ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 4, April 2016

# Blowfish Ciphering based Provable Multicopy Dynamic Data Possession In Cloud Computing

J.Sheeba Mercy[1], Dr.K.Ruba soundar[2], M.Piramu[3]
[1]PG scholar, PSR Engineering College, Sivakasi , Tamil Nadu, India
[2,3]Professor, Computer Science and Engineering, P.S.R. Engineering College, Sivakasi, Tamil Nadu

***Abstract*—Due to the rapid development of cloud computing and the increase in Cloud Service Providers (CSP), data outsourcing has become a trend in recent years. This enables the data owner doesn't require to update his data. However, it demands security to be sustained for the consumer to trust the service providers. In the proposed work, the data stored in the cloud is encrypted using the blowfish symmetric key ciphering approach along with the novel Map-Based Provable Multi-Copy Dynamic Data Possession (MB-PMDDP) scheme. It is the most secure method that uses the key size of 448 bits. The Message Authentication Code and the secure hash algorithm is applied to verify the data integrity of the system. The data owner need not update every copy, instead data in his cloud can alone be updated.Once the data is updated, then the MAC code also gets updated. The access to data is provided upon requests and corresponding permission from the data owner. The performance analysis of the proposed method is compared with that of Advanced Encryption Standard (AES). The evaluation showed improved security and integrity.**

***Index Terms* – Cloud Computing, Data Security, Multicopy Storage, Data Integrity, Blowfish, Advanced Encryption Standard (AES).**

## I. INTRODUCTION

Cloud computing has opened up in a huge way to service the online users with ample space for sharing and storing.

The cloud service providers has taken up many ventures to attract the users to land into their juncture. In order to accomplish this, the data security and integrity is the prime concern to the users. The mainservice models offered by the cloud computing are

- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- Software as a Service (SaaS)

All the services offered from the cloud and all the data that are stored in the cloud servers requires security features in order to trust the Cloud Service Provider (CSP). However SaaS demands more security. The data owners are always are at their edges if their data is being used as private datasets or if it is being sent to the third party without authorizations. Thus there exists cyber-trust demands in cloud services. The cloud storage has gained popularity for its low maintenance cost and due to their on-demand services among both the individual users and the corporate users.There are both merits and demerits in the cloud storage systems. The cloud storage enables the user to reduce the cost and resource of local data storage. The demerits of the cloud storage can be

- Loss of physical control
- Possibility of data theft

Although the security threats can be monitored by various encryption schemes available, the trust worthiness of the CSP for their services is still missing. Also the present consumers wants their data to be stored in multiple servers of various data centers. But this type of demand incur charges for storage in an infrastructure. However there is no proof that the CSPs have stored in multiple servers. There should be a guarantee that the CSPs do the service as stated in the service agreement. The main objectives required to be met by the service providers are

- There should be an evidence for the customers that the CSP store their data as agreed upon and are not cheated.
- The block level operations for dynamic data outsourcing
- An authorized users must have access to the file copies stored by the CSPs

These requirements can be satisfied for designing a reference model for proving the possession of dynamic single copy schemes. This is termed as Provable Data Possession (PDP). This PDP is an approach that helps the users to validate the data integrity over the remote servers. The challenge response protocol helps to aid the PDP model through verification of data generated by the data owners. The data owners send their file to the CSPs without having any local copy for themselves. This poses the threat to the user for their data security. Thus various research has come up to develop an efficient PDP approach.The outsourcing of data provides dynamicity of data for various applications. Data dynamism means that the data stored in the remote CSP servers has to be accessible to both the authorized users as well as to the users who was authorized by the data owners. Some schemes presented earlier have focused only on unchanged data in the cloud servers, they are called as static or warehouse data. The data which is dynamic can perform block level operations. The block level operations is the accessibility and editing ability of the data shared for insertion, deletion, appending, to perform modifications, to append data into the file. Thus an approach is required for quick, secure, convenient data storage with maximum capabilities without investing in many infrastructure. It also will not demand the need for software licensing or to appoint a

personal for the same. It ensures the external level security to the data. The demerits of the existing system

The proposed scheme incorporates Blowfish ciphering for encryption and Secure Hash algorithm based SHA1 for authentication. The SHA1 generates Message Authentication Code (MAC), which helps in the verification of integrity in all the replicas of the data stored in the cloud service provider. The MAC integrated with the encrypted data provides strong security by giving strict access rights only to the authorized users. The experimental results evaluate the performance of the proposed system.

The fore coming sections of this paper are structured as follows: Section II surveyed the classicalstyles for solving the security issues in cloud computing Section III provides an overall description of the Map-Based Provable Multi-Copy Dynamic Data Possession (MB-PMDDP) scheme using blowfish ciphering. Section IV shows the performance analysis of the proposed system. Section V presents the conclusion and future work of the paper.

## II. Related Work

*Barsoum and Hasan*[1] proposed a Map Based Provable Multicopy Dynamic Data Possession (MB- PMDDP) approach for addressing the challenges of Cloud Service Providers (CSP). The major steps of the work was

- It provided the customers with the proof that they store data securely with the right CSP
- It provided dynamic data outsourcing with block level operations
- It allowed the authorized users to access the data stored in the cloud by the CSP

The block level operations included block modification, insertion, deletion and appending of data as a blocks. Also in [2] stated another two methodologies for

- To prevent CSP to cheat the users by utilizing reduced storage with minimum copies.
- To provide dynamic data outsourcing with block level operations

Thus the work presented the security measure for the cloud users against the degraded quality of service by certain CSPs. *Bajwa*[3] focused on the solutions pertained to the issues of cloud computing systems, mainly of that of data security, leakage, availability and accessibility.*Shen and Tzeng*[4] suggested dual scheme for delegated integrity check. The schemes suggested were

- Personal health records based integrity check scheme
- Data retrieveability

These schemes was applicable for the data present in the hierarchical cloud. The performance of the proposed work was proved using its ability to proof unforgeability andin distinguishability. *Yang, et al*[5] constructed a novel design for effective public auditing. The proposed framework shared data over the cloud by preserving the identity and traceability. The blind signature approach was adopted to provide data privacy and to generate authenticators.*Wei, et al*[6] presented the efficient and dynamic multi copy possession scheme with their optimal features. The data owner can utilize Fully Homomorphic Encryption (FHE) algorithm for multi copy generation. It allowed dynamic block data operation. The public verification of third party auditor became possible with the proposed scheme. It was able to resist the forgery, other attacks and replacements.*Barsoum*[7] proposeda pairing-based provable multi-copy data possession (PB-PMDP) scheme,in which, the strategies to be followed for replication, security and integrity of outsourced data in the cloud were discussed. The creation of multiple copies of data was verified over the un trusted cloud servers. It gave the user with the access to data as well as to archive the data desired by the data owner. *Mukundan, et al*[8] presented Dynamic Multi- Replica Provable Data Possession Scheme (DMR-PDP) that focused on the dynamic files along with the static data files and to reduce the cost incurred in this proposed scheme. It ensured to check the honesty of the CSP.*Sookhak, et al*[9] reviewed the auditing of data in the distributed cloud network. The auditing was classified based on the erasure coding, network coding and replication. The study illustrated the uniqueness and similarities of various techniques along with the issues associated with the systems. Zhao, et al [10]introduced a fully homomorphic encryption algorithm to address the issue of security in cloud computing. The algorithm helped to provide security along with the information retrieval from the encrypted data. Thus the data storage and data transmission was safe. *Tan and Teh*[11] presented performance evaluation of the resources in the virtual machines by applying machine learning technique and linear regression analysis with reference to TPC-H benchmark data. The real data is not involved hence it was said to be secure during evaluation.*Huang, et al*[12] generated a novel code to work along with Dynamic Provable Data Possession (DPDP) scheme to overcome the data security problem persisting in the network. The dynamic operations of the proposed scheme is a memory adversary model that improved the system performance as well as the viability. *Du, et al*[13] formulated the Proofs of Ownership and Retrievability (PoOR) model for mutual validation of the network. Erasure coding was utilized in order to prove the recoverability and security of the system. The storage resource wasmaintained optimally using merkle tree and homomorphic verifiable tags.*Mohan and Katti*[14] proposed a new provable secure sigma Provable Data Possession (PDP) scheme to provide computation and communication without complexity. A challenge response protocol helped to transmit small and constant amount of data.*Sontakke and Manjrekar*[15] suggested multi owner with sharing approach. The work identified the corrupted data copy and corrected it before performing the dynamic operation. The work allowed many owners for the single data on the sharing basis. It verified the data integrity and reconstructed the corrupted copies of data using the Attribute based encryption standard.

The earlier Advanced Encryption Standard (AES) uses a combination of Exclusive-OR (XOR), octet substitution, row

and column rotations, and a mix column. AES allow block sizes of 128, 168, 192, 224 and 256 bits, and a key size of 128 bits. Each byte in the matrix is updated using an 8 bit substitution box,which is derived from the multiplicative inverse of nonlinear properties. The inverse function is combined with an invertible affine transformation to avoid attacks based on simple algebraic properties. The bytes in each row are shifted in a cyclic manner using a certain offset, by keeping the first row unchanged. The demerits of the existing system includes

- The key size of the existing AES system was too small
- Data stored in the CSPs are prone to insecurity
- The key size of the MAC, MD-5 is lower than the Sha-1 algorithm

## III. Proposed Method

The proposed blowfish encryption based PDP scheme involves data owner registration to the cloud service. Their data to be uploaded are split into smaller data and is being uploaded. A MAC is generated for every split data. The data can be accessed by the data owners upon their request. The accessibility is governed with the blowfish encryption scheme. The block level operations can then be performed by the users.Fig. 2 illustrates the general architecture of the proposed system. The architecture sequences the steps followed for the proposed system. The data owner selects the data and the split data has their MAC generated. Whenever the data owner needs to modify the data stored in association with the CSP, the request signal is sent to the CSP.

The data transmission and the data reception was carried over with the specific encryption scheme. The encrypted data can be retrieved by the user with the keys shared by the data owner among his trusted users. The data retrieval is susceptible to MAC verification for enabling secure data access.

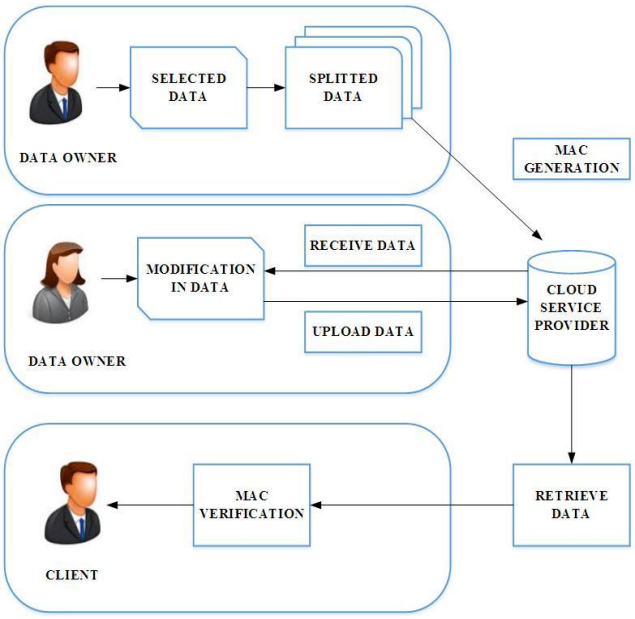


Fig.2 Architecture of the proposed system

The modules of the proposed system includes

- Data Owner Registration
- Data Uploading
- Users Request
- Users Accessing Data

Each step of the proposed system can be visualized in the following subsections in detail. Fig. 2 depicts the flow diagram of the proposed system. Through the flow diagram it is understood that the blocks of dynamic data stored by the data owner can be modified, inserted, deleted, appended following the brief but strong security check. Thus the flow guarantees the storage of multiple copies over diversified cloud data centers are accessible. Thus, verification of the cloud service providers will create the trust for the CSP among the cloud users. The file copies stored at different data centers are chargeable, hence the right to prove their genuine service is truly a useful scheme for practical implementation.

