IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-5 E-ISSN: 2347-2693

Extensible and Fine-Grained Characteristics-Positioned Information Storage in Cloud Computing

S. Rajput[1], Iyapparaja M.[2*]

[1]School of Information Technology and Engineering, VIT University, Vellore, India
[2]School of Information Technology and Engineering, VIT University, Vellore, India

[*]*Corresponding Author: iyapparaja.m@vit.ac.in, Tel.:9942532920*

www.ijcseonline.org

Received: 15/Apr/2017, Revised: 23/Apr/2017, Accepted: 23/May/2017, Published: 30/May/2017

***Abstract*—** With the improvement of distributed computing, outsourcing information through distributed server's pulls in loads of considerations. To ensure the security and accomplish adaptable fine-grained record access control, (ABE) was proposed and utilized as a part of distributed storage framework. As client repudiation is the essential issue in ABE plans. we proposed an cipher text-arrangement trait-based encryption (CP-ABE) plan with effective client repudiation for distributed storage framework. The concern about client repudiation can be explained productively by presenting the idea of client gathering. At the point when any client leaves, the gathering supervisor will redesign client's PK with the exception of the individuals, who have been declined. Also, CP-ABE plan has substantial calculation cost, as it becomes straightly with the intricacy to access structure. To diminish the calculation price, utilizing big calculation burden to cloud administration suppliers without spilling document substance and mystery keys. Notably, our plan can withstand conspiracy assault performed by denied clients collaborating with existing clients.

***Keywords*—** Distributed Computing, Cipher-Text Attribute-Based Encryption, Data Owner, Cloud Server, Private Keys, Co-Llusion Attack.

I. INTRODUCTION

Cloud is a general indication used to depict another classification about a structure placed registering that happens over the web, Essentially a stage on from adequacy Computing. Pay for utilizing and as required, versatile, scale all over in limit and functionalities. It has met the growing demand for handling resources and limits assets for a couple wanders due to its purposes of economy, flexibility, and accessibility. Starting late, a couple appropriated capacity organizations, e.g. Microsoft Azure and awes were constructed and can supply customers with versatile and element store. With the extending of tricky information deploy via Cloud, circulated capacity organizations are going up against numerous challenges including data security and data get to overlook. To grasp those issues, trait-based encryption arranges has been associated with conveyed store services. Sahai and Waters initially proposed ABE plot named fuzzy personality based encryption which is gotten from id substance based encryption (IBE) [7]. As another proposed cryptographic primitive, ABE scheme has the upside of IBE plan and also gives the typical for "one-to-numerous" encryption. Straightforwardly, ABE chiefly principally incorporates two orders called ciphertext-system ABE (CP-ABE) and key p olicy plan ABE (KP-ABE).problem raise of giving your private key to others. A KP-ABE cipher-text are marked with a cluster of trait& PK's is identify with accessed architecture that supervision the cipher-texts a user can decrypt [1].

They demonstrate the beneficial CP-ABE with customer dissent limit. The materials & compute administrations are accessible to overall population, endeavours, partnerships and organizations markets. With the change of passed on figuring, outsourcing information to shared slave pulls in stores of thoughts. To ensure the security and complete adaptable fine-grained record getting controlled, trait-based encryption was proposed and utilized.

In this, proposed another multi-expert CP-ABE framework which addresses these two issues decidedly. In this new framework, there are various Central Authorities (CAs) and Attribute Authorities (AAs), the CAs issue personality related keys to clients and are not included in any property related operations, AAs issue describes related keys to clients and every AA deals with an alternate space of characteristics.

The framework is adaptively reliable for classic standard with versatile specialist debasement and can bolster expansive trait universe [8]. We proposed a protection saving de-centralized (PPDCP-ABE) plot where the focal expert is not required, specifically every specialist working autonomously no further needed participation to instate the framework [10].

II. PROBLEM DEFINATION

The existing paper deals with Property based encryption is a sort of open key encryption in which the mystery key of a end user & cipher-text are reliant upon qualities In such a framework, the un crumbling of a cipher-text is conceivable just if the arrangement of characteristics of the client Kei matches the properties of the ciphertext.In which issue of User Revocation& unsuitable for statistics protection in cloud storage systems. We here provide the solution which deals with both of the issues [3].

III. MOTIVATION

The fundamental significance of this project is to ensure the security and accomplish adaptably fine-grained record get to control, (ABE) was proposed and utilized as a part of distributed storage and outsource high calculation cost to cloud specialist [5].

Rest of the paper is organized as follows, Section I contains the introduction of cloud computing with CP-ABE algorithm and how revocation performed, Section II contain the related work of our project what are the techniques we used. Section III contain the literature review of some paper taken as reference. Section IV contain the methodology with flowcharts .Section V describes results and discussion of proposed technique. Section VI concludes research work with future directions.

IV. RELATED WORK

Despite ABE has shown its merits, user revocation and attribute revocation are the essential concernment.The revocation issue is much hard to do unusually in CP-ABE schemes, due to any attribute shared by users. This implies that revocation will affect the single user & other users .short while ago, some work proposed to handle this issue in an effective manner.Boldyreya et al showed an IBE scheme with effective revocation, that is suited to KP-ABE [9][11]. Tysowski et al gave a simple strategy to perform client disavowal operation by joining CP-ABE with re-encryption [12]. In their plan, each user having a place with a gathering and holds a gathering mystery key issued by the gathering. Nonetheless, gave idea won't avoid arrangement assault execute from abolish clients collaborating with existing clients. The reason is that every client's gathering mystery key is same for a similar gathering. Elements of the denied clients can be utilized by the client in a similar gathering without the predetermined attributes. Also, we bring up that a similar security hazard in the plans [2][3].Through applying ABE plans for distributed storage ser-indecencies, we can both guarantee the security of put away information and accomplish fine-grained information get to control. Sadly, ABE plot requires high calculation overhead amid performing encryption and unscrambling operations. This deformity turns for more extreme for lightweight gadgets because of their obliged figuring assets. To lessen the registering assets. To diminish the estimation price for asset compelled gadgets, some cryptographic operations with high computational load were outsourced to cloud specialist co-ops[13].Combined intermediary re-encryption with lethargic re-encryption system, Yu et al composed a KP-ABE conspire with fine-grained information get to control. This plan requires information gets to control [4]. This plan requires that the root hub in the get to the tree is an AND entryway and one kid is a leaf hub which is related to the spurious property. The spurious ascribe is required to be incorporated into each information archive's trait set and will never be refreshed. In their plan, cloud specialist co-op stores all PK's segments for client's private key aside from the one comparing to the fake property. Green et al gave a productive CP-ABE plot with outsourcing decoding [14]. In their plan, user's private key is blinded through utilizing an irregular num-ber. Both PK's and the arbitrary number are kept mystery by the user.The client shares his blinded private key middle to perform an outsourced decoding operation [4][14]. We utilize the comparative procedures as to extend our plan with outsourcing capacity. No single expert can decode any ciphertext. Keeping in mind the end goal to secure protection of the client, Han et al.presented a decentralized KP-ABE plot with security saving [10]. Essentially, Qian et al given a decentralized CP-ABE with completely concealed get to structure [15]. Besides, they proposed a protection saving individual wellbeing record utilizing multi-expert ABE with denial [7]. Recently, some traceable CP-ABE plans were genius postured with a specific end goal to discover a productive answer for recognizing malignant clients who intentionally share their decoding keys [2][15].

V. BASIC ABE/KP-ABE ALGORITHM

1. Setup: the calculation taken info a security attributeK and gives back people in general key PK and a framework ace mystery key mk. Pk's utilized for message sender's fo encryption. masterkey utilized for production of client mystery kes and is knwn just by the authorities.

2. Encryption: This calculation takes a message M, the otside key, &an arrangement traits info. & yields figure content E.

3. GeneratedKey: This calculation taken information a get to prototype Q & ace mystery key &just measures up to Q.

4. Decoding: It takes info the client's mk DK for accessing structe &cipher-text L, inwhic encoded underthe characteristic set&The calculation yields the messag if & just if characteristic sats fulfills client's get to structure's P [6].

CP-ABE Algorithm:

1.Setup: This calculation info is an security constraint K & gives back people in general key P-K and a frame-work ace mystery kai. primarykey as utilized by messaging $ender's to en-crypt. masterkey utilized to create client mystery key's & known just for autorized.

2.Encryption: The calculation received message M, the outside key& an arrangement properties information which yields figure content e.

3.Generated key: This calculation taken into info a get to framed F &ace M-K. It yields a mystery key SK that allows the client to decode a message encoded inside an arrangement properties if& measures up to P.

4.Decoding: The info of client's mystery ke to Accessing frame F & cipherstext CE, which scrambleed inside quality se-t. This ca lculation yields the mesg H if & just when the charac-teristic group fulfills client's get to format F.

VI. LITERATURE SURVEY

GOYAL. PANDEY, A. SAHAI, AND B. WATES,

The problem here enclosed is encrypt data to other side party by sharing your PrivateKey. They introduce a crypticscheme to access the attribute by their own charactertic attribute policy .cipher-text are marked with a cluster of sets & privatekey's were identify with accessed design that rule which cipher-texts a user can decrypt.

Q. HUANG, Z. MA, J. FU, X. NIU AND Y. YANG

An attribute-based DRM scheme in cc by combining the techniques of cipher-text (CP-ABE) and proxy re-encryption (PRE).we obtain powerful characterstic & client denial allowed by the attribute authority to delegate the key server to refuse to issue the assistant key for the revoked users.The proposed scheme is secure, efficient, and privacy-preserving.

KAN YANG, XIAOHUA JIA, KUI REN

we design an access control framework in shared pool storage and propose a fine-grained access control scheme based on (CP-ABE) approach. The data owner is responsible for defining and enforcing the access policy and efficient attribute revocation way i.e.,CP-ABE system's,By which attribute revocked price is minimized. Resulted inefficient & secured in random model.

SHUCHENG YU, CONG WAN†, KUI RN†, AND WENJING LU

The problem in accessing at same point in fine-grained, versatility, and information privacy of getting to control in reality still stays uncertain. We accomplish this objective by abusing and interestingly consolidating strategies of trait-based encryption (ABE), intermediary re-encryption, and languid re-encryption.

XIAFENG CHEN, JINGWEI LI, CHUFU JIA, JIANFENG MA, WENJING LOU

A Fuzzy IBE plot takes into consideration a PK for seen as an Identity-Based Encryption of a message under a few qualities that form a (fluffy) character. Our IBE plans are both bug-tolerant and secure against plot assaults. Furthermore, our essential development does not utilize irregular prophets. We demonstrate the security of our plans under the Selective-ID security model.

J. HR AND D. K. NOH

An another multi-expert CP-ABE framework which addresses these two issues decidedly. In this new framework, there are various Central Authorities (CAs) and Attribute Authorities (AAs), the CAs issue personality related keys to clients and are not included in any property related operations, AAs issue describes related keys to clients and every AA deals with an alternate space of characteristics. The framework is adaptively reliable for given model with versatile specialist debasement and can bolster expansive trait universe.

VII. METHODOLOGY

There were many solutions propose to solve user privacy problem, we have also proposed a strong way to protect user data leakage in untrusted cloud background In today's time mobile user has increased massively and has started using Flickr to de-anonymize Twitter, using Facebook to de-anonymize WiFi mobility traces, providing various services by the small organization, so these organizations may use the third party shared pool of data to process large user query point. So always occurrence chance that user data will be miss used the malicious cloud service provider.we give a cipher text-arrangement trait-based encryption (CP-ABE) plan with effective client repudiation for distributed storage framework. Problem raised of client repudiation can be explained productively by presenting the idea of client gathering. At the point when any client leaves, the gathering supervisor will redesign client's PK with the exception of the individuals, who have been declined. Also, CP-ABE plan has substantial calculation cost, as it becomes straightly with the

intricacy for opening structure. To diminish the calculation price, we expand huge calculation burden to cloud administration suppliers without spilling document substance and mystery keys. Notably, our plan can withstand conspiracy assault performed by denied clients collaborating with existing clients.

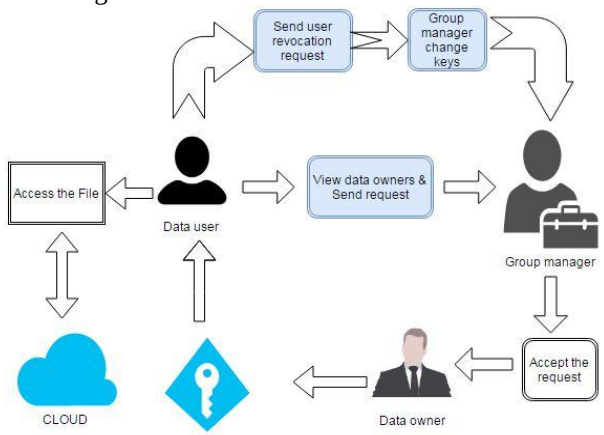

Fig4.1: System Architecture

System Architecture:

The System Architecture contains 4 entities Data owner, Cloud storage, group manager and data user. Data owner protection process will take place at the beginning where a user get a PK of downloading file (i.e., owner private key for that file) from cloud storage. The Data owner transfers our document. At the time documents are put away to cloud. Transferring every last record contains mystery key. Trust expert keeps up all information proprietor transferred documents mystery key. This is the third module of our venture. After that, Data client sees all information proprietor and all information proprietor transferred records. Then the client sends a demand to the proprietor. Right now ask for first go to gathering administrator then information owner. After that, data user send the request to data owner at the time request first go to the group manager. Group manager if accept request means this request go to data owner otherwise group manager cancel the request. Then data owner get the data user request if data owner accepts the request means data user get data owner secret key else data owner cancel the request means data user can't access the uploaded files. This is the fifth module of our project. Data owner and group, the manager accepts the data user request means data user get data owner secret keys. Then data user uses data owners secret keys access the data owner files. This is the six module of our project. After that, data user sends revocation request to the group manager. Group manager if accepting data user revocation request means at the moment data user left from this application and Group manager change all data owner secret keys.

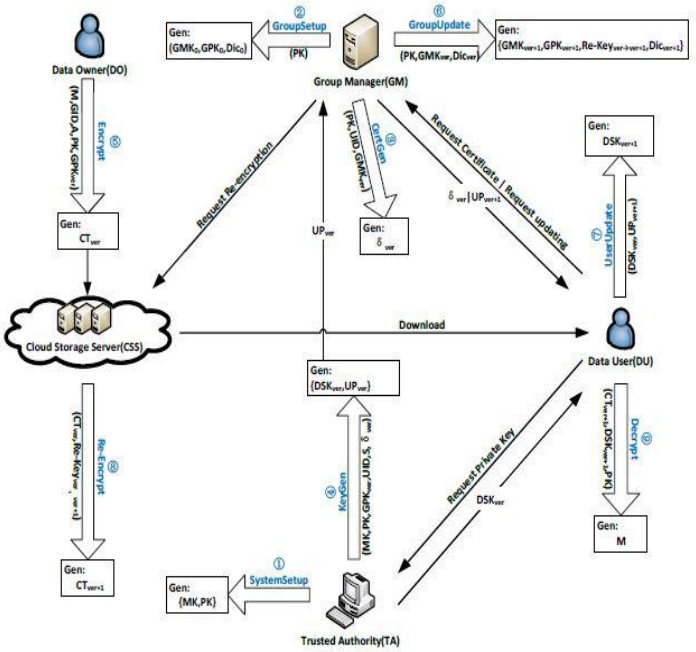

Fig. 3. CP-ABE with efficient user revocation.

Fig4.2: Security Model

System Design:
It consists of six modules:

User Interface Design:
It is created for security purpose. i.e., Login Page, we have to enter login id & password. Only valid client can access the page. It will check user login & pass is match or not . If any wrong id & pass is passed, we can't enter into login window to user window it will display an error message(this is verified by the server) .so that any unauthorized person cannot access this page. By this way we are providing a good security for our project.

Data Owner Upload File:
This is the second module of our project. Data owner upload our file. At the time files are stored to cloud. Uploading any file contains a secret key .Trust authority maintains all data owner uploaded files secret key.

Data User Send Request:
This is the third module of our project.Data user view all data owner and all data owner uploaded files .Then user send request to owner. At the moment request first go to GM then data owner.

Respond To GM & Owner:
This is the fourth module of our project. In this module data user send request to data owner at the time request first go to group manager. Group manager if accept request means this request go to data owner otherwise group manager cancel the

request. Then data owner get the data user request if data owner accept the request means data user get data owner secret key else DO cancel the request means data user can't be access the data owner files.

User Get Permission:

This is the fifth module of our project. In this module data owner and group manager are accept the data user request means data user get data owner secret keys . Then data user use data owners secret keys access the DO files.

User Revocation Request:

This is the six module of our project. In this module data user send revocation request to group manager. Group manager if accept data user revocation request means at the moment data user left from this application and Group manager change all data owner secret keys.

CLOUD COMPUTING

Microsoft Azure:

Microsoft Azure, in the past called by WA, Microsoft's open distributed computing stage. It gives an scope to shared storage administrations, it includes register, examination, stockpiling, and systems administration. Clients can pick and look over these administrations to create and scale new applications, or run existing applications, in the general population cloud.there are 11 primary administrations given from MA i.e., Compute,Web and mobile,Data storage,Analytics,Networking,Media and content conveyance organize (CDN),Hybrid integration,Identity and get to administration (IAM),Development,Management and security.To guarantee accessibility, Microsoft has Azure server farms situated the world over.

VIII. RESULTS AND DISCUSSION

We designed a java based prototype system for implementation of basic five entity of the system cloud, data owner, the unauthorized user data user, that it Trust authority and group manager. We implemented proposed plan& running on Windows PC with 2 Duo Intel Core PENTIUM IV 2.6 GHz and 512 MB DD RAM. In this, we implement the coding part using eclipse. Here the proposed techniques are used in the coding part to document file. Considering that as that it resists colllise attack done by denied clients adjusting with present user.To overcome from this we made a certificate in use by which no one can generate any valid PK combining their private keys. Our CP-ABE scheme is used to encapsulate AES key, which achieves fine-graind entry govern and efficiently enduser revocked. So, our focus on the estimation price performed on System The results of our experiment give result that it is efficient for resource constrained devices.

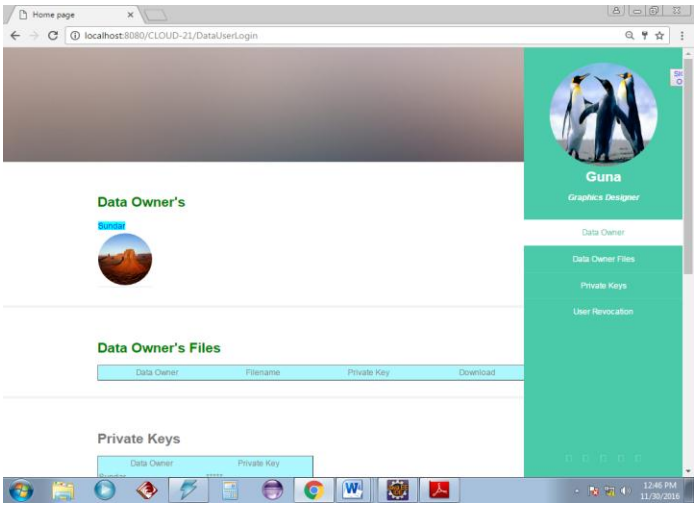

Fig.5.1:Data Owner login

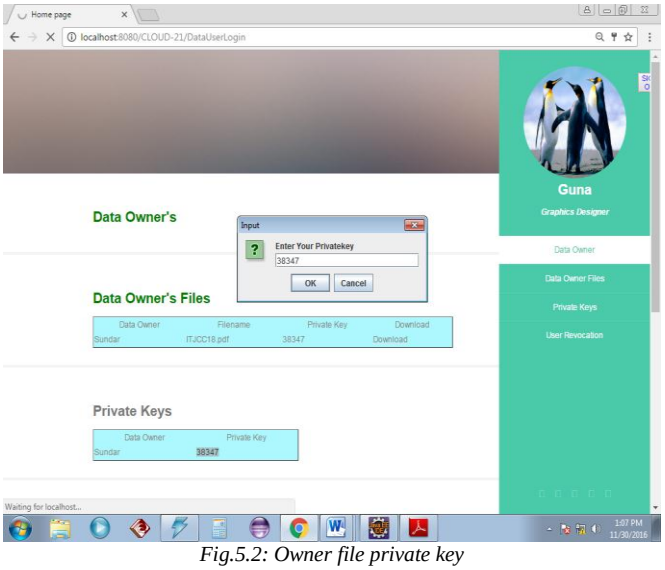

Fig.5.2: Owner file private key

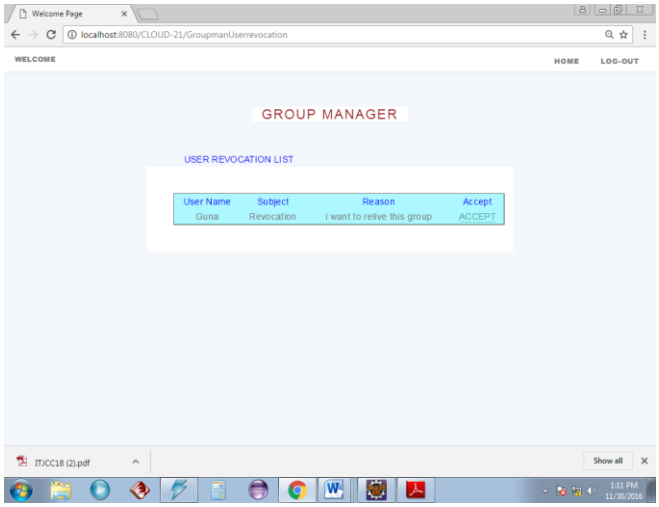

Fig.5.3:User Revocation Request.

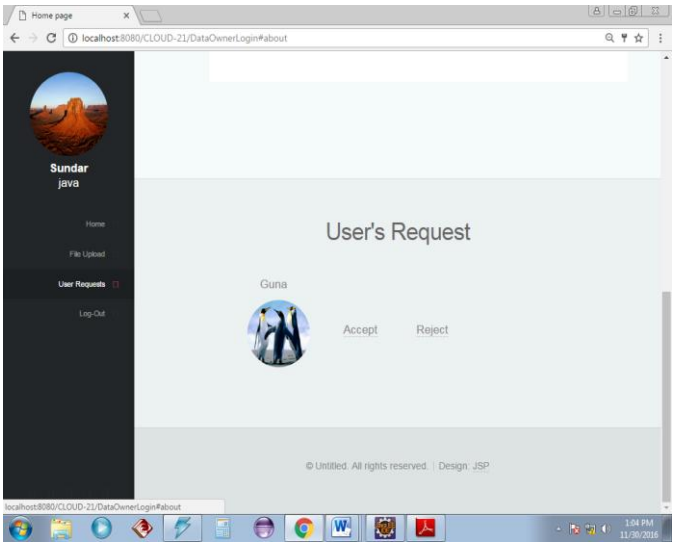

Fig.5.4: User Request To download a file.

VI. CONCLUSION AND FUTURE SCOPE

In this article, we provided a formal definition and security model for CP-ABE with user revocation. We also construct a concrete CP-ABE scheme which is CPA secure based on DCDH assumption. To resist collusion attack, we embed a certificate into the user's private key. So that malicious users and the revoked users do not have the ability to generate a valid private key through combining their private keys. Additionally, we outsource operations with high computation cost to E-CSP and D-CSP to reduce the user's computation burdens. Through applying the technique of outsource, computation cost for local devices is much lower and relatively fixed . The results of our experiment show that our scheme is efficient for resource constrained devices.
:

REFERENCES

[1] VG. Pandey, A. Sahai, B. Wates, *"Property Based Encryption for Fine-Grained Access Control of Encrypted Data"*, ACM Computer and Communications Security, Vol.4, Issue.2, pp.89-98, 2006,

[2] Y. Ming, L. Fan, H. Jing-Li, W. Zhao-Li, "*An Efficient Attribute Based Encryption Scheme with Revocation for Outsourced Data Sharing Control*", 2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control, Beijing, pp. 516-520, 2011.

[3] A. Sharma, RS Thakur, S. Jaloree, "*Investigation of Efficient Cryptic Algorithm for Storing Video Files in Cloud*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.6, pp.8-14, 2016.

[4] R. Lathwal, V.K. Saroha, "*A Study on Biometric Technology and Access Control System: Network Security*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.7, pp.31-35, 2014.

[5] M. Chase, *"Multi-authority Attribute Based Encryption"*, Proc. 4th Theory of Cryptography Conference, Berlin, pp. 515-534, 2007.

[6] Z. Liu, Z. Cao, Q. Huang, D.S. Wongand, T.H. Yuen, *"Fully Secure Multi-Authority Ciphertext-Policy Attribute-Based Encryption without Random Oracles"*, Proc.16th European Symposium on Research in Computer Security, Berlin, pp. 278-297, 2011.

[7] A. Sahai and B. Waters, "*Fuzzy Identity-Based Encryption"*, EUROCRYPT-LNCS, Vol. 3494, Issue. 8, pp. 457-473, 2005.

[8] J.G. Han, W. Susilo, Y. Mu, J. Yan, *"Privacy-Preserving Decentral-ized Key-Policy Attribute-Based Encryption"*, IEEE Transactions on Parallel and Distributed Systems, Vol.23, No.11, pp. 2150-2162, 2012.

[9] D. Boneh, M.K. Franklin, *"Identity-Based Encryption from theWeil Pairing"*, CRYPTO '01, LNCS, Vol. 2139, Issue.2, pp. 213-229, 2001.

[10] J. Hr and D. K. Noh, *"Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems"*, IEEE Transactions onParallel and Distributed Systems, Vol. 2, Issue.1, pp. 1214-1221,2011.

[11] P.K. Tyswski, M.A. Haan, *"Hybrid Attribute-Based Encryption and Re-Encryption for Scalable Mobile Applications in Clouds"*, IEEE Transactions on Cloud Computing, Vol. 5, Issue.8, pp. 172-186, 2013.

[12] J.W. Li, C.F. Jia, J. Li, X.F. Chen, *"Outsourcing Encryption of Attribute-Based Encryption with Mapreduce"*, Proc.14th International conference on Information and Communications Security, Berlin, pp.191-201, 2012.

[13] M. Green, S. Hohenberger, B. Waters, *"Outsourcing the decryption of ABE ciphertexts"*, USENIX, Vol.10, Issue.8, pp. 1-34, 2011.

[14] H.L. Qian, J.G. Li, Y.C. Zhang, *"Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption with Fully Hidden Ac-cess Structure"*, Proc.15th International ConferenceonInformation and Communications Security, Berlin, Vol. 23, Issue. 4, pp.363-372, 2013.

[15] J.T .Ning, Z.F. Cao, X.L. Dong, L.F. Wei, X.D. Lin, *"Large Universe Ciphertext-Policy Attribute-Based Encryption with White-Box Trace-ability"*, Proc.19th European Symposium on Research inComputer Security, Berlin, pp. 55-72, 2014.

Authors Profile

Ms. SHIKHA RAJPUT is currently pursuing Master of Computer Application from VIT University, Vellore. Her research interests are big data, cloud computing and software testing

Dr.M.Iyapparaja, He received his Ph.D in Information and communication Engineering from Anna University, Chennai. He published 20 international and national papers in reputed journals. He is currently working as Associate Professor in SITE School, VIT University, Vellore. His area of interest is Bigdata, Software Testing, Wireless sensor networks.