International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-11, September 2020

Optimization of System Framework for Secure Communication and Data Virtualization on Cloud Computing.

Nikita Kayarkar, Uday Singh Kushwaha, Prashant Richhariya

Abstract: ***The consequent deployment of vital infrastructure to provide the secure communication and virtualization not only rectifies the challenges and difficulties but also benefits with saving the process of digitization. With a bang in evolution of cloud computing the uniqueness of every organization affects the virtualization of its information communication technology and applications. The answer for such organizations is to stipulate the precise cloud computing model equivalent to the deliberated and operational goals. This research article emphasized at budding and optimizing a framework for virtual infrastructure and cloud computing model to support the organization stakeholders. Moreover it also improves the cloud security with a protected virtual infrastructure and communication model with better performance. On account of data storage security necessities and distinctiveness of cloud computing environment, a method for secured data & storage based on dynamic allocation and access control mechanism is presented. Dynamic resource allocation is applied for resource utilization that focused on data virtualization and memory virtualization, for protection and access control a modified KPABE algorithm is integrated. The combination of these methods resulting on the optimize resource use, centralizing of storage. The implementation and comparison of results revealed that the proposed modified KP-ABE has performed effectively than the other security standards and especially for resource utilization. The proposed method serves for efficient data storage, access control solutions and computation in cloud environment.***

Keywords: Access Control, Cloud Computing, Data Security, Data Storage, Dynamic Resource allocation, Virtualization, Virtual Infrastructure

I. INTRODUCTION

Cloud computing is eminent technologies that persuade numerous routine activities. It is very valuable due to its distinctive and elite properties. Since its uniqueness and openness make security an inimitable significance. Various cloud technologies has developed in sight with the security concerns for cloud service providers and its users.

Cloud Service Models-There is cloud service model present that offers various services with multiple level of security. These services are IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service) where IaaS is the lowest level services and inherits the abilities of its upward stack service model together with the security and risk issues. Among the three IaaS (Infrastructure as a Service) is an instantaneous computing infrastructure, stipulated and administered over the internet, researchers found the lowest integral levels of security and integrated functionality in it [1]. The Iaas is an on demand service and deals with the infrastructure hence rapid scales up down takes place. It reduces the expenses, complexity and management of physical resources that deals with an infrastructure of an organization. Each service model deals with pay as you go for what you use. **Virtualization**-The resources are provided to the customers or stakeholders with the technological revolution known as virtualization. The virtualization offer functional environment from abstract resources and split the utility from principal hardware. Virtualization is the key element of cloud computing for endowing with computing and storage services [2]. In cloud environment the virtualization is the responsibility of virtualization layer 4 that permits the workloads to access the storage without knowing about the information where the data stored, how it is stored and what kind of storage device is keeping the data.

Background-In addition with these features cloud computing is capable to offer the functionalities of computing such as virtual hardware storage, software and services without high investments in managing the hardware or involvement in the technical complexities. Data storage and computing are the two fundamental services offered by the cloud environment [1,2]. Though, there are still numerous troubles to be determined for personal users and enterprises to store data and locate applications in the cloud computing environment. Data security is the chief obstacle in acceptance which companions with issues like trust, privacy, compliance and legal matters. Towards the reliability and adaptability of cloud environment for the users and enterprises various security issues should be rectified primarily [3]. While it's a prerequisite to attain the confidence of users to accept some technology necessitates a trustworthy environment. Data protection, data storage and data security are the vital aspects to make cloud computing flourishing technology and to reach the users trust. Numerous techniques for data protection and security together with the efficient and secure storage are available, even though additional enhancement is needed.The major security issues are a superior storage agreement, requests to sustain simultaneous modification by multiple users to provide reliable storage agreement.

Revised Manuscript Received on September 30, 2020.
***** Correspondence Author
Nikita Kayarkar*, Student Computer Science Engineering (M.E. 4th Sem) Indore Institute of Science & Technology, Indore (M.P.)
Uday Singh Kushwaha, Asst. Professor Computer Science Department Indore Institute of Science & Technology, Indore (M.P.)
Prashant Richhariya, Asst. Professor Computer Science Department Indore Institute of Science & Technology, Indore (M.P.)