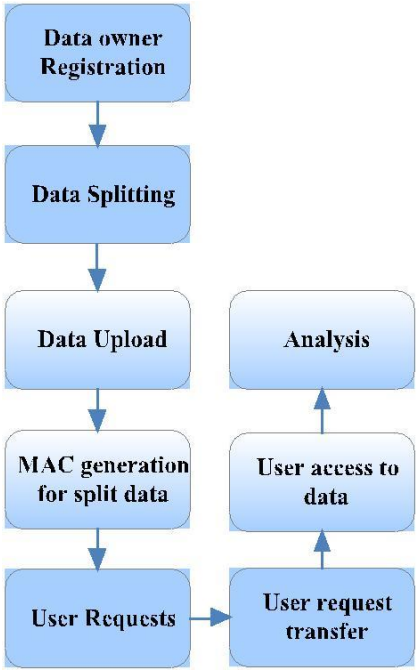


Fig.2 Flow diagram of the proposed system

1. *Data Owner Registration:*

In this first module, the data owner requires to register their details in the proposed system. Then the registered member is allowed to select the data. The data are then split into smaller data. A data owner or an organization who originally possessthe sensitive data to be stored in the cloud. The Cloud Service Providers is the ones who manages the Cloud Servers (CSs). They provide paid storage space on its infrastructure to store the owner's files. The authorized users are a set of owner's clients who have the right to access the remote data.

2. *Data Uploading:*

A MAC ID is generated for the splitted data. Then the data are encrypted and uploaded into the servers of cloud service provider. Consider a data owner possessing a file, F. Let thefile be considered to have'm' blocks of data and the CSP offers to store 'n' copies in a set of {F1,F2,… Fn} of the owner's file on different servers. The data are stored in different servers to prevent simultaneous failure of all copies.

The storage is offered to the users in exchange of a stipulated fees. The fees is chargeable as the amount of data stored per month (GB/month). The number of copies requirement is based on the nature of data. For the critical data that cannot easily be reproduced, more copies are needed. Scalability is also a greatest factor to be considered for an effective data loading. In order to achieve a higher level of scalability,

- The critical data must be replicated on multiple servers across multiple data centers.
- The Non-critical, reproducible data are stored at reduced levels of redundancy.

The pricing model of every service provider is with reference to the required number of data copies. To ensure the data confidentiality, the data owner is enabled to encrypt his data before outsourcing to CSP. After outsourcing all n copies of the file, the owner cancommunicate with the CSP to perform block-level operations on all copies. These operations may be to modify, to insert, to append, and to delete specific blocks of the outsourced data copies.

*3. Users Request:*

The service provider look for the request message from the data owner before enabling any block level operation to be performed by both data owner and the data owner authorized users. It is assumed that the communication between the data owners and the authorized users are authenticated and the keys are mutually shared between themselves. Upon receiving the request from the data owner, the CSP provides access to the data by sending a copy to the user from any of the data centers. The data can be decrypted by the shared key of the client and the data owner. The data can be received along with the MAC for every data access request given by the user.

*4. Users Accessing Data:*

The access pattern uses blowfish algorithm. The blowfish algorithm is the symmetric key encryption scheme that have same key for both encryption and decryption. The user receives key from the data owner. They get the encrypted data and decrypt the message using the shared key to view the data. The storage model used in this work can be adopted by many practical applications. The access to the copies of data is liberal for the data owners. With the proposed scheme, the data owner can archive and access the data from the CSPs as well from the data of remote servers.

