International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 1 (2016) pp 731-737

Ensures Dynamic access and Secure E-Governance system in Clouds Services – EDSE

Rajan Manro
Research Scholar, IKG Punjab Technical University, Jalandhar, Punjab, India.
Email id: rajanmanro@gmail.com

Dr. Tripat Deep Singh Dua
Asst. Professor, Department of Computer Applications
Guru Nanak Institute Of Management & Technology (GNIMT)
Model Town Ludhiana, Punjab, India.
Email id: tripatdua@yahoo.com

Dr. A.S. Joshi
Former Director, Punjab Institute of Management & Technology,
Mandi Gobindgarh, Punjab, India.
Email id: asjoshij@yahoo.com

Abstract
E-Governance process helps the public to learn the information and available of data's themselves rather than being dependent on a physical guidance. They have been driven through e-govern experience over the past decade; hence there is a necessity to explore new E-Governance concepts with advanced technologies. These systems are now exposed to wide numbers of threat while handling theinformation. This paper therefore designing an efficient system for ensuring security and dynamic operation, so Remote Integrity and secure dynamic operation is designed and implemented in E-Governance environment. The data is stored in the server using dynamic data operation with proposed method which enables the user to access the data for further usage. Here the system does an authentication process to prevent the data loss and ensuring security with reliability method. An efficient distributed storage auditing mechanism is planned which overcomes the limitations in handling the data loss. The content was made easy through the means of cloud computing by using innovative method during information retrieval. Ensuring data security in this service enforces error localization and easy identification of misbehaving server. Availability, Confidentiality and integrity are the key factors of the security. In nature the data are dynamic in cloud service; hence this process aims to process the operation with reduced computational rate, space and time consumption. And also ensure trust based secured access control.

Keywords: Remote Data Integrity Checking, Data Security, cloud server, Distributed Storage

Introduction

Nowadays, Government applications are used to access the information with the revolutions changes and make the citizens to process through internet in a simple and efficient way, in terms of interact and learn. Naturally changes of the government functions reflect in the government organization, relationship between citizens and government, businesses and institutions etc. In cloud computing, E-Governance leads a significant role of client convenient and cost savings. The infrastructure of software and hardware entails the usage over the Internet for hosting the applications remotely. E-Governance application makes easy to do the activities like income taxes, pension services, administration etc. by using IT infrastructure. It improves the redundancy reduction at various levels with the function efficiency. It provides accessibility of various services in the framework of E-Governance irrespective of language barriers and the locations. In existing models [4] various problems of framework is defined and unable all categories to address from rural urban to metropolitan citizens. The general categories of the E-Governance application are:

1. Government to Employees (G2E): Income tax etc.
2. Government to government (G2G): Administration and policy formation etc.
3. Government to Consumer (G2C): birth certificate, License, Land record etc.
4. Government to Business (G2B): Tender, Taxation etc.

The dynamic operation is the most essential process in E-government Cloud Service. Secured access system is a challenging issue because through internet at desktop level the information is exposed. The system scenario is considered to provide highly essential secured access system to prevent the information from misbehaving server. E-Governance is like a virtual access of information's with online scenarios, where every part of is done through Internet. The aim of this work is to ensure the data content availability, reinforcement and management of information through cloud service. Nowadays without worrying the technical information can be accessed by the end user through internet from anywhere at any time. After computation appropriate resources are delivered as services through the network in E- governance application as in Fig [1].

In this paper, the research work aims at designing the system which uses, an efficient flexible dynamic operation scheme is performed to ensure the availability of information and data correctness in cloud. In E- governance application through cloud service, Remote data integrity checking, Distributed storage system and Data security method is used to ensure secure storage and access. It supports dynamics data and public verification considering the untrusted server with security analysis. Unrecoverable data losses are prevented by using security mechanism with secure process. The proposed

work aims is to provide high performance, less computation cost and to reduce the data upload time and space taken in E-governance environment.

It provides a link among end users across the globe in a simple manner. Through host network services the information's are stored and accessed in the cloud service. In this work for secure accessibility and also to detect the misbehaving server and data corruption the remote data integrity checking protocol is implemented.

