Algorithm for Document Integrity Testing Pre Upload and Post Download from Cloud Storage

Mohd. Tajammul, Rafat Parveen

Abstract: This era is of business and marketing, those who have no proper equipments, they can also proceed in this field. This is just because of cloud computing. Many organizations are still in ambivalence whether to adopt cloud computing or not. The biggest barrier before them is security of their sensitive data. This research paper is an attempt to encourage such organizations or individuals who are still thinking to adopt this fruitful as well as cheap and best service. In this paper we have proposed an integrity testing algorithm which tests whole documents at character level before uploading to cloud storage and after downloading from cloud storage. The idea of the algorithm resembles to the idea of ‘error detection and correction’. For more clearance of the idea refer future scope.

Index Terms: Integrity, Cloud Computing, Error Detection and Correction, character level testing.

I. INTRODUCTION

Cloud computing is a multifarious mechanism which is in progress of many decades of research and development. Cloud computing in itself is not a single technology rather it is a combination of various technologies. Out of which Internet is considered as backbone of it. Other technologies are distributed computing, parallel computing and virtualization etc. One of the main advantage of this technology is its accessibility at remote location. One can access this service on pay-per-use basis anywhere any time. He or she can access unlimited resources which are available with cloud service provider to satisfy clients’ request to finish their work on time or as per service level agreement.

The main idea of cloud computing was given by Professor John Mc Carthy in 1969. In his words, he said that “If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility. The computer utility could become the basis of a new and important industry” [10-11].

Douglas Parkhill in his book ‘The Challenge of the Computer Utility’ defines the features of cloud computing in 1966. Cloud computing is super-set of Virtual Private Network (VPN) along with network infrastructure that is utilized by telecommunication. The National Institute of Standards and Technology (NIST) defines “a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models” [10-11].

A. Deployment Models of Cloud Computing

• Public Cloud: - This is one of the simplest models of cloud computing. It is publically accessible. If data which we want to store on cloud storage is not more sensitive, we should use public cloud [7].
• Private Cloud: - This cloud model is available for single particular organization or for individual who can keep his or her secure or sensitive data on it. This model is owned by particular individual or by specific organization. The complete capacity of this cloud is availed only by someone who owned it [18].
• Community Cloud: - If some trusted parties or some trusted organizations develop their cloud and the full capacity of this cloud is availed only these known organizations then this type of cloud is called as community cloud [17].
• Hybrid Cloud: - The cloud formed by combining the features of two or more clouds. This is suggested in situation where one type of cloud is unable to fulfill the need of clients. Advantage of forming this cloud is that it supports various types of requirements of customers which are beyond the capabilities of just one cloud [18].

B. Service Models of Cloud Computing

There are three service models of cloud computing.

• Software-as-a-Service: - This is top most service model of cloud computing. In this model software is available to the cloud user who can use it. Maintenance of this software is done totally on provider’s side, client can use but cannot do any fingering in it. There are various companies available in the market providing SaaS. Some of them are as: NetSuite, Microsoft, SalesForce.com, IBM and Oracle [18].
• Platform-as-a-Service: - This model is the considered as middle model in cloud architecture. This model is available for those who want to setup their business without having proper equipment. In this model a
platform is given to the clients or to the users on which they can develop their applications. For example a software engineer wants to setup his software development company but have only laptops without proper platform on which he can develop software. Cloud SaaS is available for such people. Some of the companies which are providing PaaS are as: Microsofts, Azure GAE[7].

- **Infrastructure-as-a-Service:** This model is the lowest model of cloud computing architecture. In this service model an infrastructure is reserved for the client for pay-per-use basis. For example if a organization wants to store its data beyond its boundary, it can go for storage as a service to cloud service provider or if someone wants to perform some computation which is beyond the capabilities of single node, he can go for computation as a service to cloud service provider. In this case both of them will be given service on the basis of SLA (Service Level Agreement) and will be charged pay-per-use basis. Out of famous IaaS providers, some of them are GoGrid, Flexiscale, Joyent, and Rackspace [18].