A storage area was proposed which assures Fork-Join-Causal-Consistency and eventual consistency and successfully confront the attacks like discard of data[3].It also grant support in the accomplishment of further safety protections in the trusted cloud storage environment. A safe and reliable trusted cloud environment SPORC proposed in the early 2010 that endows with real time interaction and association for multiple users and the untrusted cloud servers are only able to access the encrypted data.

Due to mass computation at the client side the operation continues inadequate support [4].Even as analysis of data and information a compulsory precondition of any organization is compact processing cost and data storage. For a verdict, until and unless the trust is built between the cloud service provider and its consumers no data is transferred to the cloud by any organization. To attain supreme level of data security in the cloud there are still several gaps to be filled. This research work focuses on the data security and privacy along with data storage virtualization and use in the cloud.

The purpose of this work is to develop a frame work and optimize the prerequisites of a principally strong and efficient access control scheme. The scheme must lessen the security concerns of cloud environment with the improved trust copious cloud based applications along with various service segments. With these projections the focal points of our work are to enhance cloud security and felicitate with better performance algorithm with secure and time constraint communication together with a secure virtual infrastructure that provide efficient access scheme and reduced data storage configurations.

II. RELATED STUDY

There are assorted distributed systems where a user is only proficient to access the data if the user posses some credentials or attributes [5]. To enforce these approaches that intervene the access control and offers a trusted server to store the data. Despite the fact that the stored server data is compromised then the confidentiality of data will be compromised. Earlier Attribute Based Encryption [6] systems employed attributes to illustrate the encrypted data and construct policies into user's keys; The user credentials and party encrypting data identifies a policy for who is able to decrypt based on the system attributes. The notion of this scheme is in close proximity to conventional access control methods such as Role-Based Access Control (RBAC)

Consequently there is a sturdy necessity of a system for distinguishing complex access control on encrypted data among secure data virtualization [7,8]. The description of ABE scheme and data virtualization in cloud computing is discussed here with different combination of schemes for security which could be a point of reference for understanding the assortment of ABE system. In 2005, fuzzy identity based encryption technique was visualized by Sahai and Waters [5] as the first Attribute Based Encryption scheme in which a set of recommended attributes is considered as uniqueness and it obtains both cipher text and recipients. The data can be accessed by only the recipients who have similar attributes to the fuzzy identity.

Usually there are two major category of attribute-based encryption schemes that are widely used: Key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE) [5,35]. The figure 1 below gives the categorization of ABE scheme. In the KP ABE scheme the secret key of user are formed with reference to an access tree which depicts the privilege range of the user accompanied by the encryption of data over set of attributes [5].

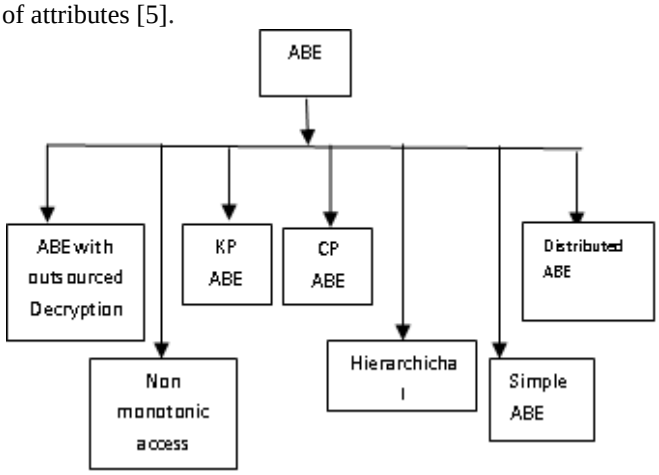

Fig 1: Categorization of ABE scheme.

On the contrary CP ABE employs the set of attributes for user's secret key generation and utilizes the access trees to encrypt data [9].ABE can be employed for log encryptions, rather than encrypting every part of log with keys the encryption of log can occur with attributes that are equivalent to the recipient attributes. The authors [10], [11] put up outsourcing of frequent computation troubles and preserve the privacy of input file, they'll be modified as outsource decryption in ABE systems. Though, the schemes proposed in [10], [11] use Gentry's fully homomorphic encryption system [12] as a constituent, and therefore the overhead in these schemes is presently overlarge to be matter-of-fact [13]. Parno et al. [23] set up a crucial connection between verifiable computation and ABE. They illustrated an approach to construct a verifiable computation scheme with public delegation and public verifiability from any ABE scheme and the way to construct a multifunction verifiable computation scheme from the ABE scheme with outsourced decryption presented in [16]. Goldwasser et al. [15] offer a concise functional encryption scheme for common functions, and show that, by substituting the ABE scheme used in [14] with their concise functional encryption scheme, one can achieve a delegation scheme which is both widely verifiable and secret, in the sense that the prover doesn't find out anything regarding the input or output of the function being delegated. Of these schemes [10,11,14,15] specialize in delegating general functions, and aren't sufficiently efficient for the matter at hand.

Tianyi et al [17] explored an optimized coRBAC model for cloud environment which inherits the features of earlier RBAC model and distributed RBAC (dRBAC) and provide advance access control system for services hosted on cloud environment. This model attained the reduced time and space complexities of access control system in conjunction with secure connection establishment, improved certification process, and setting up multilevel cache.

Al-Attab Basel et al [18] the author reiterated the current and trusted role-based access control models extracted from the literature and on foundation of security features a comparison on existing model is characterized.

The lowest privilege standards, policy management, flexibilities of configuration, scalability and separation of duties are a few of the features utilized for the study. This relative study assists in variety of appropriate cloud computing model for organization and enterprises where role based control model (RBAC) is bring into play for their internal network.

The author proposed a framework and an illustrative assessment of RBAC models for cloud environment focused on conception, fundamental components and architecture of trusted models along with analysis criteria of security features that each model can offer. The conclusion came up with Access Control for Cloud Computing (AC3) Model best assemble the cloud access control necessities and guarantees secure allocation of resources between probable untrusted tenants. Further enhancement and valuation of RBAC for secure access and network system for cloud computing is recommended as future work.

T shashank et al [19] offered a better method of two party key issuing protocols with weighted attribute that guarantee both Key authority and Cloud service provider unable to identify the entire secret key of an individual user. To increase the expressive power of an attribute from binary to arbitrary state with simplified access policy the weight of attribute is introduced.

The Proposed weighted attribute CP-ABE method stated bigger attribute space than the existing CP- ABE method. While the CP-ABE has only 2n possibilities of elements, the improved weighted CP-ABE can have n2 different possibilities. Hence this technique provides enhanced confidentiality and privacy of data in cloud environment besides the key authority, cloud service providers with outsiders. A reduced encryption complexity of a cipher text with low cost of storage is also achieved.

Saravana et al [20] set up the combination of digital signature, hash functions and an asymmetric encryption scheme to propose a new encryption scheme with fundamentals of (ABE) Attribute based encryption. The author found it efficient for critical cloud applications because of multiple steps and every step is an instance per call server and once the authentication is unsuccessful it doesn't shift to the next level. It involves a dual authentication with digital signature and a public key then the secret key is generated. Therefore the decryption of data is difficult. It has some overhead of time due to multiple steps in encryption and decryption but as per prior security concern it is negligible.

Gone Sowjanya et al [21] established a recognized characterization and security model for CP-ABE with user revocation. The author constructed a concrete ciphertext-policy attribute based encryption (CP-ABE) scheme which is CPA secure based on divisible computation Diffie-Hellman (DCDH) assumption. To defend against collusion attack, a certificate is embedded into the user's private key. The reason behind this is to unable the malicious user and revoked users to generate a valid private key by combining their private keys. To lessen the computation burdens of a user an outsourcing of high computation cost to Encryption cloud service provider (E-CSP) and Decryption cloud service provider (D-CSP) is activated. By this outsource technique the computation cost for local devices almost lowered and fixed. The overall analysis of various schemes interpret that due to the encryption of attributes rather than the original data ABE is more secure than any other encryption scheme the weaknesses of ABE scheme is the exclusiveness at the decryption of data, expensive cost of communication, computation cost for users[21]. Throughout the study, we examined that as a few of the security and access control issues are still exist in cloud computing environments that can be exposed by presented techniques, several others have specific properties associated with virtualized infrastructure, resource utilization and efficient communication with control access but there is a strong need to provide a thriving approach which resolves these problems. Our work focused on the optimization of the system and to produce an efficient algorithm that improves the security and data storage problems.

III. PROPOSED SYSTEM

The proposed system is focused on secure data sharing and decentralized access control. The aim is to model an effective algorithm which enables secure and timely data sharing with less complexity of time. To resolve the data storage problem with resource utilization the existing KP-ABE algorithm is modified with dynamic resource allocation algorithm.

Block diagram and Flow Chart of proposed System- The User send resource allocation list to the resource allocation manager over the public cloud. Firstly the request is send to the interface agent that has idea about the resource repository and it forward the allocation list to the resource manager. Resource allocation manager draw on the dynamic allocation algorithm to allocate the resource and grant the data virtualization. Block diagram and flow chart of proposed system is shown in below figure.2 and 3.

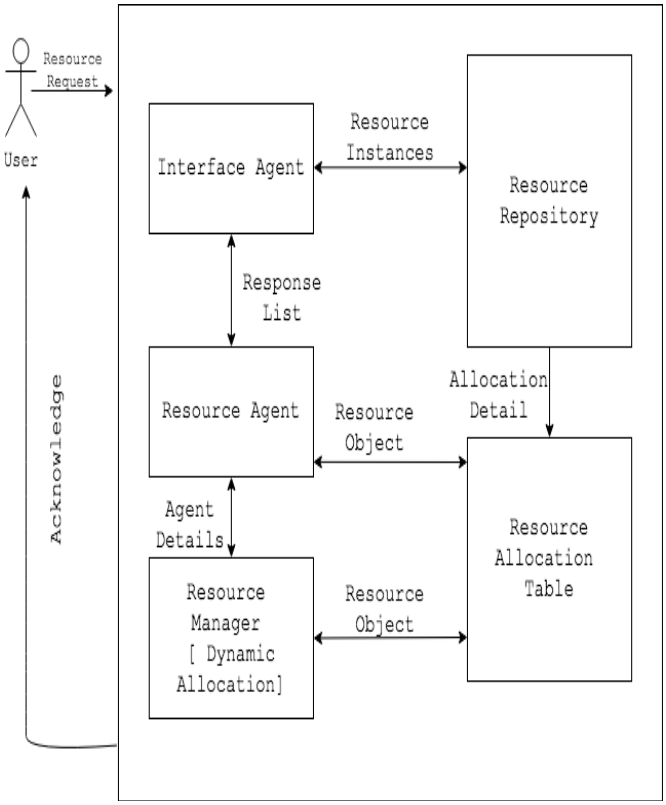

Fig 2: Block diagram of proposed system

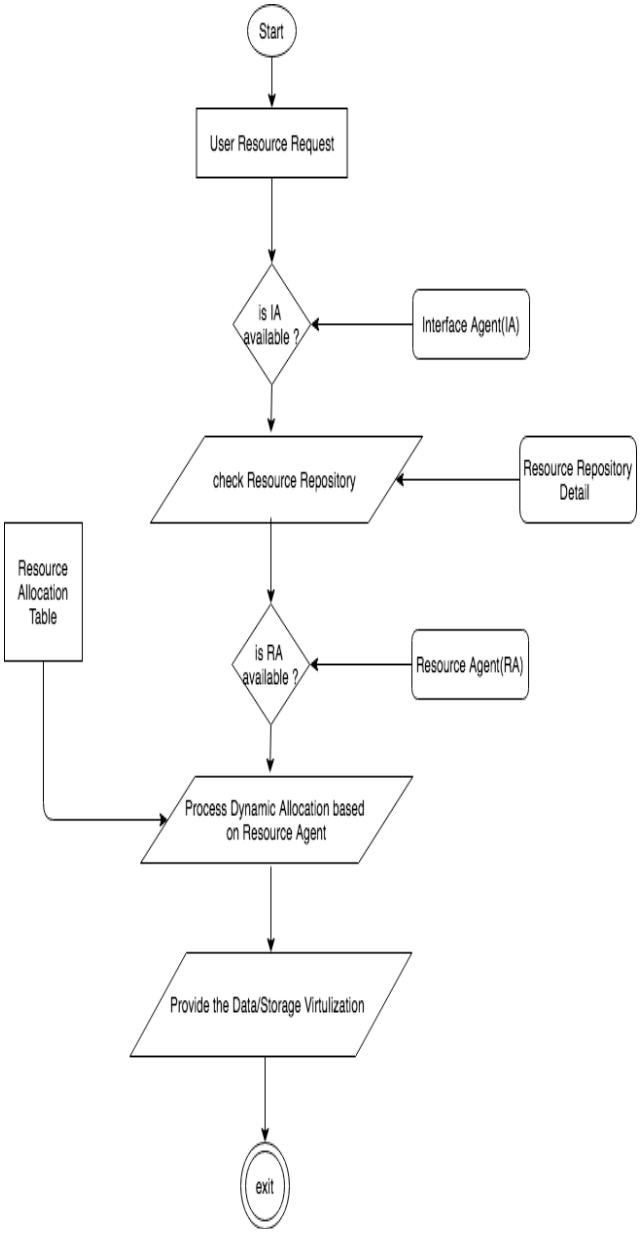

Fig. 3: Flowchart of proposed System

Virtualization- Several virtualization techniques are available that have fundamental components of distributed computing innovation and uses the abilities of distributed computing without limit. Virtualization techniques are divided in the following categories.

- Data Virtualization
- CPU Virtualization
- I/O Virtualization
- Storage Virtualization
- Network Virtualization
- Server Virtualization
- Desktop Virtualization
- Application Virtualization
- Memory Virtualization
- Para Virtualization

Our work focuses on data virtualization and memory virtualization.

In below figure 4 shows data virtualization, CPU virtualization, I/O virtualization with the methodology. Dynamic allocation is the major process in Data virtualization, CPU virtualization, I/O virtualization.

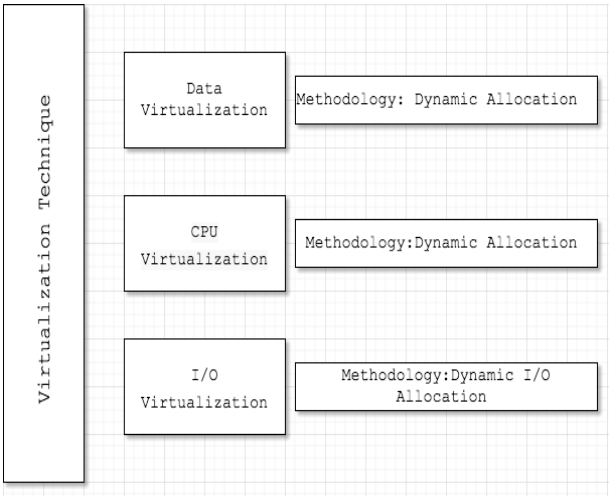

Fig 4: Virtualization techniques

Dynamic Resource Allocation- Dynamic allocation is a memory management technique where throughout the execution a program can request and return memory. Whenever there is a requirement of memory for a virtual machine, the available pooled memory on a physical host is distributed among the VMs that are operating on the host [22]. The allocation of memory occurs only if the virtual memory is not using the complete memory. The server resources can be capitalize according to the business needs with utilization, unmatched flexibility, performance by allocating moving server loads from one virtual workspace to the next. The figure 5 shown below has the consumers and data sources with virtualization methodology.

Preconditions- The proposed algorithm for dynamic resource allocation is based on the preconditions:

- Resource Repository
- Resource Table
- Resource Allocation table
- Interface Agent List
- Resource Agent List

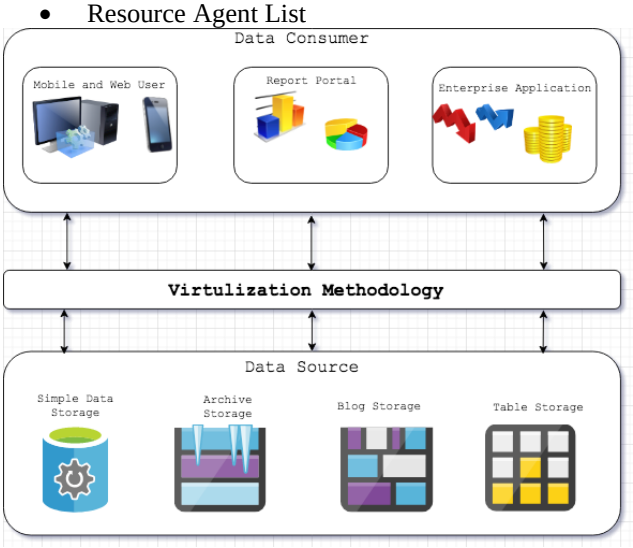

Fig. 5: Data sources with virtualization methodology

Key Policy Attribute Based Encryption (KP-ABE) Attribute-based encryption (ABE) is the contemporary cryptographic technique having competent tools for secure data sharing and distributed access control.

Key-policy attribute-based encryption (KP-ABE) is a considerable type of ABE. The key based encryption is a sort of public key encryption which have cipher text and a secret key of user dependent upon the attributes of a user and the deciphering is only achievable if the attributes of cipher text matches the set of user key attributes.
In KP-ABE, the data encrypted over a set of attributes based on the access tree, the user's secret key generation takes place which discovers the privileges and scope of the concerned user. The figure 6 correspond to the encryption technique here, the user here provides his attributes for e.g. his illness which can be fever, diabetes etc., name of the hospital like A,B,C,D, his gender i.e. male or female, his race i.e. Asian, black or white.

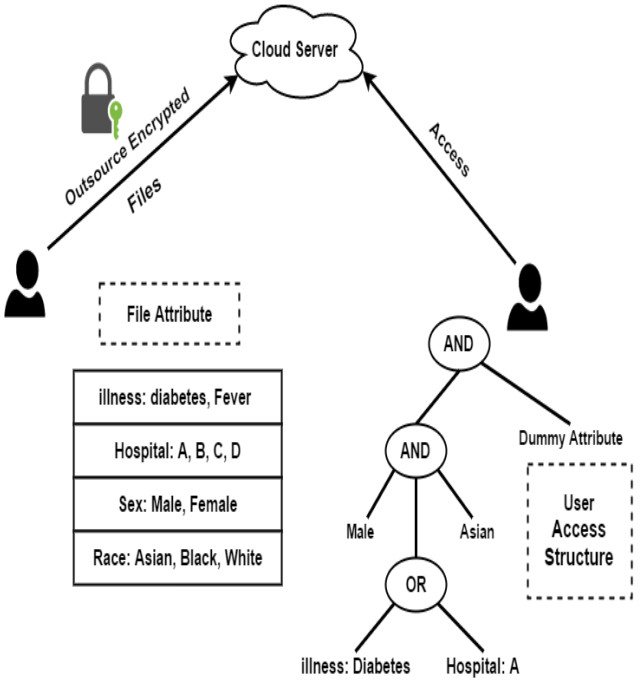

Fig 6: Attribute based Encryption

Below are the some steps needs to be followed for verifying the applicability and operations of proposed Modified KP-ABE. These are:
Step 1: Do login to the system by some defined user id and password; it could be recreated by using sign up function.
Step 2: Based on this user elements and some other attribute of the user, the system will generate the various intermediate keys with fixed size.
Step 3: User can generate composite key after verifying all the generated keys. User can view the various generation factors from which comparison can be made with existing key generation methods.
Step 4: User can upload the file and apply homomorphic encryption on this using above generated key.
Step 5: During this encryption some other factors related to the effectiveness of the approach are used for comparison purpose such as throughput, Encryption Time
Step 6: User can also view the previously uploaded and encrypted files and download it.
Step 7: User can save the changes as applied on cipher text and let them reflected on original data. User can also discard changes then the files retains to its original content.
The proposed algorithm provides a clear understanding with its each step. It will help the method to provide better resolution of the current situations of Virtualization with the modifications in existing algorithm.

IV. RESULTS

The proposed system is implemented on openshift public cloud and java eclipse. Results are measured and analyzed on the factors encryption decryption time complexities and available resources of system which is compared with traditional and other available systems.
The below table 1 elaborates the time complexities of different file uploading and encryption using KP-ABE and modified KP-ABE method. To find out the efficiency of an encryption scheme with its throughput the encryption time is calculated and vice versa for the decryption end this time signifies the speed of any encryption scheme. The throughput of the encryption scheme can be calculated as the total plaintext in bytes encrypted divided by the encryption time. Below the table shows a comparison between the encryption time complexities for existing method and modified KP-ABE.
The comparison has been made on the encryption and decryption of an uploaded file. Different file formats are uploaded to check the consequence of result.
Thus the result implies that our proposed method takes less time in securing the data. The comparative result proved that the proposed modified KPABE is more efficient than the existing method in terms of time complexity, data sharing, and user's security.
The results also revealed that through modified KP ABE the resources are less utilized than the existing method. The result are depicted in terms of utilized memory, utilized RAM by each user during execution, at time of request each user send memory details to public cloud. Also illustrates how much memory and RAM is available on server during execution of cloudlets.
In existing system the available memory and RAM used is less and in proposed system the available memory and RAM used is more.

Table 1: Time Complexities of modified KP-ABE for encryption of different Files

S. No	File Name	File Size	Encryption Time (AVG) (KP-ABE)	Encryption Time (AVG) Modified (KP-ABE)
1	Resume.pdf	5.6MB	10275.0	9275.0
2	CombinedF.pdf	1.6MB	3288.334	2988.334
3	REPORT.doc	3.8MB	7407.0	6403.38
4	Database.sql	1MB	1432.02	1336.02

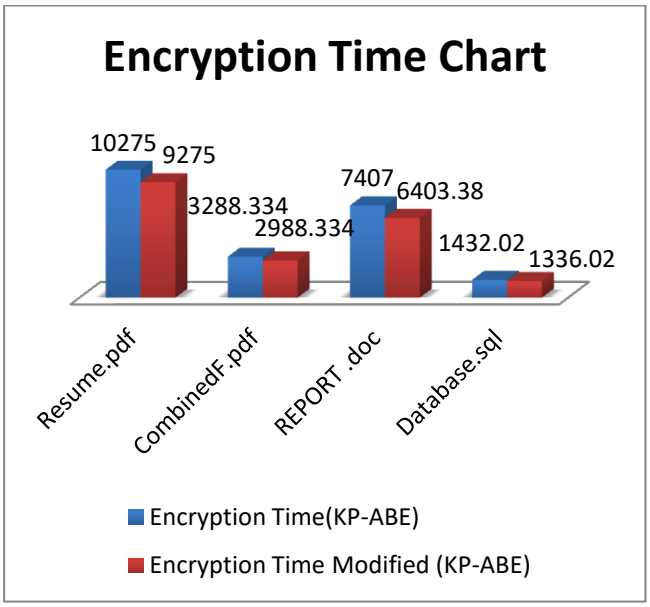

Fig 7: comparison graph for encryption

Table 2: Time Complexities of modified KP-ABE for decryption of different Files

S.No	File Name	File Size	Decryption Time (AVG) (KP-ABE)	Decryption Time (AVG) Modified (KP-ABE)
1	Resume.pdf	5.6MB	8363	7363
2	CombinedF.pdf	1.6MB	717.6667	607.9
3	REPORT .doc	3.8MB	5018	4586
4	Database.sql	1MB	698	588

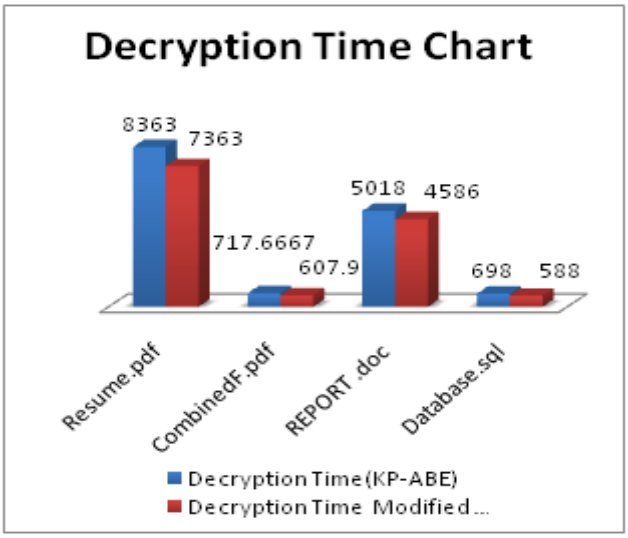

Fig 8: Comparison graph for decryption

V. CONCLUSION

This paper discusses the storage virtualization and its relation with secure cloud environment. This research article briefly outlines the concept of storage virtualization and secure data sharing. To achieve the security with improved virtualization KPABE scheme is used with dynamic resource allocation. An analysis on the time complexities of different file uploading and encryption using KP-ABE and modified KP-ABE method has been made. To find out the efficiency of an encryption scheme with its throughput the encryption time is calculated and vice versa for the decryption end, this time signifies the speed of any encryption scheme. Attribute-based access control schemes guarantees the data confidentiality in cloud. Through the attributes the data owners are allowed to define an access structure and encrypt the data with these so that data owners can characterize the attributes that the user requires to hold in order to decrypt the cipher text. We also constructed a modified KP-ABE scheme which is more efficient in terms of access control, data sharing, resource utilization and security assumption.

REFERENCES

1. Sosinsky B (2011) Cloud computing bible. Https://doi.org/10.1145/358438.349303
2. Elhadj benkhelifa, Virtual Environments Testing as a Cloud Service: A Methodology for Protecting and Securing Virtual Infrastructures [IEEE]February 28, 2019, August 20, 2019. Digital Object Identifier 10.1109/ACCESS.2019.2912957
3. P Mahajan, L Alvisi, M Dahlin Consistency, Availability, and Convergence - University of Texas at Austin Tech Report, 2011 – Citeseer
4. Ariel Feldman,William P.Zeller, Michael J Freedman, Edward Felten sporc: group collaboration using untrusted cloud resources, 9th USENIX Symposium on Operating Systems Design and Implementation · OSDI 2010,Vancouver, BC, Canada
5. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. EUROCRYPT*, 2005,pp. 457–473
6. A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proc. EUROCRYPT*, 2010, pp. 62–91.
7. T. Okamoto and K. Takashima, "Fully secure functional encryption with general relations from the decisional linear assumption," in *Proc. CRYPTO*, 2010, pp. 191–208.
8. V.Goyal, O. Pandey,A. Sahai, and B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Computer and Communications Security*, 2006, pp. 89–98.
9. Bethencourt, J.; Sahai, A.; Waters, B. (2007-05-01)."Ciphertext-Policy Attribute-Based Encryption". 2007 IEEE Symposium on Security and Privacy (SP '07): 321334. Doi:10.1109/SP.2007.11.
10. R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Proc. CRYPTO*, 2010, pp. 465–482.
11. K.-M. Chung, Y. T. Kalai, and S. P. Vadhan, "Improved delegation of computation using fully homomorphic encryption," in *Proc. CRYPTO*, 2010, pp. 483–501.
12. C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. STOC*, 2009, pp. 169–178.
13. C. Gentry and S. Halevi, "Implementing gentry's fully-homomorphic encryption scheme," in *Proc. EUROCRYPT*, 2011, pp. 129–148.
14. B. Parno, M. Raykova, and V. Vaikuntanathan, "How to delegate and verify in public: Verifiable computation from attribute-based encryption," in *Proc. TCC*, 2012, pp. 422–439.
15. S. Goldwasser, Y. T. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich, "Succinct functional encryption and applications: Reusable garbled circuits and beyond," *IACR Cryptology eprint Archive*, vol. 2012, p. 733, 2012.

16. M. Green, S. Hohenberger, and B.Waters, "Outsourcing the decryption of ABE ciphertexts," in *Proc. USENIX Security Symp.*, San Francisco, CA, USA, 2011.
17. Zhu Tianyi , Liu Weidong, Song Jiaxing, " An efficient Role Based Access Control System for Cloud Computing" , 2011 11th IEEE International Conference on Computer and Information Technology
18. Basel Saleh Al-Attab, Dr. H.S.Fadewar, Role-Based Access Control's Framwork For Cloud Computing, conference 103rd Indian Science Congress, Mysuru 2016 at Mysore University, Information and Communication Sciences & Technology (Including Computer Sciences).
19. T. Shashank & Vijay Kumar (2018). Weighted Attribute Data Sharing in Cloud Computing. International Journal of Pure and Applied Mathematics. ISSN: 1314-3395
20. Saravana kumarn,Rajya Lakshmi GV,Bala Murugana B " Enhanced Attribute Based Encryption for Cloud Computing "Conference: International Conference on Information and Communication Technologies (ICICT,2014), At CUSAT,Kochi,India, Volume: Volume 46, 2015, Pages 689–696, *in* Procedia Computer Science , DOI: 10.1016/j.procs.2015.02.127 ·
21. Gone Sowjanya & Srinivas Rao, "Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 5 Issue 8, 2018, Page 42-49.
22. L. Cheung and C. C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Computer and Communications Security*, 2007, pp. 456–465.

AUTHOR PROFILE

Nikita Kayarkar, Student Computer Science Engineering (M.E. 4th Sem) Indore Institute of Science & Technology, Indore (M.P.)

Uday Singh Kushwaha, Asst. Professor Computer Science Department Indore Institute of Science & Technology, Indore (M.P.)

Prashant Richhariya, Asst.Professor Computer Science Department Indore Institute of Science & Technology, Indore (M.P.)