The paper organization is as follows: in section II related works are discussed. The proposed work for E-Governance access and storage with secure process has discussed in section III. The implementations of the proposed algorithms are discussed in section IV. In section V, The performances analysis of research work is evaluated with the comparison of existing system. Finally conclusion has discussed in section VI.

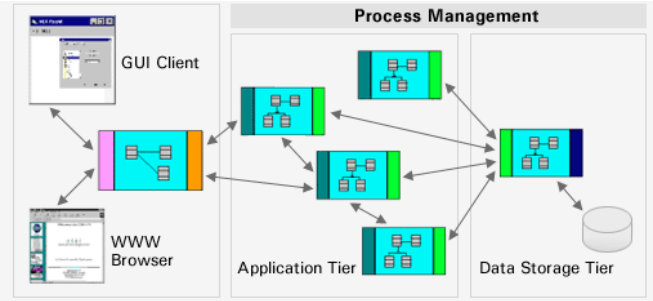

Figure 1: Typical architecture of E-Governance application

Related Works

In this section, literature survey is done about the Dynamic information access of the E-Governance application in cloud services. E-Governance system is one of the applications in cloud computing which is beneficial for all educational institutes, enterprise and industries, improving the quality of information shared and efficient learning with minimum cost. In E-Governance model, the services are available in urban and rural areas. In rural areas non-availability of infrastructure for the application is the biggest problem like technology awareness. The issues are overcomes by fulfilling the needs of E-Governance services for the rural citizens by using the application in cloud environment. The e-Governance service offers the services with the generic and oriented process of government in the computing model. It's not only for the specific area; in worldwide the application usage is providing more benefits [3], [4].

As a long term service, secure accesses of storage are provided in cloud services [2], [5]. Through encryption and decryption process, the storage and retrieval system are secured. The proxy re-encryption scheme is analysed to encode the data for secure process. These systems suggest a parameter to provide flexibility in cloud storage service and reduces the cost of the resource requirement. Untrusted server is detected by using the data integrity checking and data correctness. In the research work [1], the data partitioning is discussed. The data will be split into many parts using the splitting technique for easy storage of data in cloud. For flexible distributed storage in E-Governance application in cloud server, pre-computation process and integrity mechanism is discussed in [6]. To detect the data correctness and error localization in the application the integrity checking is implemented. It is used to achieve the integrity of dependable storage services, availability, flexibility and the quality of the data. The scheme shall be resilient against the threat and the attack in cloud services [22], [23].

In cloud storage, the data integrity is analysed in the research works [9]. Data integrity is supported by dynamic data operation and public auditability to have evaluation of the quality in services and independent perspective with the third party auditor. Multiple auditing tasks are devised here to increase the efficiency of storage model. A secure storage system consists of public auditing and data integrity checking. For efficient access of multiple users simultaneously TPA is implemented for a fast performance, the work conducted on Amazon EC2 were discussed in [8], [1]. In E-Governance application in cloud have forwarded various Hadoop components and specify it for access by the hardware commodity or thin clients. It initiated the layer on domain for the expert system [7], [12].

Public auditing is established in the cloud data storage to help cloud economy. When needed of accessing the risk of outsourced data the trusted entity and the capabilities data owners do not group as an external audit party. For reality of cloud storage the public auditable secure cloud storage services is analysed and evaluated in [11].

In the work [10], author discussed about the encryption and access control of outsourced data in cloud. By HASBE scheme a flexible access services and the secure data storage is handled in cloud computing. It provides the performance, security, complexity, scalability and flexible access of the outsourced data through encryption and access control with a hierarchical structure of users. Cryptography scheme is discussed in [20], [21]; this scheme is used to provide an efficient secure storage using public key. RSA algorithm is used here for the secure process of the secret documents. It provides more security that is robust against the threats and attacks over the public network. RSA algorithm is implemented for the speed transmission and for communication between networks. It consists the key generated for the secure process and in all networks gateway the database are detected for the storage of data's. For speeding up of RSA decryption for retrieval of data from cloud and to improve the performance the algorithm is implemented with the load transferring and multi prime techniques are analysed in the research works. The author outlines the security of the data storage in cloud and the privacy of the system [22]. The critical security issues are listed for the secure process and to find the solution for it. In the public cloud environment the secure access is the major issue, to overcome this some of the security algorithm are considered [17].

