Scientific Journal of Impact Factor (SJIF): 3.134

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 1, January -2016

Parallel and Context Based Access control in Cloud Using Multi Agent System

Hiren V Mer,
[1]*Assistant Professor, Atmiya institute of Technology and Science, Rajkot*

Abstract: *Cloud computing is one of the fast growing Technology for the search and access. it has been concerning about the security. Cloud computing support large scale infrastructure used to increase performance of computing. This technology support Multi agents with the security and with the help of integration of the agents it is Multi Agent System (MAS) which is capable of intelligent behavior. They run in an environment where they communicate with each other using message passing technique. Each agent has its own set of behavior and they run independent of each other. When a message arrives each agent shows their own behavior and hence an agent shows their coordination. The use of MAS in cloud computing help us for searching context with better performance and it is also providing the security. The JADE is a platform which supports agent. This paper discusses about Cloud computing models and architectures, information retrieving technique, security techniques and the use of MAS that improve the performance of big data search from Distributed File System (DFS) with secure access which is difficult to achieve using single agent or thread.*

Keywords— *Cloud Computing, Distributed File System, JADE, MAS,NIST,CP-ABE*

I. INTRODUCTION

Cloud computing provide elastic services, high performance and scalable storage of data to a large and on a daily basis increasing number of users. Cloud computing enlarged the arena of distributed computing systems by providing advanced Internet services that complement and complete functionalities of distributed computing provided by the Web, Grid computing and peer-to-peer networks. Even Cloud computing systems provide major infrastructures for high-performance computing with dynamism adapt to user and application needs.[1]

Cloud computing had be defined on the basis of many concepts like processing, storage resources, the service-oriented interface and Architcture and the exploitation of virtualization techniques etc. [2] The National Institute of Standards and Technology (NIST) had given a complete reference definition. NIST defined “Cloud computing is a pay-per-use model for enabling available, convenient, on- require network access to a shared group of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be quick provision and released with nominal administration effort or service provider interaction.”

Moreover, “Cloud model promotes availability,reliability and is comprised of five key characteristics, three delivery models, and four deployment models.”

-Five essential elements of cloud computing are:

□ □ On-demand self-service
□ □ Broad network access
□ □ Resource pooling
□ □ Rapid elasticity
□ □ Measured Service

-Three main service model of cloud computing are:

□ □*Software as a Service (SaaS)*

Cloud consumers release their applications on a hosting environment, which can be accessed through networks from a variety of clients (e.g. web browser,PDA,etc.) by application users. Examples of SaaS include SalesForce.com, *Google Mail, Google Docs, and so* forth.

□ □*Platform as a Service (PaaS)*

PaaS is a development platform supporting the full software Lifecycle which allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud. Hence the difference between SaaS and PaaS is that SaaS only hosts completed cloud applications whereas PaaS offers a development platform that hosts both completed and under progress cloud applications.Eg. Google App Engine.

□ □*Infrastructure as a Service (IaaS)*
Cloud consumers can use IT infrastructures (processing, storage, networks, and other fundamental computing resources) provided in the IaaS cloud. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers.
Four cloud deployment models have been defined in the Cloud community:
□ □*Private Cloud* - The cloud infrastructure is operated exclusively within a single organization, and managed by the organization or a third party anyway whether it is located premise or off premise. Academics often build private cloud for research techniques and teaching Learning purposes.

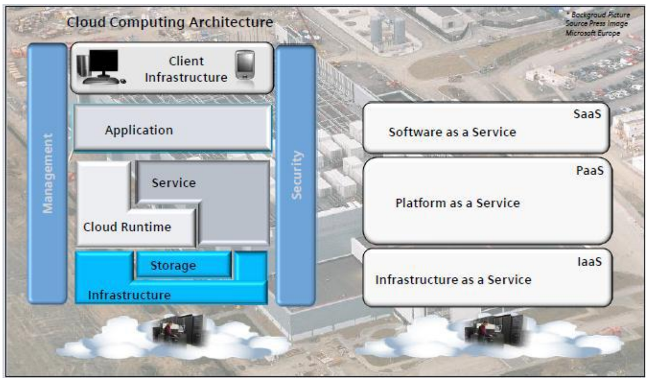

Fig.1.Cloud Computing Service Model.[3]

□ □*Community Cloud* - Several organizations jointly construct and share the same cloud infrastructure as well as policies, requirements, standards, and concerns. The cloud infrastructure could be hosted by a third-party vendor or within one of the organizations in the community.

