Efficient FragSecure Framework for Data Security and Fragmentation in Cloud Computing

Ashima Narang, Deepali Gupta, AmandeepKaur

Abstract*: With the development in the technology, the risks of the threats and theft are increases day-by-day and this will put question mark in user's mind while using the different technologies like Cloud. The demand of the Cloud is also increasing due to its different services so there is a need to prevent the cloud network from external or internal attacks with the objective to make it more secure to provide better and efficient services. The number of security mechanisms was proposed for security where some of them use a concept of fragmentation that divides the data into subparts and then encrypt and store each part into different servers. These mechanisms are good enough to provide security but the problem of data loss due to fragmentation was introduced. So, to cop up this problema novel framework is designed with secure environment to protect cloud from theft of the data/tasks given by users and also reduces the data loss factor. In this framework,data is divided into fragments on the basis of different criteria to control data loss and then each fragment is encrypted using hybrid security algorithm. This framework is simulated on local cloud environment with a large amount of data storage where data is of different types like, image, audio and text data. The results achieved is better as compare to the existing frameworks in terms of Data Loss, Storage time, and Size of the data after encryption.

Keywords: Cloud Computing, Security, Fragmentation, Data Storage, Hybrid Encryption.

I. INTRODUCTION

In this Era of Technology, Cloud becomes the top most technology used by different industries and organizations due to its services and offerings. The research and analysis market [1] show that the services of cloud will rise day-by-day. The main advantage of the cloud is, it helps to reduce the cost of different services like software, infrastructure and platform cost. Due to this advantage a lot of enterprises startedusing cloud services for different purposes. It reduces the cost by improving utilization, reducing infrastructure and administration cost and fast services. Cloud Computing is one of the computing techniques which provides highly scalable resources through internet and provide services on demand of users and pay per use basis. Cloud provide different services in which Cloud Storage is one of the most used service. Now-a-days different applications like iCloud, Dropbox, Google Drive are used for storage and it changed the level of storage and improve the way of files stored [2]. Cloud Storage is the key infrastructure to achieve seamless information sharing and service interaction experience from different users, different applications, and different devices around the world using Internet. The use cloud is now-a-days similar to other public services like electricity, water that is available in anywhere and anytime. It provides highly flexible and high-performance service having high capacity and high security which solves the problems of number of users for storage like, low price, safety, high capacity and stability and due to this opted by many individuals and organizations as well. The services provided by cloud are based on five different attributes named as: Scalability, Elasticity, Multitanancy, self-provisioning of resources and pay as you go. It makes new advances in processors, disk storage, Virtualization innovation, broadband Internet association, and quick, economical servers have joined to make the cloud amore convincing arrangement. So as to give information stockpiling administrations, distributed storage utilizes programming to interconnect and encourage cooperation between various sorts of capacity gadgets. Contrasted with conventional capacity strategies, distributed storage presents new difficulties in information security, dependability, and the executives. The general cloud architecture contains different network entities in the model [3] and these are (i) Users/Clients, (ii) Cloud Service Provider (CSP) and (iii) Third Party Auditor (TPA). Clients, who have information to be put away in the cloud and depend on the cloud for information calculation, comprise of both individual buyers and associations. A CSP, who has noteworthy assets and skill in structure and overseeing dispersed distributed storage servers, claims and works live Cloud Computing frameworks, TPA is a discretionary substance, who has ability and capacities that clients might not have, is trusted to survey and uncover danger of distributed storage benefits in the interest of the clients upon solicitation.In cloud information storage, a client stores his information through a CSP into different cloud servers, which are running in a concurrent, collaborated and disseminated way. Information excess/redundancy can be utilized with method of eradication remedying code to additionally endure issues or server crash as client's information develops in size and significance. From that point, for application purposes, the client associates with the cloud servers through CSP to get to or recover his information. As clients never again have their information locally, it is of basic significance to guarantee clients that their information is in effect effectively put away and kept up. That is, clients ought to be furnished with security implies so they can make consistent accuracy confirmation of their put away information even without the presence of nearby duplicates. This paper deals with the security mechanism that were used for providing security while storing data on cloud servers and proposed a novel approach for this. The next sections include different security methods that were opted in cloud by different authors, proposed FragSecure Framework, its implementation on local cloud environment and performance analysis on the basis of time, size and data loss.

Revised Manuscript Received on May 07, 2019.

Ashima Narang, Computer Science Department, Maharishi Markandeshwar University, Sadopur, India.

Deepali Gupta,Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India.

AmandeepKaur, Computer Science Department, Maharishi Markandeshwar University, Sadopur, India.

II. SECURITY IN CLOUD COMPUTING

Security is a major concern in Cloud computing because of its increased demand and use. There are number of approaches developed by the authors to provide security in cloud data storage architectures but still lack of security is there in cloud and due to some of the security mechanisms, data loss increases. Here are some security mechanisms that were developed for cloud environment to provide security at different levels.A Multi-objective Optimization Model was developed by Liu et al. [4] for reliable data storage services in cloud computing. This work considers both reliability and cost of storage services. The cost was analyzed on the basis of three different cost factors and that are (i) Data Migration Cost, (ii) Storage Space Occupation Cost, and (iii) Communication Cost. Similarly, reliability factor is also depending on the (i) transmissionreliability, (ii) equipmentstability, and (iii) softwarereliability. For optimization, Particle Swarm Optimization algorithm is designed with multi-objective model. For Experimentation of this proposed model, data set of 120 TB was used which contains 10 sub-files with different size. In this work, three different strategies were followed for storage and these are:

A. The Integral Storage

In this all the sub-files treated as a single file and stored on the server.

B. Separate Storage

In this each subfile can be stored separately on the server.

C. Splitable Storage

In this all the sub files can be partitioned into several smaller fragments and then stored on the server.

Experimental results show that their proposed model was positive and effective.The experimental results also demonstrated that the proposed model can performmuchbetterwithproperfilesplittingmethods. Cloud computing is now-a-days very popular and used by various organizations. Health care sector is also the one of them who uses cloud services and need security mechanisms to manage their data on cloud architectures [5]. With the increasing demand of the cloud, cloud becomes a multiuser network where multiple users can store their different type of data as per their requirement. Because of multiuser ability, Ou et al. [6] proposed an efficient security mechanism for cloud using location-based Scheme. In this when a user entered into cloud environment, LBS provider provides the information about the location of the user/data owner for only registered LBS users. Unregistered and revoked users were not able to use the services. When these Registered LBS users upload their data, it encrypts using hybrid encryption algorithm. The results proofs that the performance of this proposed LBS Query Scheme is better than others but it consumes more time. Fragmentation scheme is very popular now-a-days to provide security. Alsirhani et al. [8] proposed a security mechanism for cloud using fragmentation mechanism. In their fragmentation mechanism they introduced the concept of master and slave Clouds. In master cloud, all the data is stored after encryption using hybrid encryption algorithm where AES-CBC technique is used. Master cloud maintains the entire relation in one place through indexing. Then vertical fragmentation was implemented on this and creates a variable number of replicas of the columns that are stored in the slave clouds in encrypted form. The performance of this technique was evaluated on the basis of different parameters and achieved good results. In this work, they have not mentioned any fragmentation criterion. Manjula et al. [9] also worked on fragmentation mechanism but they divide their data after encryption which leads to data loss. The other fragmentation-based security mechanisms were proposed by various authors and were described in [10-17]. As per the results presented by these authors, fragmentation helps at higher level to provide security but the main drawback of the fragmentation is data loss. So, there is a requirement to develop an efficient mechanism for fragmentation which will help to prevent data loss and provide better security.