In the work [14], the author generated and discussed about the Huffman algorithm for the data compression and decompression. It provides the performance of the system and reduces the cost of the services. PDLZW Algorithm takes place for storage to improve the performance and to reduce the storage space of data when compared to general process. Tree based structure is used in this algorithm to list the order

for speeding up the data rate of the compression and decompression. The technique consists of encoding and decoding process for the secure access in cloud. Based on progress of encoding the bit rate accuracy and the performance are analysed by the algorithm are discussed in [16]. The data compression algorithm consisting of the comparison between the techniques used in the algorithm for compression and decompression are evaluated.

In paper [15], author discussed about the lossless compression technique that is used for compressing and storing the data in cloud. Huffman algorithm has been achieving the output and it consists hybrid technique of the code components. Huffman model requires O(σlogn) bits as a size of text. The encoding scheme ws designed for the worst case scenario, to calculate the time and the performance of the compression and decompression of the data. In this case it requires σlog logn+O(σ+log2n) bits and encoding and decoding is supported in O(log logn) time. This scheme consists of the model used to analysis the time taken for compression / decompression as discussed in [14].

The perceptions for the issues in security and solution for related issues are essential to provide ensure access in hybrid cloud computing of E-Governance application [18]. In Information and Communication Technology (ICT) world the model provides the process speed and more information by cloud computing. The main factors are on demand self-service, pay per use, rapid elasticity etc. A public cloud service provides the management and control by the vendors like Canonical / Eucalyptus, Amazon.com, Google.com, Microsoft, Oracle/Sun etc. In Private cloud services, the overall controls and loaded process of software are provided by VMware, Microsoft, Eucalyptus, Citrix etc. Governments are adapted or planning to have efficiency improvement and cost reduction of services and infrastructure. Also, several security issues are considering in the sector during the adaptation speed [13], [19].

In this survey much of the discussions are related to works, which ensures the E-Governance services in the cloud environment. Integrity checking and computation process are ensuring dynamic data operation and services. The limitation with existing mechanism have performed the dynamic processing with more time and cost in cloud services for secure storage of data. The proposed work overcomes such limitations with high performance, reduced cost and limited data storage space in cloud. It also ensures resilience against threats, attacks and misbehaving server. It also helps in reducing the time and cost consumed making an efficient and secure service in E-Governance environment.

E-Governance Service with Secure Storage and Access

E-Governance cloud service system; includes secure process and control of the system. This system provides the strategy for improving the system in cloud service environment. Relevant hardware and software resources are engaged for computing in the E-Governance environment to meet the requirements of the end user. E-Governance application is accessible via cloud around the world. Proposed system is hosted through third parties' data center on server. Storing of original data is complex, for efficient data storage on server partition and encryption method is implemented in E-Governance environment. It aims in providing secure access and the integrity assurance. It provides less provision time. By this method, a flexible access is provided in the E-Governance environment. Dynamic remote data integrity checking method is implemented to detect threats and provide secure process. Data access and the dynamic operation are supported with end user. By the secure model of the system, it will detect the threats and also prevents the data from any attack. The proposed architecture ensures access of E-Governance system as shown in Fig [2].

Data is stored in secured manner by the integrity checking process. Ensuring data correction when data is accessed from the server. With this system, cloud service enables the services in secured manner. As per the schedule, the process and the management of the system are ensuring secure access and security. And the daily process of the system and the content are managed and stored in the server. The content can be accessed at any time for the end user reference and it's available always on server.

In E-Governance cloud server; the data is encrypted and decrypted with key generating for ensure security for accessing. Encryption method is used to encrypt the files for ensuring secure data to store in storage server. Decryption method is used to decrypt the data for accessing from server. Accessing of the original file consists with the merging technic. This technic used to reconstruct the separated files in to single or original file as end user required.