□ □*Public cloud* - This cloud is used by the general public cloud consumers and the cloud service provider has the full ownership of the public cloud with its own policy, value, and profit, costing, and charging model.

Hybrid cloud - The cloud infrastructure is a combination of more than one cloud (private, community, or public) that remain unique entities but are bound together by standardized or appropriate technology that enables data and application portability.

1.2 Intelligent System and Multi Agent System

Intelligent System: An Intelligent agent is a special type software component that can be act independent on behalf of its user. The amount of intelligence in an agent varies depending on the task assigned and the environment where it is used. An agent is special with its, Autonomy- having its own thread of control, Social- cooperating with other agents, Intelligence- perceives its environment and responding to it, Proactive- exhibiting its goal directed behaviour, Learning- the ability to improve performance and decision making over time when interacting with the external environment.[15]
Multi Agent System: A **multi-agent system** (**MAS**) is composed of several interacting intelligent agents within an environment. Multi-agent systems are used for solving the problems that are difficult or not possible for a single agent or a monolithic system to solve. Intelligence may include some methodical, functional, procedural or algorithmic search, find and processing approach. The use of Multi Agent makes the cloud to service in better way. [16]
The agents in a multi-agent system have several important qualities:
□ □**Autonomy**
□ □**Local views**
□ □**Decentralization**

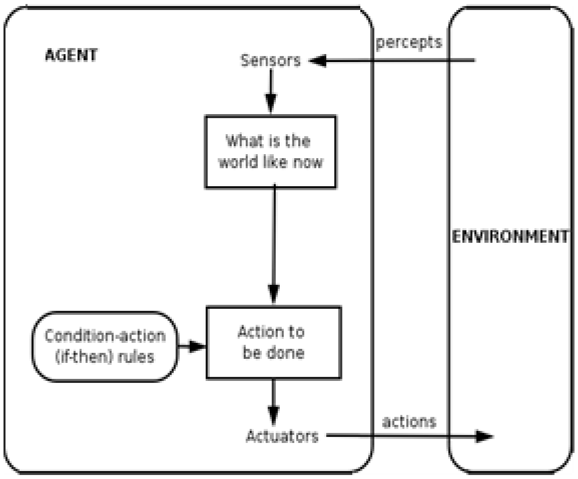

Fig 2. Intelligent Agent [15]

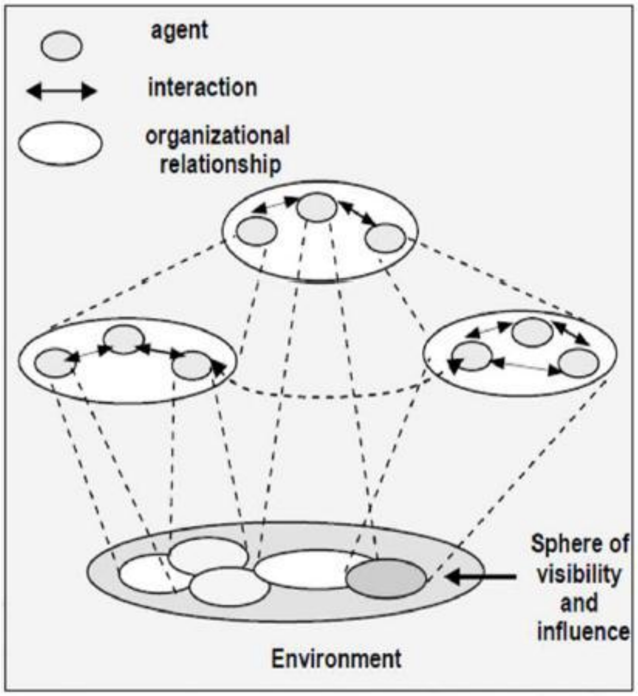
agent
interaction
organizational relationship
Sphere of visibility and influence
Environment

Fig 3 .Multi Agent System [15]

To summarize this, multi-agent systems (MAS) present an additional distributed computing paradigm based on multiple interacting agents that are capable of intelligent behaviour. Multi-agent systems are often used to solve problems by using a decentralized approach where several agents contribute to the solution by co-operating one each other. One quality of software agents is the intelligence that can be embodied into them in accordance with some collective artificial intelligence approach that needs cooperation among several agents that be able to run on a parallel or distributed computer to achieve the needed high performance for solving large or more complex problems keeping execution time low.

In cloud computing, users store their data files in cloud servers. Thus, it is crucial to prevent unauthorized access to these resources and realize secure resource sharing. In traditional access control methods, we generally assume data owners and the storage server are in the same secure domain and the server is fully trusted. However, in the cloud computing environment, cloud service providers may be attacked by malicious attackers. These attacks may leak the private information of users for commercial interest as the data owners like administrator commonly store decrypted data in cloud servers. How to realize access control to the encrypted data and ensure the confidentiality of data files of users in an untrusted environment are problems that must be solved by cloud computing technologies and applications. Moreover, since the number of users is large in a cloud computing environment, how to realize scalable, flexible and fine-grained access control is strongly desired in the service-oriented cloud computing model.

This CP-ABE with constant cipher text size and maintains the size of cipher text and the computation of bilinear pairing at a constant value, which improves the efficiency of the system and reduces the extra overhead of space storage, data transmission and computation. Second, we design a hierarchical access control system. This system supports inheritance of authorization that reduces the burden and risk in the case of single authority. Finally, we prove our scheme has indistinguishable security under an adaptive chosen cipher text attack and we analyze the performance of our scheme. We present a simulation model to apply our scheme in a cloud environment.

II. RELATED WORK

Dinesh Kumar R C, Ashwin R [7], they discuss about the MAS and the usage of the intelligent agents and how it is used for searching purpose in the cloud. Multi-agent systems (MASs) can integrate with Cloud Computing System.So that we can get high-performance and making clouds more flexible and autonomic.

Vishal Jain and Mahesh Kumar Madan [8], they define capabilities of MAS that permits the user to solve methodic, functional algorithmic and or technical query to discover and process the data. The aim of authors is to retrieve the information using Multi Agent System with Data Mining technique in Cloud Computing environment. In this research paper, cloud computing allows the users to retrieve meaningful information from virtually integrated data warehouse that reduces the costs of infrastructure and storage.

Gagandeep Singh Narula,Vishal Jain, and Dr.Mayank Singh[10],In this paper they illustrates working of JADE and defines schemas (classes and subclasses) and instances (objects) with user defined methods that helps in execution of program by writing code in Java Script. It is known that responsibility of developing agents in complex and business environments is controlled by software framework called JADE (Java Agent Development Framework).Even they try to implement a framework for MAS using JADE on Online Shopping System.

Yu Mon Zaw, Nay Min Tun[10],They propose a framework for Web Services Based Information Retrieval Agent System for Cloud Computing Environment. The proposed system framework is intended to apply in Medical field. Efficiently composed cloud Web Services with the use of Multi-Agents features can give new form for cloud wide information retrieval systems.The proposed system will become an intelligent way for searching or retrieving information from Cloud environment.

S.Balasubramaniam, Dr.V.Kavitha [12],In this study rigorous analysis is made on Data retrieval techniques which are used to retrieving the original data from the encrypted data on the cloud environment. Many searchable techniques have been analyzed based on single keyword, multiple keyword search, Ranking, Similarity search, Fuzzy tolerance. The goal is to enable rich search semantics in a privacy preserving manner and efficiently support for large scale and distributed nature of cloud data.This study only explained various data retrieval techniques for text data.