III. EFFICIENT FRAGSECURE FRAMEWORK

In this advanced era of technology, the use of Cloud reaches on its heights and the requirement of security is increases day-by-day due to increase in security breaches. A number of researchers work on the same and provides different frameworks and architectures for security. In paper [18], a secure cloud architecture is generated where data is divided into fragments and then each fragment is encrypted using a pair of keys generated at the client end for signature and decryption and other pair is generated for file block identifier to check the integrity of the data. This framework provides security but due to fragmentation data loss is there because the type of data may not be the same for each user and then here fragmentation increases the risks of data loss. To deal with this issue, a novel architecture is proposed for cloud environment in which data is fragmented on the basis of data type, size and other parameters and each fragmented block is encrypted using hybrid encryption algorithm. The detailed design of this proposed system is as shown in figure1. In this framework first input data is send to cloud server by a user/client of the cloud. Data may be of text type, image type or audio data. This data is when received by a cloud server then first it is passed through fragment module where fragmentation criteria (F.C.) is checked for each type of file and accordingly data will be fragmented into ‘n’ number of fragments. Then each fragment is encrypted using hybrid encryption module. These encrypted fragments are then mapped with the different servers located at different locations.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

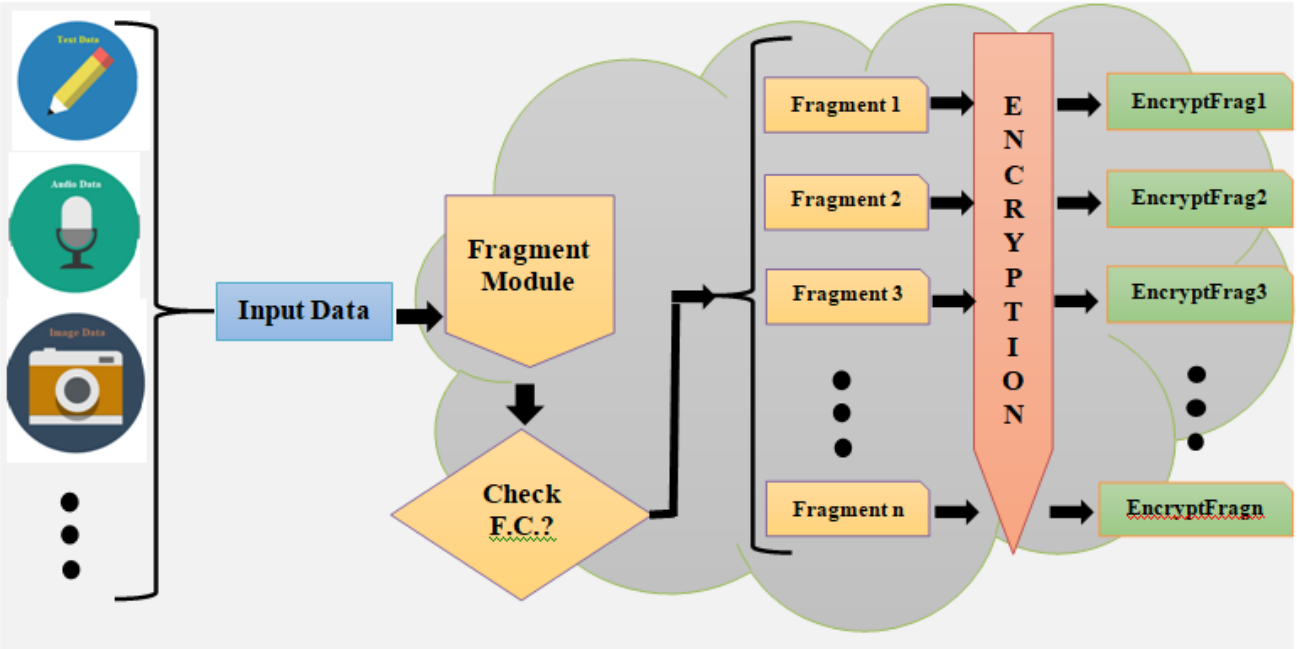

FIG. 1: PROPOSED FRAGSECURE FRAMEWORK

In this work, two modules play an important role (i) Fragment Module and (ii) Encryption Module. The detailed description of these modules is as given below:

Fragment Module: Fragmentation is the main concern and, in this work, the main focus is drawn on this module. Here first the type of data is checked means data is image, audio or text type because each type of data has different properties. Secondly, the size of the data file is also checked because it also affects the performance of the fragmentation module.