In EDSE work, compression technique is used to store data with minimal storage space and with better performance access. Compressions techniques take place after encrypting of the data and decompress take place before the decryption as shown in the Fig [3]. During the retrieval, the data are decrypted by generating the public key. In this work, ensuring of storage take place with high performance and scalability. This ensures data security from unauthorized access. Integrity checking is used to avoid the threats and to recover the failures; here Remote data integrity checking is used for the secure process of the data in E-Governance cloud server during storage and access. The remote integrity checking method manages the verification, error localization, error recovery and misbehaving server.

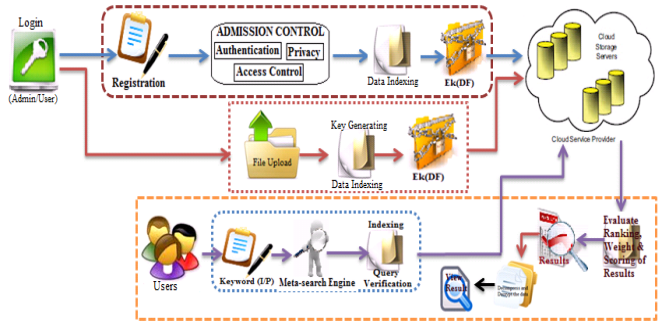

Figure 2: Dynamic secure storage system

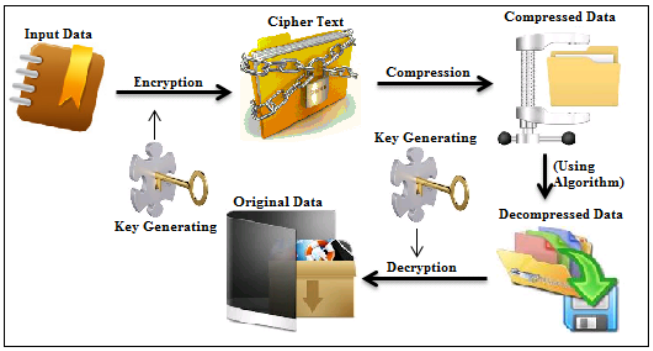

Figure 3: Encryption/ Decryption and Compression/ Decompression

$$\text{Sender} = \text{Partitioning} + \text{Encryption} + \text{Compression}$$
$$\text{Sender} = C_x\,(E_e\,(P_x))$$
$$\text{Receiver} = \text{Decompression} + \text{Decryption} + \text{Merging}$$
$$\text{Receiver} = \sum_{i=1}^{n} (D_x\,(D_e\,(M_x)))$$

In this work, flexible and efficient access control is provided for authentication purpose and also to detect the attacks. By this mechanism the storage time, space and the computation costs are reduced. As per the function of storage and retrieval the overall process of this research work take place for efficient secure access of data from the cloud server.

Implementation Issues

In this section, Implementation and Analysis of the proposed method of E-Governance application in cloud server is done. An efficient storage access of the system involves with the integrity check, by implementing the proposed work. Access control, storage time and the computation cost are the parameters considered in this environment. Implementation of proposed work in E-Governance service provides an efficient secure storage and less provision time. By this method, the content is stored in cloud server efficiently in secured manner. The implementation issues of EDSE work are discussed as below.

A. Improved Adaptive Huffman Technique

Normally for sending and receiving of data from one end to other end requires lot of time and space but by using proposed technique the storage time and space is reduced and this technique supports the real time process.

B. Improved RSA Double Encryption And Decryption Technique - IRDEDT

The key is generated to encrypt the data for storing and retrieval of data in the data base server. To ensure the security RSA algorithm is improved with the double encryption technique. Key Variants have been reviewed and analyzed against the attacks.

In Un-predictable technology revolution, Lifespan of this algorithm is indeed of matter. By this modification in RSA double encryption algorithm its lifespan is extended and the process performance has been improved.