Thus the proposed system provides well efficient structure with the following advantages

- Efficient hardware implementation possible
- It does not require any licensing
- Crypto-analysis of blowfish algorithm is well explored
- Faster execution

## IV. Performance Analysis

The proposed work uses blowfish algorithm which is a symmetric block cipher that can replace the existing algorithms DES and AES effectively. It has a block size of 64-bit and their key length varies from 32 bits up to 448 bits. The blowfish based scheme is evaluated to be faster than the existing standards for encryption. The work uses Standard Hash Algorithm, SHA1 for authentication. The performance of the novel scheme,MB-PMDDP using blowfish encryption algorithm is analyzed based on the following parameters

1. Encryption time
2. Execution time
3. Computation time and
4. Corrupted percentage

These parameters are evaluated for the proposed MB-PMDDP system and the existing provable possession of dynamic single copy system to prove the high performance of this novel scheme using blowfish algorithm.

1. *Encryption Time*:

The time taken by the system to encrypt a data into areadable format is known as encryption time. The unit of the parameter is given in seconds. The following Fig 3 shows the analysis of the Encryption time of the proposed blowfish based system with respect to existing AES system.

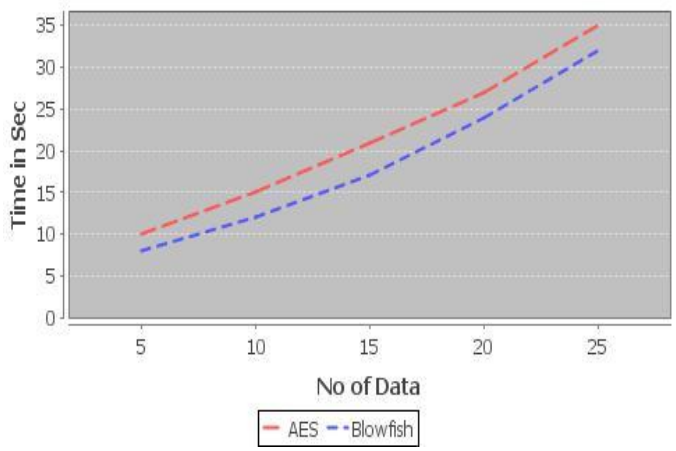


Fig.3 Encryption time Comparison

2. *Execution Time:*

It is stated as the total time spent for running a specific computation. The execution time is evaluated in order to analyze the speed of the processing of the whole application. It has to be maintained as low as possible. As per the experimentation performed over the proposed system and the existing system, it is proved that the proposed system takes lesser time than the existing schemes. Fig 4 illustrates the analysis report of execution time taken by both the schemes.

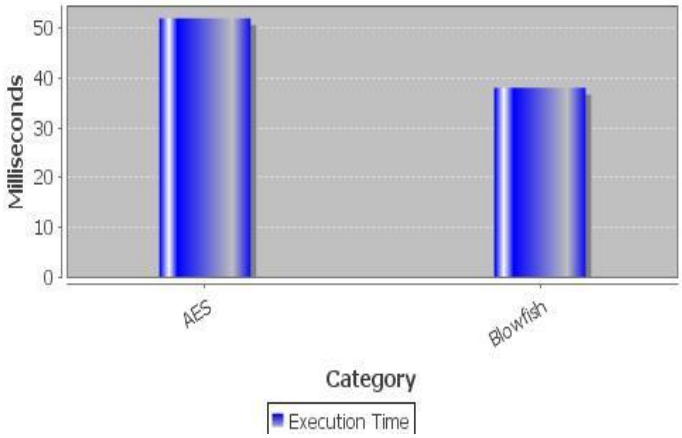


Fig.4 Execution time Analysis for the existing AES and proposed blowfish algorithms based PMDDP

*3. Computation time:*

The computation time also known as running time is the total amount of time required to perform a sequence of computations designed to execute a specific task.It is also called as the time complexity of an algorithm. It is computed by determining the amount of elementary operations performed by the proposed scheme. The computation time may vary based on the type of data, size of data and the number of replications of copies required by the user.The computations must be simple and should not be complex for the system to perform the computation with ease within the stipulated time. Fig 5 shows the comparison result of computation time of the proposed MB-PMDDP with the existing provable possession of dynamic single copy scheme.

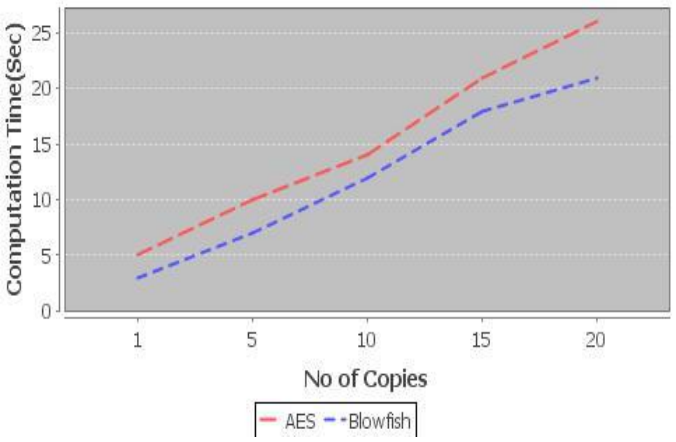


Fig.5 Comparison of Computation time of AES based PMDDP and blowfish standard algorithms

*4. Corrupted percentage:*

The amount of data getting corrupted due to the adapted processing schemes are evaluated. Due to the dynamic nature of data stored over the cloud system, the data tends to get corrupted. It is considered to occur because of common error that happens due to reading, writing, during storage, during transmission and processing. This unintentional data loss may incur greater loss of reputation. The outputs are graphically illustrated in the Fig 6. From the results it has been proved the proposed scheme have less corruption compared to the existing system.

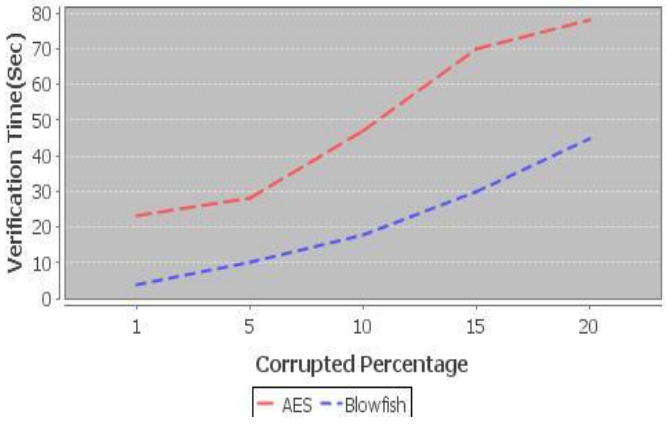


Fig.5 Comparison of level of corruption in proposed AESbased PMDDP and blowfish standard algorithms

## V. Conclusion and Future Work

The cloud services are being sought by the cloud users due to the low cost, minimum management strategy requirement. Thus large amount of private data are stored in recent decade. Thus, Cloud Service Providers (CSPs) offer Storage as a Service (SaaS) for providing a paid service for local data storage. The proposedMap-Based Provable Multi-Copy Dynamic Data Possession, MB-PMDDP uses blowfish encryption reduces the cost of storage and computations involved in it. The user needs to register in the proposed scheme and upload the data that needs to be stored in the cloud servers. The data are split and coded using SHA1 to have good data integrity. The blowfish encryption enables the data owner to protect and share keys for authenticating the authorized users. The performance metrics were evaluated and the graphs supporting their fast execution, encryption, computation are presented and the corruption during multiple copy generation is lower than earlier methods.

## VI. REFERENCE

[1] A. F. Barsoum and M. A. Hasan, "Provable multicopy dynamic data possession in cloud computing systems," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 485-497, 2015.

[2] A. F. Barsoum and M. A. Hasan, "On Verifying Dynamic Multiple Data Copies over Cloud Servers," *IACR Cryptology ePrint Archive*, vol. 2011, p. 447, 2011.

[3] M. S. Bajwa, "A Concern towards Data Security in Cloud Computing," *International Journal of Computer Applications*, vol. 114, 2015.

[4] S.-T. Shen and W.-G. Tzeng, "Delegated integrity check for hierarchical cloud data," *Journal of Computer Security*, vol. 23, pp. 471-508, 2015.

[5] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," *Journal of Systems and Software*, vol. 113, pp. 130-139, 2016.

[6] J. Wei, J. Liu, R. Zhang, and X. Niu, "Efficient dynamic replicated data possession checking in distributed cloud storage systems," *International Journal of Distributed Sensor Networks*, vol. 2016, 2016.

[7] A. F. Barsoum, "Replication, Security, and Integrity of Outsourced Data in Cloud Computing Systems," 2013.

[8] R. Mukundan, S. Madria, M. Linderman, and N. Rome, "Replicated Data Integrity Verification in Cloud," *IEEE Data Eng. Bull.*, vol. 35, pp. 55-64, 2012.

[9] M. Sookhak, A. Gani, H. Talebian, A. Akhunzada, S. U. Khan, R. Buyya, *et al.*, "Remote data auditing in cloud computing environments: a survey, taxonomy,

and open issues," *ACM Computing Surveys (CSUR)*, vol. 47, p. 65, 2015.

[10] F. Zhao, C. Li, and C. F. Liu, "A cloud computing security solution based on fully homomorphic encryption," in *16th International Conference on Advanced Communication Technology (ICACT), 2014*, 2014, pp. 485-488.

[11] C.-H. Tan and Y.-W. Teh, "Secure Hardware Performance Analysis in Virtualized Cloud Environment," *Mathematical Problems in Engineering*, vol. 2013, 2013.

[12] K. Huang, J. Liu, M. Xian, H. Wang, and S. Fu, "Enabling dynamic proof of retrievability in regenerating-coding-based cloud storage," in *IEEE International Conference on Communications Workshops (ICC), 2014* 2014, pp. 712-717.

[13] R. Du, L. Deng, J. Chen, K. He, and M. Zheng, "Proofs of Ownership and Retrievability in Cloud Storage," in *13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE* 2014, pp. 328-335.

[14] A. Mohan and R. Katti, "Provable Data Possession Using Sigma-protocols," in *IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2012* 2012, pp. 565-572.

[15] M. P. V. Sontakke and M. A. A. Manjrekar, "Provable Multi-Copy Dynamic Data Possession With Multi-Owner In Cloud Computing System."

**Author's Information:**

J.Sheeba Mercy received in BE degree in Unnamalai Institute of Technology, Anna University, Tamilnadu ,India and PG scholar in PSR Engineering college, sivakasi, Tamilnadu ,India.

Dr.K.RubaSoundar received the A.M.I.E., degree in Computer Science and Engineering from The Institution of Engineers (India) in 2000. He received the M.E., and Ph.D., degrees in Computer Science and Engineering from Anna University, Chennai in the year 2004 and 2010 respectively. Currently he is a Professor in Computer Science and Engineering Department of P.S.R. Engineering College, Sivakasi, Tamil Nadu, India. He has authored / coauthored over 85 research articles in various Journals and Conferences in the areas of Image Processing, Wireless and Wired Networking.

M. Piramu received the BE degree in A.K.C.E. Krishnan Kovil-M.K.University, Tamil Nadu, India and Master's degree in MepcoSchlenk Engineering College, Sivakasi, Tamil Nadu, India. Currently she is a Professor in Computer Science and Engineering Department of P.S.R. Engineering College, Sivakasi, Tamil Nadu, India.