![Diagram of Service Models of Cloud Computing](image)

**Figure 1.** Service Models of Cloud Computing [7]

C. **Features of Cloud Computing [19-20]**

There are numerous features of cloud computing, some popular are listed here:

- 24X7 on demand service
- Resource pooling
- Broad network access
- Measured service
- Pay per use service
- Rapid elasticity

D. **Issues of Cloud Computing**

The field of cloud computing is very broad, therefore issues and challenges before cloud are uncountable. Some important have been listed here.

- Issue of Resource Scheduling and Management
- Issue of Portability and Interoperability
- Issue of Reliability and Availability
- Issue of Power Consumption
- Issue of Performance
- Issue of Security and Privacy
- Issue of Scalability and Elasticity

Out of above issues, one important issue is security and privacy. This paper has been written from cloud security perspective, therefore we will discuss this issue of security and privacy in little bit deep. Out of numerous security issues we have selected some important which are listed as:

- Issues of Data confidentiality.
- Issues of Web application security.
- Issues of Data breaches.
- Issues of Virtualization vulnerability.
- Issues of Availability.
- Issues of Data access.
- Issues of sign-on process and Identity management.
- Issues of Network security.
- Issues of Data security.
- Issues of Data segregation.
- Issues of Authentication and authorization.
- Issues of Data locality.
- Issues of Backup.
- Issues of Data integrity.

E. **Our Contribution**

As far as the matter of our contribution is concern we have summarized our work in four points. During this research paper, we have come to know, how to design and develop an algorithm on the basis of matrices rather than group. We have proposed an algorithm which will produce a matrix of input file automatically and then data or file may be uploaded on cloud server in plain or in encrypted form by AES (Advanced Encryption Standard) Algorithm. So far up-to our knowledge, there
exist no such type of algorithm which test the integrity of data. This is first attempt to go towards the matrix approach and non linear for integrity testing. Our contribution has been summarized as under:

- **Firstly**, we have designed an algorithm which will generate a matrix pre-uploading and post-downloading data on cloud storage. This matrix will help to prove that the file has not been altered during the journey from our desktop to cloud server and from cloud server to our desktop.

- **Secondly**, we have used AES algorithm for encryption after creating matrix of the given file. This algorithm will increase the security of our data as our data crosses our boundary it required to be kept safe from hackers. Although we can send file in plain form but it is common intelligence to encrypt file as and when it crosses the boundaries.

- **Thirdly**, we have designed a conceptual architecture of the proposed system to make concept easier to be understood. This architecture indicates the flow of information from end user to cloud and from cloud to end user in secret and effective manner.

- **Fourthly**, we have calculated the results for checking the efficiency of our algorithm. In proposed, work we have computed duration of time taken by algorithm for matrix creation and for integrity testing. Moreover we have applied AES and DES for small amount of data for encryption and decryption. For result calculation we have collected data from two sources range from 500KB to 5000KB. Nature of the data with source as and size has been shown in Table 1.

Rest part of this paper is organized as: Sec. 2 discusses literature survey, Sec. 3 discusses motivation and research gap, Sec. 4 discusses proposed algorithm, Sec. 5 shows data collection, Sec. 6 discusses experiments, Sec. 7 shows conclusion and finally Sec. 8 shows future research directions in proposed work.