Access control is a classic security issue. Various ac-cess control models have been proposed since the 1970s, e.g. DAC[16],MAC[17],Bell-La Padula[18],Biba[19] etc. In 1996，Sandhu et al. proposed the Role-Based Access Con-trol Model[20](RBAC).Variousimproved RBAC models have been proposed and been widely used in practice. With the development of information technology, tradi-tional access control is not very suitable for access control in cloud computing for the following reasons. First, the flexibility of the access policy is inadequate and it is more difficult to extend it to a hierarchical and large-scale application in a cloud computing environment. Second, these access control schemes needs to strengthen their adaptability to a cloud computing environment. Third, their adaptability to dynamically change roles is simply not enough. The role of users changes dynamically in many applications.How to achieve a dynamic change of role is a problem that should be solved regarding trditional access control. Finally, high security requirements need a new access control model. In traditional access control schemes,we generally assume the storage server is fully trusted. How-ever, in a cloud computing environment the data owners and storage server are not in the same secure domain and the cloud service provider may be untrusted. A general solution for this problem is to store the encrypted data file in a server and decryption keys to authorized users.Thus,unauthorized users (includes cloud service provider) cannot decrypt the encrypted files and it can control the decryption ability of users to achieve access control. This method provides an idea for realizing the confidentiality of data stored on untrusted server.To achieve easy public-key encryption deployment, Shamir proposed the concept of identity-based encryp-tion (IBE) [21].A user’s public key is his/her identity, such as e-mail address or phone number. An encryptor can create a ciphertext under the receiver’s identity with-out asking for the receiver’s public key before hand. The first fully functional IBE scheme was presented by Boneh and Franklin [22]. They constructed an IBE scheme by exploiting the Weil pairing and they proved its selec-tive security in the random oracle model.Similarly to IBE, a number of identity-based cryptographic primitives have been proposed [23][24][25][25][27][28][29].Several advanced cryptographic primitives allow defining more controllable decryption. Hierarchical identity-based encryption (HIBE), first proposed by [30], is an identity-based cryptographic primitive that extends IBE with key delegation to relieve the private key generator in IBE from heavy key management burden when thereis a large number of users in the system.

A user can decrypt the ciphertexts if and only if his attributes satisfy the ciphertext's policy. In 2007, the first CP-ABE scheme was proposed by Bethencourt et al.[33]which adopted the general group model and threshold access tree. This scheme is suitable for an application needing a simple access policy. Many improved ABE algorithms have been introduced [34][35][36][37][38]and ABE schemes have been presented. Since users' decryption keys are associated with a set of attributes, CP-ABE is conceptually closer to traditional access control models such as Role-Based Access Control (RBAC). Thus, it is more natural to apply CP-ABE to enforce access control of encrypted data. Howeverthe disadvantages of these schemes relate tothe size of ciphertext, and the computation of encryption and decryption depends linearly on the number of attributes. In cloud computing, it will limit the application of ABE in practice if the number of attributes is too large and the length of ciphertext is too long. In addition, the huge user numbersin a cloud computing environment means it is impractical to complete the authorization and distribute secret keys using only one at-tribute authority.Ruj et al. [39] proposed a new model for data storage and access in clouds. This scheme distributes keys to data owners and users by key distribution centers(KDC). In 2011,Wang et al.[40]proposed a hierarchical attribute-based encryption scheme (HABE) by combining a HIBEsystem and a CP-ABE system to provide not only fine-grained access controlbut also full delegation and high performance. In 2012, Wan et al. [41]proposed a hierarchical authority structure with a central authority(Central Authority) and used the algorithm ASBE[42]to realize scalable and flexible access control and valid at-tribute revocation in clouds. In 2014,Deng et al.[43]proposed a new versatile cryptosystem referred to as cipher-text-policy hierarchical ABE (CP-HABE)with short ci-phertexts .These schemes suppose KDC or CA is fully-trusted and can defend against various malicious attacks that are difficult to realize in a cloud. However, in a cloud computing environment the service provider may be un-trusted. Furthermore, in previous ABE schemes, the size of the ciphertext and the number of pairing computations vary linearly with the number of attributes. These limit the usage of ABE in real applications because the size of the ciphertext is too long with the thousands of attributes in a cloud computing environment. The first CP-ABE scheme with a constant ciphertext size was proposed by Emura et al. in [34]and the policies were restricted to AND-gates. Herranz et al. [44]constructed another con-stant size ciphertext CP-ABE schemethat maywork for the (t,n)-threshold policy. Geet al.[45]proposed a CCA secure CP-ABE scheme with constant size ciphertexts that can support flexible threshold access structure in the standard model.

III. PROBLEM DEFINITION

Here we can see the attribute based access control is used for the multi user system base on HDFS file sytem.and another paper had the concept of the Multi agent system for the keyword search so we can use this access control method for this multi user system.Itcan help for security and control of the user access.

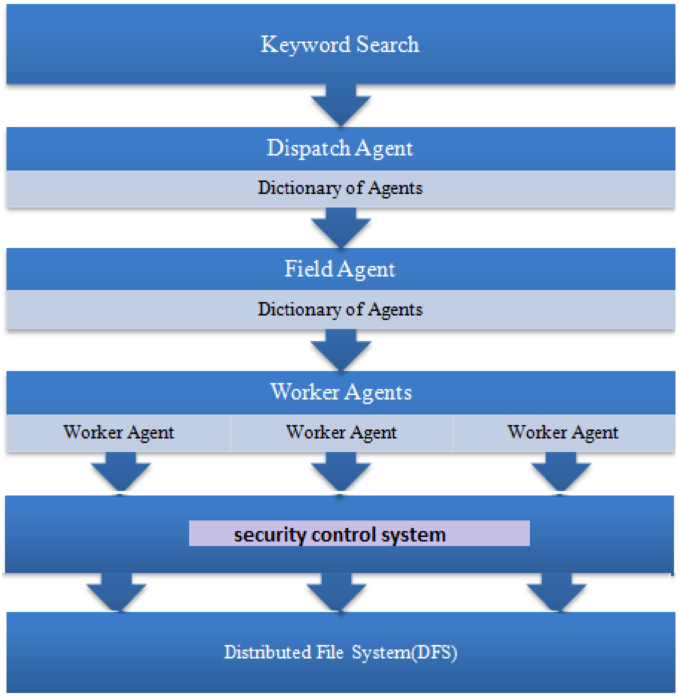

Fig 4 .Multi Agent System with security

IV. Proposed Work

This all the papers gives the idea for the parallel search and security for the access of the text through the multi agent system .so here I am applying the security in the multi agent system for the secure and fast access. Then we can apply security to all the multi agent system here you can see the block diagram.

V. Conclusion

Based on this my proposed work here it shows when we search keyword in single system we cannot search efficiently and effectively. Then It shows multiuser system to search fast keyword from the file system. and I am applying the security access in this Multi user system. See the Block diagram to see the Multi Agent system. Now you can implement using HDFS and this access control system. See the fig 4.

References

[1] Talia, D.2012.”Cloud Computing and software agents: Towards Cloud Intelligent Services”,

[2] The NIST Definition of Cloud Computing,Peter Mell Timothy Grance NIST Special Publication 800-145

[3] http://resources.sei.cmu.edu/asset_files/Presentation/2010_017_001_23337.pdf

[4] research.ijcaonline.org/egov/number1/egov1004.pdf

[5] Wikipedia.http://en.wikipedia.org/wiki/ multiagent

[6] Dinesh Kumar R C and Ashwin R, International Conferenece on EGovernance & Cloud Computing Sevices(EGov ’12)

[7] vishal jain and mahesh kumar madan“Information Retrieval through Multi-Agent System with data mining in cloud compuitng,IJCTA|JAN-FEB 2012,www.ijcta,com

[8] An approach for information extraction using jade ,volume 4,N0.4,April 2013,journal of Global Research in Computer Science

[9] Web Services Based Information Retrieval Agent System for Cloud Computing,volume 2-issue1,67-71,2013.www.ijcat.com

[10] Optimizing Web Mining using Multi-agent System, Shah Yesha B., Prof G.B.Jethava,International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 10, December 2012

[11] S.Balasubramaniam, Dr.V.Kavitha" A Survey on Data Retrieval Techniques in Cloud Computing"Journal of Convergence Information Technology(JCIT) Volume8, Number16, November 2013

[12] Amazon Elastic Compute Cloud (Amazon EC2). http://aws.amazon.com/ec2/

[13] Amazon Web Service (AWS). http://s3.amazonaws.com/

[14] Google App Engine (GAE). http://code.google.com/appengine/

[15] Microsoft Azure. http://www.windowsazure.com

[16] R.W. Conway, W.L. MaxWell and H.L. Morgan, "On the im-plementation of security measures information systems," *Communations of the ACM*,vol. 15, no.4, pp:211-220, April. 1972.

[17] D.E. Denning,"A Lattice Model of Secure Information Flow," *Communications of the ACM*,vol. 19, no. 5, pp:236-243, May. 1976.

[18] D.E. Bell and L.J. LaPadula, "Secure Computer System: Unified Exposition and Multics Interpretation,"Technical Report TR-A885320, The MITRE Corp.,Bedford, MA, Mar. 1976.

[19] K.J. Biba,"Integrity Considerations for Secure Computer Sys-tems," Technical Report TR-A423930,The MITRE Corp.,Bed-ford, MA, Apr. 1977.

[20] R. Sandhu, E.J. Coyne and H.L. Feinstein, "Role-based access control models," *IEEE Computer*,vol. 29, no. 2, pp:38-47, Feb. 1996.

[21] A. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology: Conf. of CRYPTO 84, LNCS 196,pp: 47-53, 1984.

[22] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, *Advances in Cryptology : 21st Annual International Cryp-tology Conf.*(CRYPTO 2001), LNCS 2139, pp:213-229, 2001.1.

[23] M. Green, G. Ateniese, "Identity-based proxy re-encryption", *Applied Cryptography and Network Security:5th International Conf.*(ACNS 2007),LNCS 4521, pp:288-306, 2007.

[24] H. Wang, Z. Cao, L. Wang, "Multi-use and unidirectional iden-tity-based proxy re-encryption schemes", *Information Sciences*,vol.180,no.20,pp:4042–4059,2010

[25] J. Shao, Z. Cao, "Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption",*In-formation Sciences*,vol.206,pp:83–95,2012.

[26] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, Y. Chen, "Forward-secure identity-based signature: security notions and construc-tion",*Information Sciences*,vol.181,no.3,pp:648–660,2011.

[27] L. Chen, Z. Cheng, N.P. Smart, "Identity-based key agreement protocols from pairings",*International Journal of Information Se-curity*,Vol.6,no.4,pp:213–241 ,July2007.

[28] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, "Provably secure one-round identity-based authenticated asymmetric group key agreement protocol",*InformationSciences*,vol.181,no.19,pp:4318–4329, 2011.

[29] S. Liu, Y. Long, K. Chen, "Key updating technique in identity-based encryption", *Information Sciences*,vol.181,no.11,pp:2436–2440,2011.

[30] J. Horwitz, B. Lynn, "Toward hierarchical identity-based en-cryption",*Advances in Cryptology:International Conference on the Theory and Applications of Cryptographic Techniques*(EU-ROCRYPT 2002),LNCS 2332, pp:466-481,2002.

[31] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryp-tion,"*EUROCRYPT '05: Proc. Advances in Cryptology,* R. Cramer, ed.,pp. 457-473, May. 2005.

[32] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"*Proc. ACM Conf. Computer and Comm. Security (CCS '06),*A. Juels,R.N. Wright, and S.D.C. di Vimercati, eds., pp. 89-98, Oct./Nov.2006.

[33] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy at-tribute-based encryption," *Proceedings –IEEE Symposium on Se-curity and Privacy*,pp. 321-334, May. 2007.

[34]] K. Emura, A. Miyaji, A. Nomura, K. Omote and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with con-stant ciphertext length," I*nformation Security Practice and Experi-ence:5th International Conf.* (ISPEC 2009),LNCS5451,pp:13-23, 2009.

[35] V. Goyal, O. Pandey, and A. Sahai, "Bounded ciphertextpolicy attribute-based encryption," *Automata, Languages and Program-ming:35th International Colloquium*(ICALP 2008),LNCS 5126,pp:579-591, 2008.

[36] L. Ibraimi, Q. Tang, P. Hartel and Q. Jonker, "Efficient and provable secure ciphertext-policy attribute-based encryption schemes," *Information Security Practice and Experience: 5th Inter-national Conf.*(ISPEC 2009),LNCS5451, pp:1-12, 2009.

[37] M. Chase, “Multi-Authority attribute based encryption,” *Lecture Notes in Computer Science*,vol.4392, pp: 515-534, 2007.

[38]] S. Yu, C. Wang, K. Ren and W. Lou, “Achieving Secure, Scala-ble, and Fine-grained Data Access Control in Cloud Compu-ting,” *Proceedings –IEEE INFOCOM*,pp:1-9, 2010.

[39] S. Ruj, A. Nayak and I. Stojmenovic, “DACC: Distributed Ac-cessControl in Clouds,” *Proc. 10th Int’l Con. Trust, Security and Privacy in Computing and Communications (TrustCom)*,IEEE, pp: 91-98, Nov. 2011.

[40] G. Wanga, Q. Liu, J. Wu and M. Guo, “Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers”,*computersand security*,vol.30,pp:320-331,2011.

[41] Z. Wan, J. Liu and R.H.Deng, “HASBE: A Hierarchical Attrib-ute-Based Solution for Flexible and Scalable Access Control in Cloud Computing,” *IEEE Transactions on Information Forensics and Security,* vol. 7, no. 2, pp: 743-754, Apr. 2012.

[42] R. Bobba, H. Khurana and M. Prabhakaran, “Attribute-sets: A practically motivated enhancement to attribute-based encryp-tion,” *Computer Security:14th European Symposium on Research in Computer Security*(ESORICS 2009),LNCS5789, pp: 587-604, 2009.

[43] H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrer d and L. Zhang,” Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts”,*Information Sciences*,vol.275,pp:370-384,2014.

[44] J. Herranz,F.Laguillaumie and C.R`afols, ”Constant Size Ci-phertexts in Threshold Attribute-Based Encryption”,*Public Key Cryptography:13th International Conference on Practice and Theory in Public Key Cryptography*(PKC 2010),LNCS6056, pp: 19–34, 2010.

[45] A. Ge, R. Zhang and C. Chen, “Threshold Ciphertext Policy Attribute-Based Encryption with Constant Size Ciphertexts,” *Public Key Cryptography :13th International Conference on Practice and Theory in Public Key Cryptography*(PKC2010),LNCS7372, pp: 336-349, 2012.

[46] D. Boneh, X. Boyen and E.-J. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” *EUROCRYPT ’05: Prof.Advances in Cryptology,* R. Cramer, ed., vol.3494, pp: 440-456, 2005.

[47] The Pairing-Based Cryptography Library. http://crypto.stanford.edu/pbc/

[48] The GNU Multiple Precision Arithmetic Library. http://gmplib.org

AUTHOR INFORMATION:

Hiren V Mer (M’28) Assistant Professor in Atmiya institute of technology and science,Rajkot.he had published the 8 papers in different journals.he is expertise in the cloud computing,network security and Database.