Algorithm 1: Fragment Module

Input: Data (i)
Output: Number of Fragments, Size of Fragment
Start
Upload Data File 'Data(i)'
Check F.C. (Fragmentation Criterion)
Check Type of Data
Type 1: Image (.jpg,.bmp,.tiff, and other Image Files)
Type 2: Audio File (.mp3)
Type 3: Text File (.txt, .doc)
Switch (Type (Data(i)))
Case 1:
If Size (Data (i)) is Large
Then number of fragments= (4x4=16)
Else If Size (Data (i)) is Medium
Then number of fragments= (3x3=9)
Else If Size (Data (i)) is Small
Then number of fragments= (2x2=4)
End of IF
Case 2:
If Size (Data (i)) is Large
Then number of fragments= 7
Else If Size (Data (i)) is Medium
Then number of fragments= 5
Else If Size (Data (i)) is Small
Then number of fragments= 4
End of IF
Case 3:
If Size (Data (i)) is Large
Then number of fragments= 6
Else If Size (Data (i)) is Medium
Then number of fragments= 4
Else If Size (Data (i)) is Small
Then number of fragments= 2

End of IF
End of Switch
Stop

Encryption Module: The main focus of this module is to encrypt each fragmented block and store these blocks on different servers along with its identification numbers.Here for encryption, hybrid algorithm is used where combination of RSA and ECC is used as hybrid [19]. The performance of this combination provides better security as analyzed. The detail process of encryption is as follows:

Algorithm 2: Encryption Module
Input: Fragmented Block (i)
Output: EncryptFrag(i)
Start
For Each Fragment Block
Do
Generate Keys using RSA Algorithm
Output (i) ←Encrypt Fragment Block (i) using Key
Generate Keys using ECA Algorithm
EncryptFrag(i) ← Encrypt Output(i) using Key
Stop

IV. SIMULATION ANALYSIS AND RESULTS

Toanalyse the performance of proposed framework, a local cloud environment is generated using .NET. In this local cloud environment, a user can login and store their data to the cloud server. The main focus of this work is to reduce packet loss which is due to fragmentation. So, the parameters used to analyse performance is Time, Size of data after encryption, and Data Loss. For analysis 200 files were uploaded on the server contains 100 text files, 60 image files and 40 audio files. All thesis files are of different sizes and total size of all the files is1.7 GB. Fragmentation is done using proposed mechanism and for comparison a random fragmentation mechanism [18] is also implemented. The simulation results of this implementation is as given below:

Time Analysis*:* Time can be measured for storing each file on server. Here Time can be defined as a time taken to store data on the server and total time can be calculated by adding the time of all files that are stored on the server. Total time can be calculated as:

$$Totaltime(T_{Total}) = \sum_{i=0}^{n} T_i$$

Testing has been done for these three methods on a dataset of 200 files. Where 100 text files,60 image files and 40 audio files has been uploaded to the cloud environment with two different methods and Total Time for storing data on server is as shown in figure 2.