II. LITERATURE REVIEW

In [3], Hassan Rasheed, proposed infrastructure and data auditing in cloud computing where author has divided security auditing issues into two categories that is data auditing and infrastructure auditing. In [7], Mohd. Tajammul, Rafat Parveen and Mohd. Shahnawaz discussed a no. of security related issues and challenges in cloud computing. In [8], Subhashini and V. Kavitha discussed a survey on security issues on service models of cloud computing where authors discussed 14 security issues on SaaS and some on issues on PaaS some rest on IaaS. A large no. of solutions and tests has also been suggested to overcome these issues. In [10], Manas MN et al. discussed cloud computing issues and methods to overcome. Authors have discussed there isolation on the basis of SaaS, PaaS and IaaS and finally isolation at VM in memory and cache in multitenant environment. In [17], Mohd Tajammul and Rafat Parveen, discussed big ten information security management system standards. In [2], Zuojie et al. proposed a scheme for multitenant environment to search with authorized keyword. Which solves the problem of finding encrypted files on storage in cloud computing. In [1], Liefi Wei et al. Proposed SecCloud and SecHDFS for storage and computation which encrypt the data before sending it to the cloud and before

computation data will be decrypted without intervention of service provider. In [4], Laurace T. Yang et al. Proposed GNFS algorithm with parallel block and also Weidman algorithm for RSA security in cloud computing. Authors have also discussed the limitations of RSA and also discussed how GNFS is used in factoring large integer having more than 101 digits. In [9], Dimitrias Zissis, Dimitrias Lekkas addressed cloud security issues in tabular form representation by discussing levels of security users and security requirements and threats also. In [5], Den Bonch and Mathew Franklin, proposed an identity based encryption from weil paring where authors shown a model based on bilinear map between groups and also given several applications of such system. In [12], Manish M Potey et al. proposed a homomorphic encryption for security of cloud data. Authors showed that computation is performed on encrypted data in public cloud and results will be saved on users system. In [13], P. Ravi Kumar et al. Discussed various data security issues as well as resolution technique in cloud computing. In [6], Ali Azouaghge et al. proposed an efficient algorithm for data security in cloud computing where they encrypted data by AES and encrypted key produced by AES, by Elgamal. Then they sent data on cloud and stored key at local server. In [18], Tim Mather, Subra Kumaraswamy discussed Infrastructure security, security of data and storage, se- curity management in cloud and also identity access and management as well as key exchange and problem associated with it. In [11], Micheal Armbrust, shows a view of cloud computing where they proposed to clear the cloud away from the true potential and obstacle posed by cloud computing capabilities. In [14], Hsun Chuang et al. proposed an efficient privacy protection technique for cloud computing which satisfy the users’ requirements of privacy and also maintain performance of the system at the same time. In [16], Mahindha proposed a double encryption by applying DES algorithm on plain data and again applied RSA on encrypted data produced by DES and hence achieved two level encryption. In [15], Qian Wang et al. Tried to enable public auditability as well as data dynamics for cloud storage. Authors discussed integrity, public auditability and dynamic data operations. In [21], Naga Malleswari TYJ, Vadivu G, discussed deduplication of virtual machines in respect of data security breaches.

III. MOTIVATION AND RESEARCH GAP

From the available literature it can be stated that most of the authors are focusing on encryption, decryption while others are focusing on authentication. None of the research papers is focusing on integrity testing of the document on character level. There is a lack of algorithm which checks the document at character level before uploading it to the cloud storage and after downloading it from cloud storage. Hence there is lack of such algorithm in this field which must be designed and implemented to fulfill this gap. Talking from cloud perspective, our work is based on IaaS (Infrastructure as a Service). Our work builds on the knowledge that most of IaaS are not as secure as our desktop.
This paper has been written to make IaaS or HaaS (Hardware as a Service, computation power as well as storage) more secure and trusty and to reduce the fear of hacking and to check the integrity of the data. Following questions have been set as guidelines to fulfill this aim.

1. How a particular user will come to know that the data he uploaded on cloud server maintains the integrity or free from unauthorized alteration?

2. If data has been altered then how a particular user will come to know what characters or which of the characters has been altered?

3. How can we increase the security of the file being uploaded on cloud storage which is already multitenant?

This paper is an attempt to answer all the above said questions and to fulfill the gap which has been discussed earlier.

IV. PROPOSED ALGORITHM

The concept behind the proposed algorithm is very simple. Suppose someone reserved space on cloud in encrypted form but he or she cannot trust on cloud service provider, cloud current employees and ex-employees. These people can breach security because of their accessing power and privileges which is not an easy task in general.

