newly formed offsprings inorder to make each individual independent of other. After mutation operation finally the fitness value for the newly formed individuals is calculated.

By calculating the fitness value for each individual or node, the values are analyzed and the nodes with higher fitness values are selected as the suitable node for transmission. A transaction table is maintained with previous transaction id, trust evaluation, public keys of the cloud involved inorder to identify the nodes for transmission.

4. RESULTS AND DISCUSSION

The proposed method for security model in cloud computing is implemented in the JAVA platform. The transmission nodes selected by utilizing the genetic algorithm provides better transmission techniques when compared with other algorithms. The result we obtained tends to prove that the proposed method delivers the exact result as required for the data transmission. The transmission time required for transfer of the data through the transmission nodes are given as per the table shown below,

Table 1: Comparison Transmission time using GA and MCT

Number of nodes	Transmission time using GA (sec)	Transmission time using MCT (sec)
10	3	8
30	6	14
50	10	21
70	16	33
100	26	42

As shown in table 1 the transmission time require for data transmission is much reduced when compared to the existing method like MCT. The reduction in the transmission time can further increase the performance of the system by which an efficient and secured transmission of the data is possible. Transmission time is a much important factor in data transmission and has to be provided in a better secured way which performed efficiently by our proposed method of cloud security.

Based on the above table the Comparison graph is plotted as shown below.

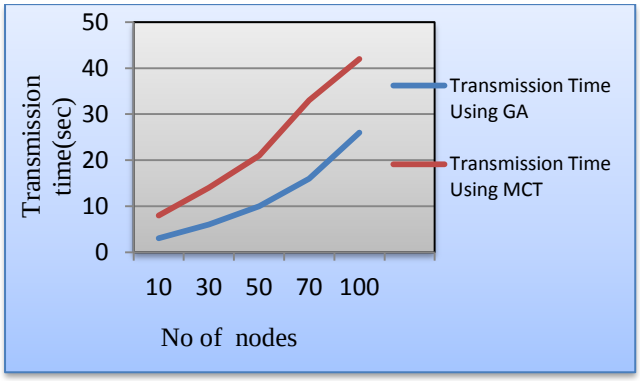

Fig 2. Graphical Representation of Transmission time in GA and MCT

As shown in fig 2, the transmission time for our proposed security system using GA is much reduced when compared with the existing method. The transmission time in cloud computing is considered as one of the major factor and so once when the time is reduced better performance can be obtained which results in providing improved security measures in much reduced time interval. Proper security is required to provide efficient cloud computing and the proposed method with the Genetic algorithm proved to deliver a better security model in cloud computing environment.

5. CONCLUSION

In this paper we have proposed an efficient security model for cloud computing based on soft computing techniques. The security system in cloud computing requires an in-depth analysis because attackers may choose to exploit cloud systems. An attacker may try to operate a clients request during the data transfer from client to the cloud system which makes the attacker to gain unauthorized access to the system. Our proposed method we utilized the reputation management system which proved to be a better mechanism to provide security to the cloud system. The usage of genetic algorithm for the selection of the nodes for the data transmission also proved to be effective method in cloud computing environment.

6. REFERENCES

[1] Bo Peng, Bin Cui and Xiaoming Li, "Implementation Issues of A Cloud Computing Platform", IEEE Computer Society Technical Committee on Data Engineering, pp. 1-8, 2009

[2] Parkhill, D. The Challenge of the Computer Utility. Addison Wesley Educational Publishers Inc., US, 1966.

[3] Kuyoro S. O, Ibikunle.F and Awodele O, "Cloud Computing Security Issues and Challenges" International Journal of Computer Networks (IJCN)", Vol. 3, No. 5, pp. 247-255, December 2011.

[4] Viega J., "Cloud computing and the common man", Computer, pp. 42, No. 8, pp.106–108,2009

[5] Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A, Licciardi A, et al. Security guidance for critical areas of focus incloudcomputing,v2.1.CloudSecurityAlliance, 2009, 25 p.

[6] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisingham, "Security Issues for cloud computing", International Journal of Information Security and Privacy, Vol. 4, No. 2, pp. 39-51, April-June 2010

[7] G. Fowler, B. Worthen, The Internet Industry is on a Cloud – Whatever That May Mean, The Wall Street Journal, March 26, 2009

[8] Wayne A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", Proceedings of the 44th Hawaii International Conference on System Sciences, pp.1-10, Jan 2011

[9] Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2010

[10] A Platform Computing Whitepaper, "Enterprise Cloud Computing: Transforming IT," Platform Computing, pp6, viewed 13 March 2010.

[11] Ramgovind S,Eloff M M,Smith E, "The management of security in Cloud computing," Information Security for South Africa,pp.1-7,2010.

[12] Meiko Jensen J ,org Schwenk,Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," IEEE International Conference on Cloud Computing,pp.109-116,2009.

[13] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan, Tang Chaojing, "Data Security Model for Cloud Computing," Proceedings of the 2009 International Workshop on Information Security and Application, 2009.

[14] Kaufman L M, "Data Security in the World of Cloud Computing, "IEEE Security & Privacy, vol.7, no.4, pp.61-64, 2009.

[15] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham "Security Issues for Cloud Computing," International Journal of Information Security and Privacy, vol.4, no.2, pp.39-51, 2010.

[16] Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales,Daniele Sgandurra, Diego Zamboni, "Cloud Security Is Not (Just) Virtualization Security," Proceeding CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security, pp.97-102,2009.

[17] A. Mell and T. Grance. "The NIST definition of cloud computing".[Online].Available:csrc.nist.gov/groups/SNS/cloudcomputing/ cloud-def-v15.doc, 2009.

[18] S. Subashini and V. Kavitha. (2010) "A Survey on Security issues in Service delivery Models of cloud computing" Journal of Network and Computer Applications (JNCA), Vol. 34, No. 1, Jul, 2010

[19] Chang-Lung Tsai and Uei-Chin Li, "Information Security of Cloud Computing for Enterprises", Advances on Information Sciences and Service Sciences. (AISSS), Vol. 3, No. 1, pp. 132-142, Feb 2011

[20] Danish Jamil, Hassan Zaki, "Security Issues In Cloud Computing And Countermeasures", International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 4, pp. 2672-2676, April 2011

[21] V. Krishna Reddy, B. Thirumala Rao, Dr. L.S.S. Reddy and P. Sai Kiran, "Research Issues in Cloud Computing", Global Journal of Computer Science and Technology (GJCST) Vol.11, No. 11, pp. 59-64,July 2011

[22] Krishna Chaitanya.Y, Bhavani Shankar.Y, Kali Rama Krishna.V and V Srinivasa Rao, "Study of Security Issues in Cloud Computing", International Journal of Computer Science and Technology(IJCST) Vol. 2, No. 3, Sept 2011

[23] Aderemi A. Atayero, Oluwaseyi Feyisetan , "Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", Journal of Emerging Trends in Computing and Information Sciences, (JETCIS). Vol. 2, No. 10, October 2011

[24] Sheikh Mahbub Habib, Sebastian Riesy, Max Muhlhauser ,"Towards a Trust Management System for Cloud Computing", In.proc.of IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[25] Chung Il Sun and Tae Ho Cho ,"Path Selection Method for Reliable Data Transmission in Sensor Networks using GA", International Journal of Computer Science and Network Security, (IJCSNS) Vol.11 No.2, Feb, 2011.

[26] Ehsan Heidari and Ali Movaghar ,"An Efficient Method Based on Genetic Algorithms to Solve Sensor Network Optimization Problem", International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.3, No.1, Mar, 2011.

[27] Aloysius George, B. R. Rajakumar and D. Binu, "Genetic algorithm based airlines booking terminal open/close decision system", In proceedings of the International Conference on Advances in Computing, Communications and Informatics, pages 174-179, 2012.

[28] http://www.wheresmyserver.co.nz/storage/media/faq-files/clouddef-v15.pdf, Accessed April 2010