Algorithm 1: Improved Adaptive Huffman Technique

```
1:  Procedure
2:    create node ZERO
3:    read Symbol(X)
4:    while (X! =EOF) do
5:     begin
6:       if (first_read_of(X)) then
7:        begin
8:          output (ZERO);
9:          create new folder - output(X)
10:               Initialize_model ();
11:               While ((c=getc (x))! =eof)
12:               compress(c, output);
13:               Update_model (c);
14:       end
15:       else
begin
16:              While ((c=decompress (input))! =eof)
17:               putc (c, output);
18:               Update_model (c);
19:               end
20:       else
begin
21:               output(X)
22:               Statement "File not exit "
23:               end
24:       read Symbol(X)
25:     end
26:  End Procedure
```

Algorithm 2: IRDEDT

```
1: Procedure
2:  private void encrypt (F - Data)
3:   begin
4:    Create a key generator
-           Create a secret (session) key with key generator
-           Initialize data for encryption with session key
5:    Send to Encryption method
6:    Get public key
-           Initialize data for encryption with public key and encrypt
session key
7:    Encryption:
-           Original plain text (a block value) = F ... F < N.
-           Chiper text = C ... C = (F^E) mod N
C = F^e mod N
8:    Send encrypted data X and session.
-           Y=Ksim(F),T=Kpub(Y),
-           Y=Kpri (T), F= Ksim(Y)
9:   end

10:  public String decrypt (encrypted key, E-data F)
11:    Decrypt the data F
12:    begin
13:      Get private key from file
-  Initialize the data for decryption with private key and with session
key.
14:      Decryption:
-           Chiper text = C;
-           Plain text = F;
-           F = C^d mod N
(or)
-           By Using CRT
M1 = C^dP mod P
M2 = C^dQ mod Q
H = (M1 - M2) inv Q mod P
Y = M2 + (Q * H)
```

14: end
15: End Procedure

Performance Analysis

In E-Governance application the dynamic operation take place with the IRDEDT and Improved Adaptive Huffman Technique. In order to evaluate the performance of the EDSE (Efficiency, Complexity and performance are include in it), to calculate this evaluate the system with different files that will be suitable for the analysis of the system. The process and the machines are defined as Intel core I5, 4.00 GB of RAM and 500 GB of hard disk.

A. Analysis Of The Dynamic Operation

Performance of the technique is evaluated in data storage and the times taken to perform process in secure manner are obtained. Fig [4] shows the time taken to split the data for easy storage and it specified the performance of the proposed algorithm when compare to existing work. Fig [5] shows the storage space for storing the split files with less space. When compare to existing work the proposed method provides an efficient storage with better result.

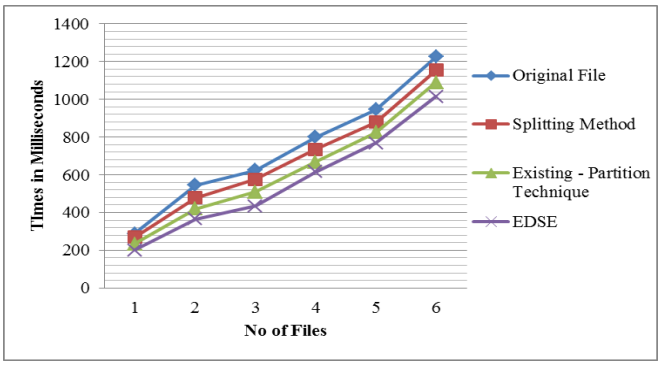

Figure 4: Time taken for Partitioning the Files

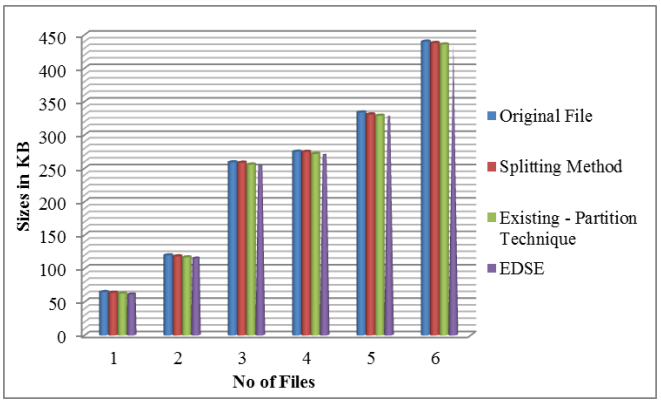

Figure 5: Storage Space for the splitted Files

B. Analysis Of Irdedt

This technique provides the security for the data after partitioning and performs an efficient access control process. As explained in the implementation part, the performance of this technique is analyzed and the result of the analysis and performance is shown in Fig [6].

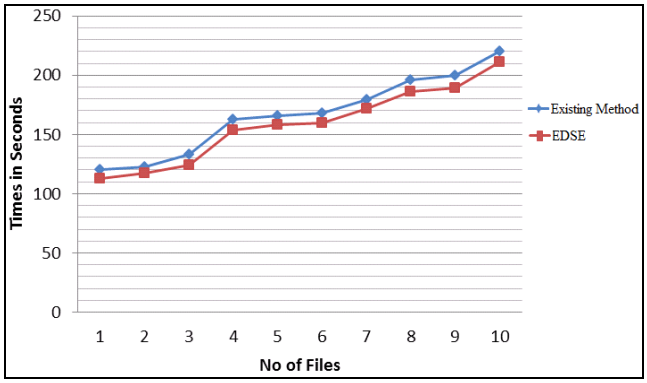

Figure 6: Time taken for Encryption and Decryption Technique

C. Analysis Of Improved Adaptive Huffman Technique

This technique helps the secured data in compressing and storing in E-Governance application server with minimal space when compared to the existing work, it also provides a secured process with complexity and efficiency. As explained in the implementation part this technique is performed in the EDSE work and the storage space of the files after compression is shown in Fig [7] and time taken for compressing the files in EDSE is as shown in Fig [8].

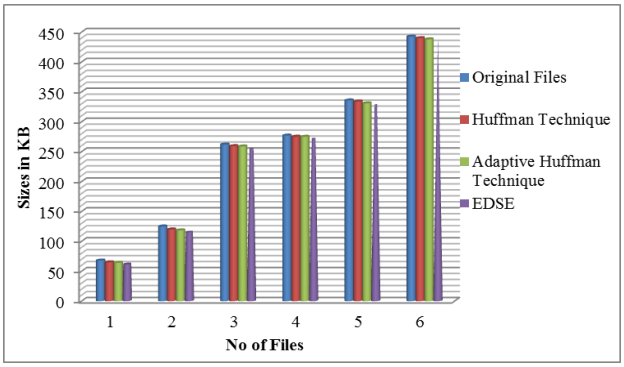

Figure 7: Storage space for compressed Files

Time and space complexity of the storage and retrieval process is evaluated as given below.

TIME COMPLEXITY: O(N*LOG|Σ|)
SPACE COMPLEXITY: O(|Σ|)

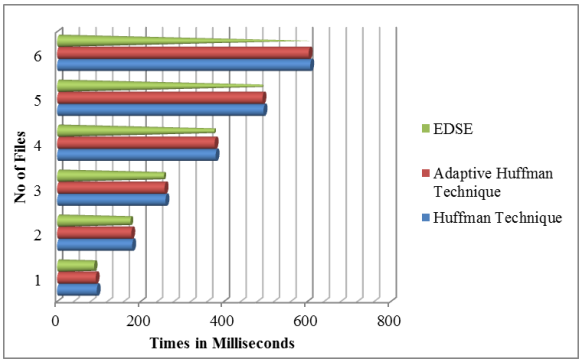

Figure 8: Storage Time for compressed Files

In this research work the complexity of the time and space is calculated to prove that the performance of this work provides an effective and efficient access for storage and retrieval of data from cloud server of E-Governance application. The result shows, this research work performance time and space has been improved with secure process. From the result of the EDSE experimental study, we have concluded this research work, as shown in performance analysis. Analysis of the research work with the existing work is evaluated.

Hence this work aims at ensuring the security process and storage process in an efficient manner. It also ensures the identification of misbehaving server, better cloud storage integrity, and enhanced error localization; while storing data in cloud server E-Governance application. So the overall performance of the EDSE work provides a secure access control, efficiency, less storage space and less time access without loss of data, Complexity, Efficient storage process and Flexible access.

Conclusion and Future Work

In this work, we propose an E-Governance service with an efficient secure data storage in cloud service. The proposed E-governance management system will be reliable, easy to use and reusability of the function is considered. E- governance System is designed to provide the information that is current and relevant to the subject area. It also provides cost-effective platform for deploying and tracking the content.

A streamlined, intuitive interface in E- governance features easily navigating diverse resources, with powerful search and information storage methodologies, manage and retrieve personalized learning plans. The dynamic remote data integrity checking method detects threats and misbehaving server while storing data in cloud server of E- governance application, ensuring data security. This research work provides a secure dynamic storage system in an easy manner improvised on cost saving, flexible access and performance complexity. Also, the proposed algorithm is applicable for all E- governance applications like Employee Management Systems, Municipal Maintenance, District Management Solutions, Tax Filing Systems, Water Boards, Billing, Payment Systems, E-police, E-court and Government office service Desk.

Future work is planned to provide higher level of security and searching mechanisms for E- governance system with outsourced computations in E- governance application. The positive investigation results lead to a proposal of the research in future and also to reduce the compression ratios and comparable to static. Still new ideas come forth as the field continues to progress further for secure storage and access in E- governance cloud services.

References

[1] Swapnil V.Khedkar , A.D.Gawande; “Data Partitioning Technique to Improve Cloud Data Storage Security,” International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3347-3350.

[2] Cong Wang; Chow, S.S.M.; Qian Wang; Kui Ren; Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," Computers, IEEE Transactions on , vol.62, no.2, pp.362,375, Feb. 2013.

[3] Dileep Kumar Gupta Abhishek Mishra Dr. G. Sahoo, “Cloud Computing: Solving Availability Problem in Future Framework for e-Governance”, International Journal of Computer Applications & Information Technology Vol. 2, Issue II Feb-March 2013.

[4] ASHISH BHUSHAN KHARE, VISHAL RAGHAV AND PRATEEK SHARMA, “CLOUD COMPUTING BASED RURAL E-GOVERNANCE MODEL”, Journal of Information and Operations Management, ISSN: 0976–7754 & E-ISSN: 0976–7762 , Volume 3, Issue 1, 2012, pp-89-91.

[5] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy- Preserving Public Auditing for Secure Cloud Storage,” IEEE Trans.Computers, preprint, 2012.

[6] Hsiao-Ying Lin; Tzeng, W.-G.; , "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," Parallel and Distributed Systems, IEEE Transactions on , vol.23, no.6, pp.995-1003, June 2012.

[7] Hardayal Singh Shekhawat and D.P. Sharma, “Hybrid Cloud Computing in E-Governance: Related Security Risks and Solutions”, Research Journal of Information Technology 4(1): 1-6, March 10, 2012.

[8] Tiancheng Li; Ninghui Li; Jian Zhang; Molloy, I.; "Slicing: A New Approach for Privacy Preserving Data Publishing," Knowledge and Data Engineering, IEEE Transactions on , vol.24, no.3, pp.561-574, March 2012.

[9] Wang Cong, Wang Qian, Ren Kui, Cao Ning and Lou Wenjing , "Toward Secure and Dependable Storage Services in Cloud Computing," Services Computing, IEEE Transactions on , vol.5, no.2, pp.220-232, April-June 2012.

[10] Zhiguo Wan; Jun'e Liu; Deng, R.H.; "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing," Information Forensics and Security, IEEE Transactions on , vol.7, no.2, pp.743-754, April 2012.

[11] Qian Wang; Cong Wang; Kui Ren; Wenjing Lou; Jin Li; , "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," Parallel and Distributed Systems, IEEE Transactions on , vol.22, no.5, pp.847-859, May 2011.

[12] Ajay Prasad, Sandeep Chaurasia, Arjun Singh, Deepak Gour, “Mapping Cloud Computing onto Useful e-Governance”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 5, 2010.

[13] K.Mukherjee, G.Sahoo, “Cloud Computing: Future Framework for e-Governance”, International Journal of Computer Applications (0975 – 8887)Volume 7– No.7, October 2010.

[14] Ming-Bo Lin; Yung-Yi Chang, "A New Architecture of a Two-Stage Lossless Data Compression and Decompression Algorithm," Very Large Scale Integration (VLSI) Systems, IEEE Transactions on , vol.17, no.9, pp.1297,1303, Sept. 2009.

[15] Renugadevi, S.; Nithya Darisini, P.S., "Huffman and Lempel-Ziv based data compressi20on algorithms for wireless sensor networks," Pattern Recognition, Informatics and Medical Engineering (PRIME), 2013

International Conference on , vol., no., pp.461,463, 21-22 Feb. 2013.

[16] Srikanth, Sure.; Meher, Sukadev, "Compression efficiency for combining different embedded image compression techniques with Huffman encoding," Communications and Signal Processing (ICCSP), 2013 International Conference on , vol., no., pp.816,820, 3-5 April 2013.

[17] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73,2012.

[18] Smithe k k, Dr.Tony Thomas, Chitharanjan K, " Cloud based E-Governance System : A Survey", International Conference on Modelling, Optimization and Computing (ICMOC2012), Sciverse Science direct, Procedia Engineering 38 (2012), 3816-3823.

[19] Rashmi Sharma, Anurag Sharma, Dr. U.S. Pandey, " E – Governance: A Successful Implementation of Government Policies using Cloud Computing", International Conference on Web Services Computing (ICWSC) 2011.

[20] Wang, Suli; Liu, Ganlai, "File Encryption and Decryption System Based on RSA Algorithm," Computational and Information Sciences (ICCIS), 2011 International Conference on , vol., no., pp.797,800, 21-23 Oct. 2011.

[21] Xin Zhou; Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," Strategic Technology (IFOST), 2011 6th International Forum on , vol.2, no., pp.1118,1121, 22-24 Aug. 2011.

[22] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[23] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1-9, July 2009.

Author Details:

Rajan Manro is an Assistant Professor and Head, Computer Science Department in Desh Bhagat University, Mandi Gobindgarh, Punjab, India. He has more than 11 years of academic experience. He has done MCA degree from the GGNIMT, Ludhiana, Punjab, India, in 2004, the Post-Graduation Diploma in E-commerce from ITI, Ludhiana, Punjab, India in 2001 and he received the M.Phil. Degree in Computer Science from Periyar University, Salem, India in 2008 .He is certified Oracle-9i (DBA) Professional. He is an author of more than 22 books on different subjects like Java, ASP.Net, Artificial Intelligence, MIS, Expert System & RDBMS. More than 14 papers are published in different journals and conference proceedings. His research interest is in the areas of Cloud Computing, e-governance, Big data Analysis AI etc. and he is presently working on it.

Dr Tripat Dua is as an Associate Professor, Computer Application Department in Guru Nanak Institute of Management & Technology, Ludhiana, Punjab, India. He received the Ph.D. degree in Computer Applications from Punjab Technical University, Jalandhar, Punjab, India in 2012. He is certified MCSE Professional. He is Member of Board of Studies of Computer Sciences of Punjab School of Education Board, Mohali, Punjab and Life member of ISTE (Indian society for Technical Education), New Delhi. His research interests include mobile adhoc networks, wireless communication networks, Cloud Computing, Big data Analysis, etc.

Dr. A.S. Joshi is retired Professor and Head, Economics and Sociology, in Punjab Agricultural University, Ludhiana. His qualification is M.A Economics, Ph.D. He is having 37 years of experience. He is member of Punjab State Electricity Regulatory Commission. More than 100 papers are published in different journals and conference proceedings.