Suppose someone rents storage on cloud and upload his data on his reserved storage and after uploading this data on cloud someone breaches security and make some changes in that data and suppose data is financial or some other sensitive data like military data, then after some times the owner download this data from cloud storage. Then an open question arises here:

How the owner of the data will come to know that his data was altered during the time it was stored on cloud storage?

To answer this question we have designed and implemented an algorithm which will test the data before uploading it to the cloud and will produce a matrix (which will contain the frequency of each and every character of the tested document) and after this user will upload this data on cloud either in plain text form or encrypted form. After some duration owner of the data will download data from cloud storage. After downloading the data user will again test the data by same algorithm and a new matrix will be produce. Now, a comparative analysis between these two matrices will be done. In our algorithm we have taken characters ‘a’ to ‘z’ and ‘0 to 9’. We stored frequency of character ‘a’ at first position of the matrix and that of ‘b’ at second position and so on…………the frequency of 9 at last position that is at 36th position. The size of matrix here is 6X6.

Although we can store our data on cloud in pure or in plain form but it is common intelligence to upload encrypted data on cloud because its nature is multitenant. In multitenant architecture many users shares the same hardware like storage or computation power. Therefore there are chances for data stolen from such suspected but cost effective place. Whenever someone performs computation on cloud server, some portion of data remains on its cache. When some other person rents this machine for computation then there are chances that the previous data available on cache may be hacked.

While sending data on cloud storage, we should know about the people who can steal or use our data without proper authorization. There are three categories of such people who are harmful to our data if we send data in plain form on cloud storage. These categories include:

- CSP (Cloud Service Provider itself)
- Internal employees of CSP
- Other clients in multitenancy and Man in the middle

Since cloud service providers and internal employees of all CSPs have all the privileges.

A. Conceptual Architecture of Proposed System

![Figure 2. Conceptual Architecture](image-url)
B. Proposed Algorithm

Algorithm: Integrit Testing

Input: Integer i=0, j=0 and $\Psi d$ as decrypted Text, $\Phi$ as Plaintext, I and F matrices of 6X6

Output: Integrit Testing

1. $F \leftarrow char\_frequency\ (\Phi)$

2. Upload this plain text or its encrypted form on cloud Storage on encrypting by AES Algorithm

3. Store F on local server

4. Download plain text or encrypted text from cloud if encrypted, converts it into decrypted text

5. $I \leftarrow char\_frequency\ (\Psi d)$

6. Test equality between I and F by repeating following steps from 7 to 8

7. While i<6 AND j<6 do Repeat
   a: if $F[i][j]$ equals $I[i][j]$
      Show- Integrity is preserved
   b: else
      Show- Integrity is not preserved

8. $i++, j++$

9. End

C. Plus points of proposed algorithm

- This algorithm checks the document and tests its integrity at character level.
- If from large file out of thousands of pages only one character is changed, this algorithm will inform us that the particular character has been changed.
- This algorithm reduces the fear of adopting cloud.
- This algorithm increases the market of cloud computing by encouraging the customers towards its adoption.
- Algorithm reduces the fear of hacking by keeping data secret.
- Market of cloud is expanded by increasing security.

V. DATA COLLECTION

For executing the algorithm, we collected data online from two sites. The data that we have collected from both the sources is in textual form only. These sources are:
- https://archive.ics.uci.edu/ml/index.php
- https://file-examples.com/index.php/text-files-and-archives

For more specific and detailed information, we are creating a table (Table I) which shows data source, type and size.

| Data Type | Data Source | Data Size |
|-----------|-------------|-----------|
| Textual   | UCI MLR     | 100KB     |
| Textual   | UCI MLR     | 200KB     |
| Textual   | UCI MLR     | 500KB     |
| Textual   | UCI MLR     | 1000KB    |
| Textual   | UCI MLR     | 2000KB    |
| Textual   | Examples.com| 500KB     |

Note - UCIMLR-UCI Machine Learning Repository

VI. EXPERIMENTS AND RESULT CALCULATION

To evaluate performance of our algorithm we developed application in java with its version jdk1.6.0 and NetBeans IDE7.2.1. Execution was performed on Intel Core i3-5005U CPU @ 2.00GHz, 8GB RAM, 1TB Hard Disk, 64 bit Windows Pro OS. Every experiment was performed on single threaded machine. All experiments were performed ten times. All the computed results are stored in table 1. We have taken file size from 1MB to 10MB. This table MCT stands for Matrix Creation Time and ITT stands for Integrity Testing Time. From Table II, it is clear that up-to 10MB algorithm is taking 2 seconds. This implies that the algorithm can be implemented for large data for which cloud storage really exist.

| File Size | MCT       | ITT       |
|-----------|-----------|-----------|
| 1 MB      | Less than 1 Second | 1 Second |
| 2 MB      | 1 Second  | 1 Second  |
| 3 MB      | 1 Second  | 1 Second  |
| 4 MB      | 1 Second  | 1 Second  |
| 5 MB      | 1 Second  | 1 Second  |
| 6 MB      | 1 Second  | 1 Second  |
| 7 MB      | 1 Second  | 1 Second  |
| 8 MB      | 1 Second  | 1 Second  |
| 9 MB      | 1 Second  | 1 Second  |
| 10 MB     | 2 Seconds | 1 Second  |

In step 2 of our algorithm, we have revealed that the file may be uploaded in plain form or in encrypted form on cloud storage. It is common intelligence to upload file in encrypted form. By the end of the step 2 we have discussed that the file will be encrypted by AES algorithm because encryption of DES was officially withdrawn in 2005. Even then we have encrypted data by using DES also.
For performing encryption by AES, we have used same environment with a small data set ranges from 50KB to 2MB data given in Table I, and computed results of encryption that are displayed in Table III, while results of decryption are stored in Table IV.

| Table III: Encryption time taken by AES and DES |
|-----------------------------------------------|
| File Size(KBs)  | AES Algorithm | DES Algorithm |
|----------------|---------------|---------------|
| 50KB           | 2             | 1             |
| 100KB          | 2             | 2             |
| 200KB          | 3             | 3             |
| 500KB          | 3             | 7             |
| 1MB            | 6             | 13            |
| 2MB            | 11            | 25            |

| Table IV: Decryption time taken by AES and DES |
|-----------------------------------------------|
| File Size(KBs)  | AES Algorithm | DES Algorithm |
|----------------|---------------|---------------|
| 50KB           | 2             | 1             |
| 100KB          | 2             | 1             |
| 200KB          | 4             | 2             |
| 500KB          | 5             | 4             |
| 1MB            | 8             | 7             |
| 2MB            | 15            | 14            |

VII. CONCLUSION

In this research paper we have proposed an algorithm which test document at character level. This algorithm test document and create character frequency matrix of tested document before uploading it to cloud storage and then upload it on cloud storage after some period when we download data form cloud we again create new matrix. Finally we compare these two matrices. If entries of these matrices at any level are different, algorithm will inform us that the particular character/characters has/have been altered.

FUTURE SCOPE

In last line of abstract of this paper we have cleared that the idea of the algorithm is same as of ‘error detection and correction’. The proposed algorithm can find which of the characters have been changed in the given documents. This is just like as error detection.

Now, future scope is to correct those characters that have been altered, this resembles to error correction.

REFERENCES

1. L. Wei et al., “Security and privacy for storage and computation in cloud computing,” Information Sciences, vol. 258, 2014, pp. 371–386.
2. Z. Deng, K. Li, K. Li, and J. Zhou, “A multi-user searchable encryption scheme with keyword authorization in a cloud storage,” Future Generation of Computer System., vol. 72, pp. 208–218, 2017.
3. H. Rasheed, “Data and infrastructure security auditing in cloud computing environments,” International Journal of Information Management, vol. 34, no. 3, 2014, pp. 364–368.
4. L. T. Yang, G. Huang, J. Feng, and L. Xu, “Parallel GNFS algorithm integrated with parallel block Wiedemann algorithm for RSA security in cloud computing,” Information. Sciences (NI)., vol. 387, 2017, pp. 254–265.
5. D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” SIAM Journal Computer, vol. 32, no. 3, 2003, pp. 586–615.
6. A. Azouaghe, Z. Karit, M. Hedabou, M. Belkasmi, and M. El Merraki, “An efficient algorithm for data security in Cloud storage,” 15th Int. Conf. Intelligent System. Design Application, 2015, pp. 421–427.
7. Mohd. Tajammul, Rafat Parveen and Mohd. Shahnazaw. “Cloud Computing Security Issues and Methods to Resolve: Review”, Journal of Basic and Applied Engineering Research, vol. 5, Issue 7; October-December, 2018, pp. 545-550.
8. S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer. Applications, vol. 34, no. 1, 2011, pp. 1–11.
9. D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation of Computer System, vol. 28, no. 3, 2012, pp. 583–592.
10. M. N. Manas, C. K. Nagalakshmi, and G. Shobha, “Cloud Computing Security Issues And Methods to Overcome,” International Journal of Advanced Research in Computer Communication. Eng., vol. 3, no. 4, 2014, pp. 6306–6310.
11. M. Armbrust et al., “A view of Cloud Computing,” Communication of ACM, vol. 53, no. 4, 2010, pp. 30–58.
12. M. M. Potey, C. A. Dhole, and D. H. Sharma, “Homomorphic Encryption for Security of Cloud Data,” Procedia Computer Science, vol. 79, 2016, pp. 175–181.
13. P. R. Kumar, P. H. Raj, and P. Jelciana, “Exploring Data Security Issues and Solutions in Cloud Computing,” Procedia Computer Science, vol. 125, no. 2009, 2018, pp. 691–697.
14. I. Chuang and S. Li, “An effective privacy protection scheme for cloud computing.” ICACT, 13th International Conference, 2011, pp. 260–265.
15. Q. Wang, S. Member, C. Wang, S. Member, and K. Ren, “Enabling Public Auditability and Data Dynamic in Cloud Computing,” IEEE Trans. Parallel and Distributed System, vol. 22, no. 5, 2012, pp. 847–859.
16. M. Tajammul, “Comparative Study of Big Ten Information Security Management System Standards”, International Journal of Engineering Research in Computer Science and Engineering, vol. 5, Issue 2, 2018, pp. 5-14.

17. M. Tajammul, “Comparative Analysis of Big Ten ISMS Standards and Their Effect On Cloud Computing”, 978-1-5386-0627-8/17/$31.00© 2017 IEEE

18. Tim Mather, Subra Kumaraswamy, and S. L, Cloud Privacy and Security, O’REILLY, 2009, pp. 336.

19. Dan C. Marinescu, Cloud Computing Theory and Practices. Elsevier, 2018, pp. 588

20. Dijiang Huang and Huijun Wu, Mobile and Cloud Computing, Elsevier, 2018, pp. 336

21. Naga Malleswari TYJ , Vadivu G, “Adaptive deduplication of virtual machine images using AKKA stream to accelerate live migration process in cloud environment”, Journal of Cloud Computing Advances, Systems and Applications, 2019, pp. 6-12. https://doi.org/10.1186/s13677-019-0125-z.

AUTHORS PROFILE

Mr. Mohd. Tajammul
Qualification: BSc((H) Mathematics, BED, MCA, M. Tech (IT), PhD Pursuing
Research Scholar Department of Computer Science, Jamia Millia Islamia, New Delhi, India

Research Work
1. Comparative Study of Big Ten Information Security Management System Standards, 2017, IJERCSE.
2. Comparative Analysis of Big Ten ISMS Standards and Their Effect On Cloud Computing, 2017, IEEE Explore.
3. M. Tajammul, R. Parveen, and M. Shahnawaz, “Cloud Computing Security Issues and Methods to Resolve : Review,” Journal of Basic and Applied Engineering Research vol. 5, no. 7, pp. 545–550, 2018.
4. Cloud Computing Security Issues And Methods To Resolve,International Conference On “Mobile Communication, Electronics, Robotics, Machine Learning, Data Mining, Information Sciences and Electrical Engineering” (MERDIE– 2018)
5. Comparative Study of Big Ten Information Security Management System Standards, 2017.
6. Comparative Analysis of Big Ten ISMS Standards and Their Effect On Cloud Computing, 2017.
7. How to connect SARC countries by cloud computing at Jamia Millia Islamia in 2017.
8. An Example of Object Oriented Programming (ATM Working) in National Conference held in Jhansi 2010.
9. 4G in Education- International Conference by MERI-CET in Jan 2012.
10. 4G What Why and When-International Conference by MERI-CET in Jan 2012.
11. 4G in Mobile Learning- International Conference by OITM in Feb 25-26 2012.

Dr. Rafat Parveen
Qualification: MSc. M Tech, PhD (Computer Science)
Associate Professor, Department of Computer Science, Jamia Millia Islamia, New Delhi, India

Research Work
• Rafat Parveen, (2017) Early prediction of Lungs Cancer Using Systems Biology communicated , IEE Journal of Systems Biology.
• Parveen, R. & Raza, K. (2013). Reconstruction of gene regulatory network of colon cancer using information theoretic approach. In Proc. of 4th International Conference (CONFERENCE-2013): The Next Generation Information Technology Summit, 26-27 Sept, 2013, p. 461-466. doi: 10.1049/cp.2013.2357 (IEEE Xplore & IET Digital Library).
• Raza, K. & Parveen, R. (2012). Soft computing approach for modeling genetic regulatory networks. Advances in Intelligent Systems and Computing, 178, 1-11, Springer-Verlag Berlin Heidelberg, doi: 10.1007/978-3-642-31600-5_1
• Raza, K. & Parveen, R. (2012). Evolutionary algorithms in genetic regulatory network model. Journal of Advanced Bioinformatics Applications and Research, 1(3), 271-280, (Global IF 1.057)
• Rafat Parveen, Simulation of Regulatory Networks, WORLDCOMP,International Conference,USAJuly 17-21,2011
• Rafat Parveen ,Read I.Hamed and Prof.Syed Lahsnon,Modelling Cellular Process of the Eukaryotic DNA Using Hybrid Functional Petri Networks, International Journal of Bioinformatics, ISSN:0974-6439, Vol. 1(2), pp. 55-56. July-Dec,2008
• Rafat Parveen ,Read I.Hamed and Prof.Syed Lahsnon, A new approach for Modeling Gene Regulatory Networks Using Fuzzy Petri Nets.Journal of Integrative Bioinformatics(JIB), Vol 7(1):113.g.p.1-16,2010,Germany
• Rafat Parveen ,Read I.Hamed and Prof.Syed Lahsnon, Petri Nets Modeling and Simulation of Transcriptional Regulation in E.Coli.A Journal of Bioinformatics and its Applications, Bioinformatics Trends;Vol(2 & 3),pp.87-91,2009
• Rafat Parveen, Read I.Hamed and Prof.Syed Lahsnon, Designing Genetic Regulatory Networks Using Fuzzy Petri Nets Approach (IJAC),Springer-Verlag Berlin Heidelberg, Vol 7(3),pp403-412.2010
• Rafat Parveen ,Read I.Hamed and Prof.Syed Lahsnon ,A new Interpretation of Gene Expression Microarray Data Sets Using Petri Net Approach, International Journal of Engineering Research and Industrial Applications(IJERIA).ISSN.0974-1518,Vol 3, No. 1, pp.11-25,2010