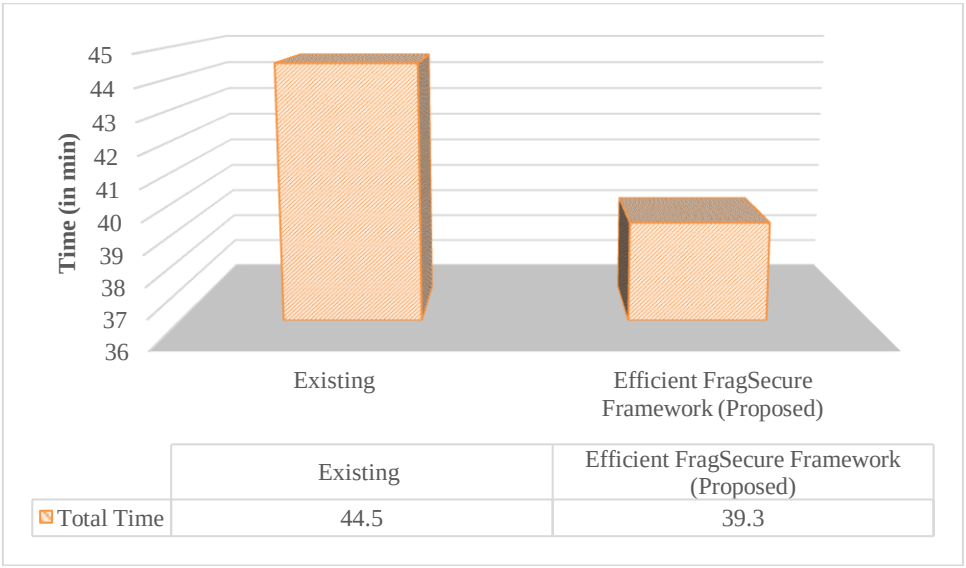

Fig 2: Total Time (in min)

In this proposed work, time taken to store data on a cloud server is less than the existing architecture because the fragmentation criterion is fixed in this according to the size of the data file but it is random in the existed framework. This will achieve 11.6% improvement as compare to existed framework and provide better performance.

Size:In this size of the data after encryption is calculated and compared. Testing has been done for these two methods on a dataset of 200 files. Where 100 text files,60 image files and 40 audio fileshas been uploaded to the cloud environment with two different methods and Original size of data is **1.7 GB**. The size after encryption is

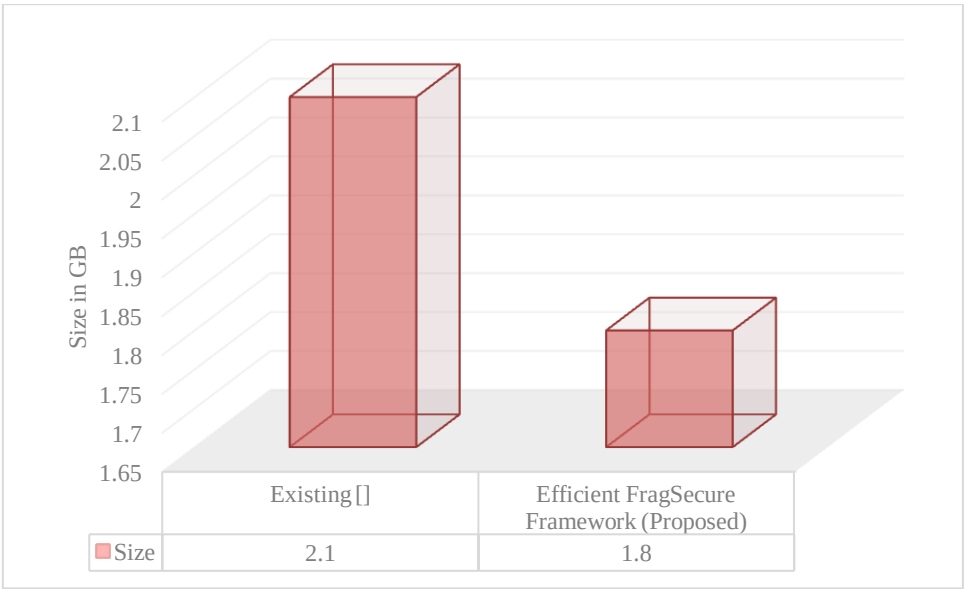

Fig 3: Encrypted Data Size (in GB)

This proposed work uses hybrid combination of the encryption algorithms where RSA and ECC is used. Both algorithms are asymmetric algorithms and generate public and private key. Public key is used to encrypt data and private key is used to decrypt data. The result of this proposed framework is improved by 14.2% in terms of encrypted file size.

Data Loss:In this work, the concept of fragmentation is used and when data is fragmented, data loss may be there. So, data loss will be calculated by comparing the size of data at cloud with the original size of the data. The formula used for calculating data loss is:

$$Data\ Loss = \frac{(Original\ Size\ of\ the\ Data - Size\ of\ Data\ at\ Cloud)}{Original\ Size\ of\ Data} * 100$$

The calculated Data Loss using proposed and existed framework is 6.9% and 19% respectively and is as shown in figure 4.

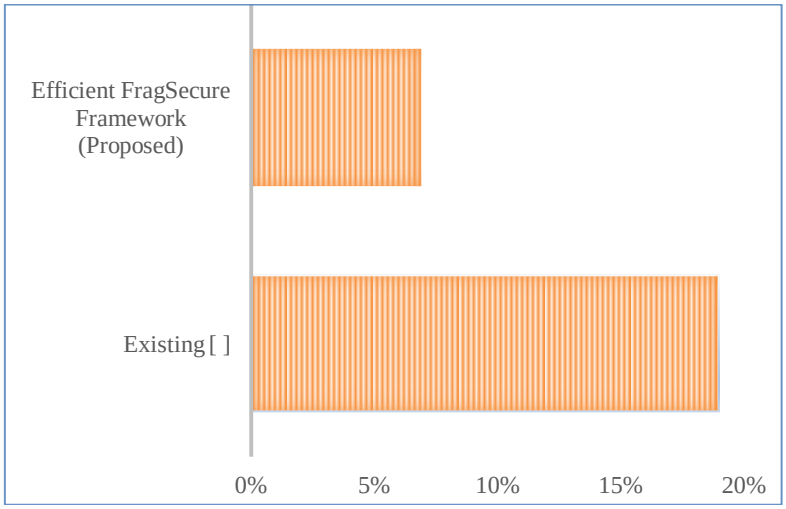

Fig 4: Data Loss in %age

V. CONCLUSION

In this work, an efficient framework for fragmentation and security is proposed. This framework is proposed to achieve the objectives to reduce data loss during fragmentation and provide high end security. For fragmentation, a fragment module is generated which decides the number of fragments and size of fragments on the basis of the original size of the data and for encryption, hybrid RSA and ECC algorithm is used which provide double encryption of the data. To analyze the performance of this proposed framework, a dataset of 200 different type of files is uploaded to the local cloud environment and results are calculated in terms of time, size and data loss and concludes that the performance of this proposed efficient FragSecure framework is better than the existed framework where random fragmentation mechanism is used along with the single encryption mechanism. This proposed approach helps to reduce the storage time as well as storage requirement by reducing the size of encrypted data with least data loss. The result shows the improvement by 12%, 14%, and 65% for time, size and data loss respectively which concludes the effectiveness of the proposed mechanism. In future, the testing of this proposed framework can be done using video files or files of large size and different formats.

REFERENCE

1. R. Saleem and O. Steen, "CLOUD COMPUTING'S EFFECT ON ENTERPRISES," Master's Thesis, 15ECTS , rep., 2011.
2. C. Yan and K. Kolehmainen , "CLOUD STORAGE SERVICES ," Thesis, rep., 2017.
3. N. Yadav and D. D. Samanta, "Data Security in Cloud Computing Using Biometrics ," Seminar Report, rep., 2013.
4. X. Liu, L. Fan, L. Wang, and S. Meng, "Multiobjective Reliable Cloud Storage with Its Particle Swarm Optimization Algorithm," Mathematical Problems in Engineering, vol. 2016, pp. 1–14, 2016.
5. K. Haufe, S. Dzombeta, and K. Brandis, "Proposal for a Security Management in Cloud Computing for Health Care," The Scientific World Journal, vol. 2014, pp. 1–7, 2014.
6. L. Ou, H. Yin, Z. Qin, S. Xiao, G. Yang, and Y. Hu, "An Efficient and Privacy-Preserving Multiuser Cloud-Based LBS Query Scheme," Security and Communication Networks, vol. 2018, pp. 1–11, 2018.
7. J. Li, J. Wei, W. Liu, and X. Hu, "PMDP: A Framework for Preserving Multiparty Data Privacy in Cloud Computing," Security and Communication Networks, vol. 2017, pp. 1–14, 2017.
8. A. Alsirhani, P. Bodorik, and S. Sampalli, "Improving Database Security in Cloud Computing by Fragmentation of Data," 2017 International Conference on Computer and Applications (ICCA), pp. 43–49, 2017.
9. S. Manjula, M. Indra, and R. Swathiya, "Division of data in cloud environment for secure data storage," 2016 International Conference on Computing Technologies and Intelligent Data Engineering (ICCTIDE16), pp. 1–6, 2016.
10. S. Liu, C. Zhang, and L. Bo, "Improve security and availability for cloud storage," 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS), pp. 382–387, 2016.
11. G. Priyadharishini, A. Sairamya, and W. Mercy, "Data Fragmentation In Cloud For Optimal Performance And Security ," International Journal of Advanced Research in Computer Science Engineering and Information Technology, vol. 4, no. 3, pp. 615–619, Mar. 2016.
12. "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security," International Journal of Science and Research (IJSR), vol. 6, no. 1, pp. 1223–1226, 2017.
13. A. Hudic , S. Islam, P. Kieseberg, and E. R. Weippl, "Data Confidentiality using Fragmentation in Cloud Computing," International Journal Communication Networks and Distributed Systems, vol. 1, no. 3/4, pp. 1–10, 2012.
14. T. Kalidoss, G. Sannasi, S. Lakshmanan, K. Kanagasabai, and A. Kannan, "Data anonymisation of vertically partitioned data using Map Reduce techniques on cloud," International Journal of Communication Networks and Distributed Systems, vol. 20, no. 4, pp. 519–531, 2018.
15. S. D. C. di Vimercati, R. F. Erbacher, S. Foresti, S. Jajodia, G. Livraga, and P. Samarati, "Encryption and Fragmentation for Data Confidentiality in the Cloud," Springer International Publishing Switzerland 2014, pp. 212–243.
16. R. Chavan and S. Y. Raut, "Cloud Security Solution: Fragmentation and Replication," International Journal of Advanced Research And Innovative Ideas In Education, vol. 2, no. 4, pp. 611–618, 2016.
17. A. Hudic, S. Islam, P. Kieseberg, S. Rennert, and E. R. Weippl, "Data confidentiality using fragmentation in cloud computing," International Journal of Pervasive Computing and Communications, vol. 9, no. 1, pp. 37–51, 2013.
18. B. Feng, X. Ma, C. Guo, H. Shi, Z. Fu, and T. Qiu, "An Efficient Protocol With Bidirectional Verification for Storage Security in Cloud Computing," IEEE Access, vol. 4, pp. 7899–7911, 2016.
19. G. P. Kanna and V. Vasudevan, "Enhancing the security of user data using the keyword encryption and hybrid cryptographic algorithm in cloud," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 3688-3693, 2016.

AUTHORS PROFILE

Ashima Naranghas completed her Btech, mtech and is pursuing PhD in the field of computer Science from various prestigious institutes of India. She has published 14 research papers in reputed journals and conferences and has guided students for projects from undergraduate and graduate courses. Sje is also an active member in the various professional bodies like IAASSE, internet society, SCIEI etc. She is the reviewer to various journals from her expertise field.

DrDeepali Guptahas completed her Btech, Mtech and PhD from the prestigious institutes and Universities of India. She has more than 50 national and international publications to her account and has guided many students for undergraduate, graduate and PhD courses. She is active member of various professional bodies like iei (india), iete, iste etc. apart from being editor-in- chief of mmu journal, she is editorial board member and reviewer of various journals. she has many awards and recognitions to her credit.

DrAmandeepKaurhas completed her Btech, Mtech and PhD in the field of Computer Sciences from the prestigious institutes and Universities of India. She has 10 national and international publications to her account. Her area of interest is networking, wireless sensor networks, algorithms and Cloud Computing.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication