iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** I **Month of publication:** January 2024

DOI: https://doi.org/10.22214/ijraset.2024.57888

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

Shared Access Control using Triple DES in Decentralized Cloud

Manjusha N. Mahamune[1], Pooja D S[2], Rashmi[2], Sri Guru Darshan R[4]
[1]*Asst. Professor,* [2, 3, 4]*Students, CSE Department, T John Institute Of Technology, Visvesvaraya Technological University*

Abstract: ***As Cloud computing is a new emergent technology despite having many beneficial factors, it faces many threats in various ways. To give the security with degrading the performance. In this project we propose an access control model featured with the efficient key update function in data outsourcing environment. Our access control is based on the combination of triple DES and role based access control (RBAC).***
The certificate is distributed in the form of token generated by the system and sent through the mail for secure transaction. In Our project a user's key is incorporated into the token which will be used to decrypt the triple DES based on role based. This 3DES and RBAC together makes hybrid encryption and can be accessed using token generated key of that role user.
This significantly reduces the overheads in updating and distributing keys of all users simultaneously compared to the existing 3DES based schemes. Decentralized Multi-Authority ABE (DMA), which is derived from 3DES that is resilient to these types of misbehaviour. Our system distinguishes between a data owner (DO) principal and attribute authorities (AAs): the DO owns the data but allows AAs to arbitrate access by providing attribute labels to users. The data is protected by policy encryption over these attributes.
Finally our system is highly secured as hybrid encryption on 3DES and RBAC to secure the data and key to decrypt is token generated and shared in the distributed system. The decentralized system helps in the parallel computing the secure transaction between the users efficiently with high performance in cloud.
Keywords: Cloud Computing, Data Encryption Standard (DES), Authentication, Attribute Based Encryption(ABE), Decentralized

I. INTRODUCTION

Cloud computing is one of the widely used emerging technique that offers various methods to acquire and manage IT resources on a large-scale.
Cloud computing, in turn, provides different types of services such as Infrastructure-as-a-service (IaaS) also sometimes called as hardware as a service (HaaS), Platform-as-a-service (PaaS) and Software-as-a-service (SaaS). Cloud computing planning promotes the resource sharing in a pure plug and provides a model that dramatically simplifies its infrastructure.
As Cloud computing is a new emergent technology despite having many beneficial factors, it faces many threats in various ways. To give the security with degrading the performance. In this project we propose an access control model featured with the efficient key update function in data outsourcing environment. Our access control is based on the combination of 3DES and RBAC
The certificate is distributed in the form of token generated by the system and sent through the mail for secure transaction. In Our project a user's key is incorporated into the token which will be used to decrypt the 3DES policy based on role based. This 3DES and RBAC together makes hybrid encryption and can be accessed using token generated key of that role user.
This significantly reduces the overheads in updating and distributing keys of all users simultaneously compared to the existing 3DES based schemes. Decentralized Multi-Authority DES (DMA), which is derived from DES that is resilient to these types of misbehaviour. Our system distinguishes between a data owner (DO) principal and attribute authorities (AAs): the DO owns the data but allows AAs to arbitrate access by providing attribute labels to users. The data is protected by policy encryption over these attributes.
Finally, our system is highly secured as hybrid encryption on 3DES and RBAC to secure the data and key to decrypt is token generated and shared in the distributed system. The decentralized system helps in the parallel computing the secure transaction between the users efficiently with high performance in cloud.

II.LITERATURE REVIEW

M. Armbrust, A. Fox, et.al [1], have proposed to give the hindrances are conquer, the cloud computing can perhaps change a vast part of IT industry, building programming more alluring as a management and decoration the way. Its equipment is composed and obtained. Engineer has the creative opinions for new intuitive web do not benefits require the substantial money costs in equipment to send their management or the human money to work. Need not be as concerned as about done provisioning to management whose level do not meet their prospects, therefore missing potential clients and income.

Administrations with extensive clump arranged activities can get their outcomes as soon as their projects can evaluate utilizing 1000 servers single hour price close for utilizing single server for 1000 hours. Properties, without giving a finest for substantial scale is strange ever.

The economies of size of substantial scale server farms consolidated with "pay as you go" asset use has proclaimed the ascent of cloud computing. It is currently alluring to send a creative new network access on the outsider web server farm instead of your own system, and to effortlessly scale its assets as it develops or decreases in notoriety and income.

Growing and contracting every day in light of ordinary diurnal examples could bring down expenses considerably further. Cloud computing exchanges the dangers of over provisioning or under provisioning to the cloud computing supplier, who mitigates that hazard by factual multiplexing over a much bigger arrangement of clients and who offers moderately low costs because of better use and from the economy of acquiring at a bigger scale. We characterize terms, show a financial model that amounts the key purchase versus pay as you go choice, offer a range to group cloud computing suppliers, and give our perspective of the main 10 hindrances and chances to development of cloud computing.

M. Green, S. Hohenberger and B.Water , et.al, have proposed to characteristic based encryption is another vision for open key encryption that permits clients to encode and decode messages in view of client qualities, the new worldview for ABE that to a great extent dispenses with this overhead for clients.

Assume that ABE figure writings are put away in the cloud. It indicates how the client can furnish the cloud with single change key that allows the cloud to de-cipher any ABE figure content satisfied by those clients qualities into a consistent size without the cloud having the capacity to peruse any part of the clients' messages. To definitely characterize and show the benefits of this procedure they give new security definitions to both CPA and repayable CCA security without-sourcing a few new developments a usage of our calculations and nitty gritty execution estimations. The average setup the client spares essentially on both transfer speed and unscrambling time, without expanding the quantity of transmissions.

J. Lai, R.H.Deng, have proposed the Attribute-based-encryption is one of the various encryption that grants customers to encrypt and translate data in perspective of customer qualities. A promising use of this is versatile access control to mixed data set in the cloud using access regulates and acknowledged attributes associated for private keys and figure compositions. Key efficiency disservices of the current A B E arrangements is that unscrambling incorporates unreasonable mixing operations and the cost of such processes creates with the complexity of the passage approach.

Safety of an ABE system without-sourced unscrambling guarantees that a foe don't have the capability to study anything about the encrypted data, be that as it might doesn't give the accuracy of the change complete by the cloud. They portray about the new prerequisite of ABE with outsourced unravelling that is undisputable status, casually, certainty ensures that a client can proficiently check if the change is done accurately. At long last it demonstrates a usage.

Starting late they proposed an ABE framework with outsourced de ciphering that by and large wipes out the unscrambling overhead for customers. A customer gives an un-trusted server say a fogs organization dealer with a key that allows the cloud to decode any A B E figure content satisfied by that customer's qualities or access course of action into a direct figure substance and it just secures somewhat computational overhead for the customer to recover the plain substance from the changed figure.

To correctly characterize and show the upsides of this procedure they give new safety definitions to both CPA and repayable CCA security without-sourcing a few new developments a usage of our calculations and nitty gritty execution estimations. The run of the mill setup the client spares altogether on both transfer speed and decoding time, without expanding the quantity of transmissions.

A.Lewko, et.al, have proposed a multi power based encryption ABE system any part can get to be power and there is no necessities for any worldwide co-appointment other than the making of an underlying arrangement of basic reference parameters. A gathering can just go about as an ABE by making an open key and issuing private key to various clients that mirror their qualities. A client can scramble information as far as any Boolean recipe over properties issued from any picked set of power. At last, our system does not require any focal power.

ABE framework with outsourced translating that, all things considered, takes out the unscrambling overhead for customers. A customer gives an untrusted server say a fogs organization dealer with a key that allows the cloud to translate any A B E figure

content satisfied by the customer's qualities or access course of action into an essential figure substance and it just achieves somewhat computational above for the customer to recover the plain substance from the alternate figure content.

To definitely characterize and show the benefits of this procedure they give new security definitions to both CPA and repayable CCA security without-sourcing a few new development execution of our calculations and point by point execution estimations. The regular setup the client spares essentially on both data transfer capacity and decoding time, without expanding the quantity of transmissions.

Earlier attribute based encryption systems accomplished plot resistance when the ABE system power together distinctive segment of a client's private key by randomizing the key. Be that as it may, in our system every segment will originate from a possibly diverse power where we accept no co-appointment between such powers. So the tie key segments are made and it additionally averts crash assaults between clients with various worldwide identifiers.

B. Waters, et.al, have proposed the new strategy for acknowledging figure content approach characteristic encryption (CP-ABE) below adhesive and non-intelligent crypto graphic suppositions in the typical model.

The answer for this permits any excerptor to determine access control as far as any entrance recipe over the qualities in the system. All together the most productive system, figure content extent and unscrambling time scale directly with multifaceted nature of the entrance equation.

The main past work to accomplish these parameters constrained to a resistant in the bland gathering model.

The tri developments in our model are presented, firstly system is demonstrated specifically safe under a suspicion that they call the decisional parameter diffie-hellman type presumption which can be seen as a speculation of the diffie-hellman example supposition.

B. Parno, M. Raykova, et.al, have proposed the wide assortment of little computationally feeble gadgets, and the developing number of computationally serious errands makes the appointment just when the reimbursed result can be reliable, which makes unquestionable calculation an absolute necessity for such situations. In this work they augment the meaning of obvious calculation in two vital bearings they are open designation and open obviousness, which have the vital application in numerous pragmatic assignment situations.

As the essential commitment of our work they set up a vital and association between undeniable calculation and properties based encryption, a primitive that has been broadly examined. They are undeniable nature calculation plan with open appointment and open obviousness from any ABE plan.

The tri developments inside our structure are presented, firstly system is demonstrated specifically secure under a suspicion that they call the decisional parameter diffie-hellman example supposition which can be understood as a speculation of the diffie-hellman type presumption.

The VC plan checks any capacity in the class of capacities encased by the reasonable ABE approaches. This plan appreciates an extremely effective confirmation calculation that depends just on the yield size. Reinforcing this association it demonstrates the development of multi-capacity confirmable calculation plan from an ABE with outsourced unscrambling an antiquated characterized as of late.

S. Yamada, N.Attrapadung, B.Santoso, et.al, have proposed the certainty of predicate encryption. An evident predicate encryption plan ensures that every honest to goodness beneficiary of a figure content will get the same message upon decoding. While undeniable nature of predicate encryption may be an alluring attribute without anyone else, we besides demonstrate that this attribute empowers intriguing applications. In particular, we give two uses of certain predicate encryption.

Firstly, we demonstrate that for a substantial class of undeniable predicate encryption plan, it is constantly conceivable to change over a picked plaintext secure plan into a picked figure content secure one.

Besides, we demonstrate that an unquestionable predicate encryption plan permits the development of a deniable predicate validation plan. This primitive empowers a client to validate a message to verifier utilizing a private key fulfilling a predetermined connection while in the meantime permitting the client to deny always having communicated with the verifier. This plan moreover ensures the secrecy of the client as in the verifier will learn nothing about the client's private key aside from that is fulfills the predetermined connection.

Lastly it shows that many currently known establish encryption arrangement which do not provide verifiability can be easily converted into schemes providing verifiability.

The results not only highpoint that verifiability is a very useful attribute of establish encryption, but also show that efficient and practical arrangements with this attribute can be obtained relatively easily.

III.METHODOLOGY

A. *Proposed System*

The below Figure describes that based on the algorithm used to produce the key, each key is generated for every file and is unique in nature. When files are uploaded in a batch, both the individual file key and the aggregate key for the entire batch of files are generated. The user who uploaded the files retains the aggregate key, which is only valid for that specific batch. The key generated for the file or the aggregate key generated by that batch of files can be used to open the file. The user can transfer the file and grant access to it by other users when he wants to share a file with them.

B. *Digital Token Generating*

Key structures were designed to preserve the security of the outsourced data. Key structures are derivatives from the user common attributes like roles. The formation of key structure assigns the access privileges to the set of the common users over the outsourced data. Using Pseudo Random algorithm produces unique big length keys using 256 characters

Pseudo Random Key Generation algorithm

Step 1. Generate 32 pseudo-random bytes with the seed key generator (described below), adding the user-supplied seed, U, if any.
Step 2. Set the 192-bit Triple DES key, K, as the first 24 bytes generated in step 1, and set the seed, S, as the last 8 bytes [Note 1].
Step 3. Set D as a 64-bit representation of the current date and time [Note 2].
Step 4. Generate the 64-bit block X0 = G(S, K, D) where G is the X9.17 RNG algorithm described in ANSI X9.17 Appendix C/ANSI X9.31 Appendix A, and where S is updated as per that algorithm.
Step 5. Set up to carry out continuous random number generator tests:
If X0 equals L or X0 equals P, stop and notify a failure of the continuous random number generator test.
Set L = X0 and store in thread-safe memory for the next call.
Set P = X0.
Step 6. For R = N until R is equal to zero, do:
Generate a 64-bit block X = G(S, K, D), updating S in the process (see below).
If X equals the previously-generated block, P, then stop and notify a failure of the continuous random number generator test [Note 3].
Set B = the lesser of R and 8.
Output B bytes from X. [Note 6]
Set R = R - B.
Set P = X.
Step 7. Generate a final block Xf = G(S, K, D) and set P = Xf [Note 3].
Step 8. Zeroise K, S, D, X and any other internal buffers used. Retain L and P for subsequent use.

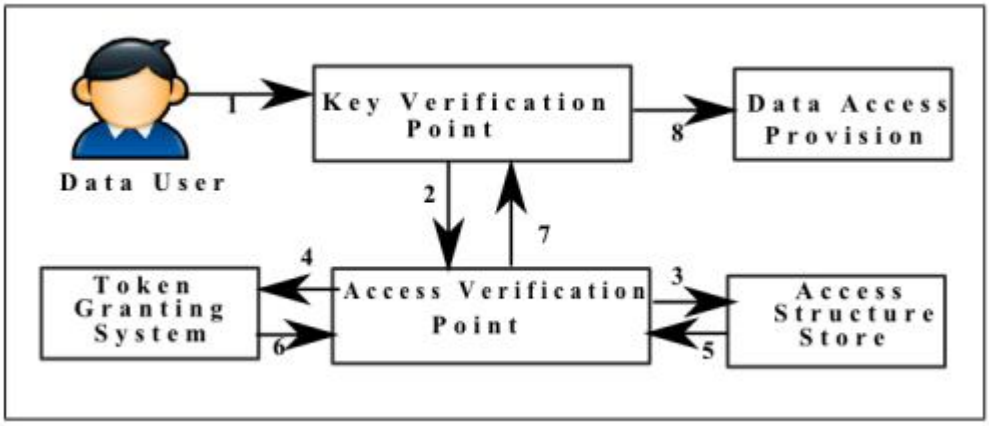


Fig. 1 Digital Token generating Algorithm

IV. CONCLUSION

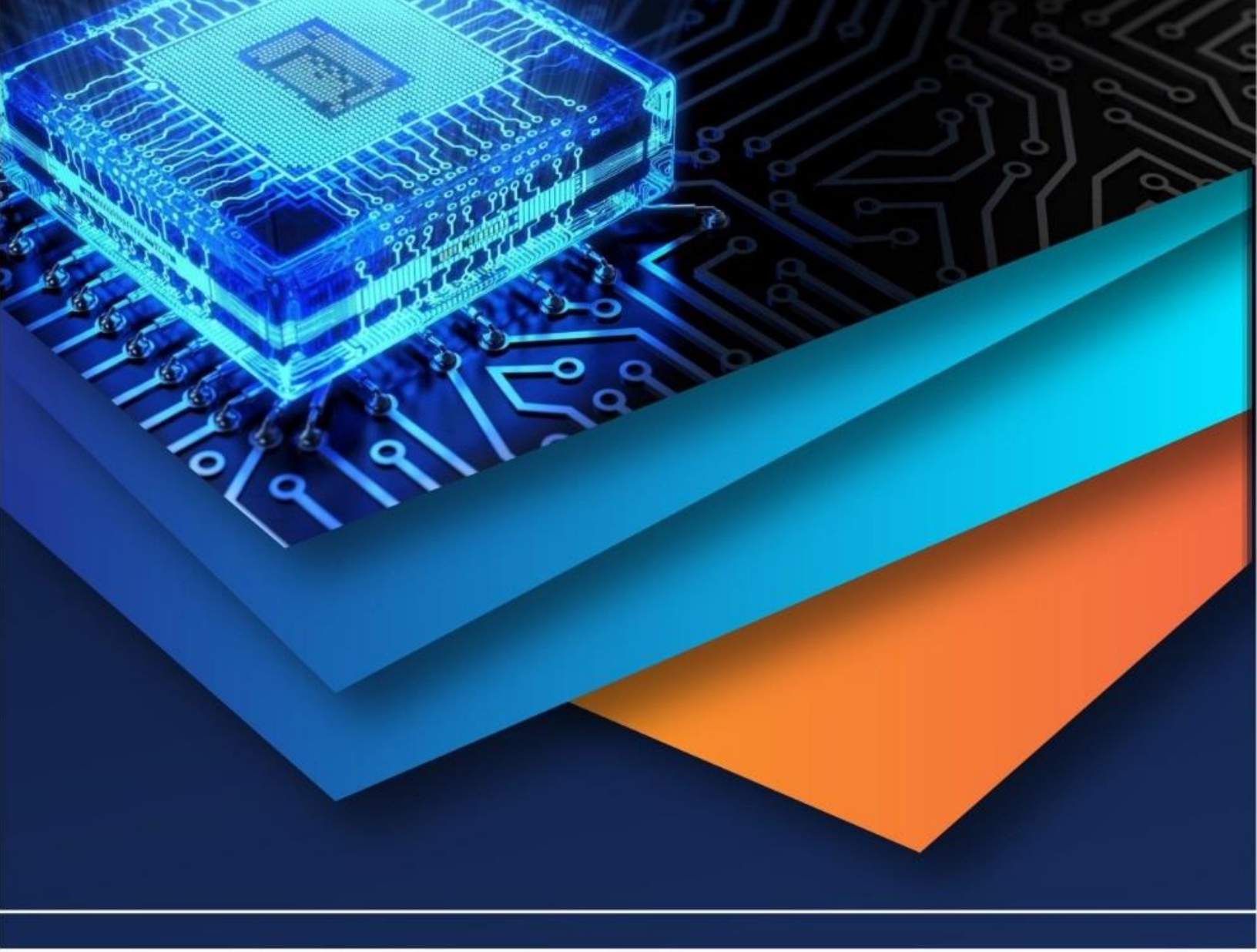
The route cipher text policy attributes-based-hybrid encryption with conformable authorization scheme. So the circuits are castoff to direct the solidest procedure of access control policy. Combined conformable calculation and encrypt with cipher text policy attribute based hybrid encryption, we could authorized the conformable partial decryption example to the server.

Then again, we actualize our plan over the whole numbers. The expenses of the calculation and correspondence utilization demonstrate that the plan is down to earth in the distributed computing. In this manner, we could smear it to guarantee the information secrecy, the fine grained access control similar approval in cloud. In the hybrid encryption there are several keys namely, random encryption, symmetric, one time verified key for different purpose enhance the security of the system. The key distribution for accessing the file on the cloud and to decrypt that we use the gmail service to distribute the generated key among the data consumer. The major security is given with registration on system also system embeds the voice authentication to login this enhance the high security. As the data owner and data user list is stored. Therefore as this system is highly secured with integration of all the technologies. The system is more secured against malicious attacks. Hence we conclude that our system is highly secured and highly efficient system.

We have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.

REFERENCES

[1] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556-563, 2012.
[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June2012.
[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search Over Encrypted Data.
[4] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role- Based Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.
[5] H.K. Maji, M. Prabhakaran, and M. Rosulek ,"Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.
[6] H.K. Maji, M. Prabhakaran, and M. Rosulek,"Attribute Based Signatures," Topics in Cryptology- CT-RSA, vol. 6558, pp. 376-392, 2011.
[7] Singh, Gurpreet, and A. Supriya. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", IJCA 67.19,pp-33-38, 2013.
[8] M. G. Jaatun, A. A. Nyre, S. Alapnes, and G. Zhao, "A farewell to trust: An approach to confidentiality control in the Cloud." pp. 1-5.
[9] T. K. Chakraborty, A. Dhami, P. Bansal, and T. Singh, "Enhanced public auditability & secure data storage in cloud computing." pp. 101-105.
[10] Randeep Kaur, Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (ISSN 2319 - 4847),Volume 3 Issue 3, pp.171-176, March 2014.
[11] Enhancing Data Storage Security in Cloud Computing Through
[12] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," IACR Cryptology ePrint Archive, p. 419, 2012.
[13] A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.
[14] J. Hur and D. Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY