ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2350-0174
Vol.03, Issue.04
June-2023
Pages: 840-851

A Survey on Light Weight Secure data sharing scheme by using ABE and CP-ABE

[1] *M. Tech., Dept of CSE, Sri Vasavi Institute of Engineering & Technology. AP, India,* uma.vaka23@gmail.com
[2]*M. Tech., Dept of CSE, Sri Vasavi Institute of Engineering & Technology. AP, India,* anilkumar.nuthakki14@gmail.com

Abstract: - With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computationally intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program-based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments.

Keywords-ABE, CP-ABE, cloud storage, DriveHQ. Cryptography

I. INTRODUCTION:-

The real fact that Attribute Based Encryption has demonstrated its benefits, client renouncement and Attribute denial is the essential concerns. The denial issue is much progressively troublesome particularly in Cipher Text Policy-Attribute Based Encryption plans, in light of the fact that each Attribute is shared by numerous clients. This implies repudiation for any property or any single client may influence different clients in the framework. As of late, some work has been proposed to equipment this issue in productive manners. Productive renouncement, which is additionally appropriate for Key Policy- Attribute Based Encryption All things considered, it isn't evident whether their plan is appropriate for Cipher Text Policy-Attribute Based Encryption. Characteristic based information offering plan to quality denial capacity.

2.2 Attribute Based Encryption Over View:-

This plan was demonstrated that it's a secure data against picked original data leaked in light of data assumption. Be that as it may, the length of secure data and client's secret key are relative to the quantity of qualities in the characteristic universe. In the key age, encryption and decoding stages, calculation includes all properties in the Attribute universe. Subsequently, it is costly in correspondence and calculation cost for clients. It supports technique to perform client renouncement activity by joining Cipher Text Policy-Attribute Based Encryption with re-encryption. In their plan, every client has a place with a gathering and holds a gathering secret key gave by the gathering. Be that as it may, their plan doesn't avoid agreement physically attack performed by revoked clients collaborating with existing clients. The explanation is that every client's gathering secret key is same in a similar gathering. The properties of the renounced clients can be utilized by the client in a similar gathering without the predetermined attributes. Moreover, we bring up that there is a similar security chance in the plans through applying Attribute Based Encryption plans to distributed storage administrations, we can both guarantee the security of put away information and accomplish fine-grained information access control. Tragically, Attribute Based Encryption plan requires high calculation overhead during performing encryption and unscrambling tasks. This deformity turns out to be increasingly extreme for lightweight devices because of their compelled registering assets. To diminish the calculation cost for asset compelled devices, some cryptographic tasks with high computational burden were re-appropriated to cloud specialist organizations intermediary re-encryption with languid re-encryption procedure, structured a Key Policy- Attribute Based Encryption conspire with fine-grained information access control. This plan necessitates that the root hub in the entrance tree is an AND door and one kid is a leaf hub which is related with the fake Attribute. The fake credit is required to be incorporated into each datum report's Attribute set and will never be refreshed. In their plan, cloud specialist organization stores the entire private key segments for user's private key apart from the one relating to the spurious quality Be that as it may, cloud specialist organization doesn't gain proficiency with the plaintext for any information record. There are few entities while encrypting data before uploading inside online cloud server.

Symbol	Description
TA	Trusted Authority
GM	Trusted Group Manager
DO	Data Owner
DU	Data User
CSS	Cloud Storage Server
E-CSP	Encryption-Cloud Service Provider
D-CSP	Decryption-Cloud Service Provider

Table 2.1 Explanation of Symbols

The secure data Cipher Text Policy-Attribute Based Encryption conspire with client denial; we expect that a client's private key incorporates two sections. One is related with his approved properties and the other one is related with the gathering which he has a place with. At the point when at least one data receiver leave the gathering, GM updates gathering key pair and updates private keys for existing clients. To disavow their entrance capacity to the put away information, GM likewise applies for re-encryption tasks from CSS. A work process of all calculations is portrayed in below figure. A Cipher Text Policy-Attribute Based Encryption plot with client disavowal comprises of the accompanying proper calculations.

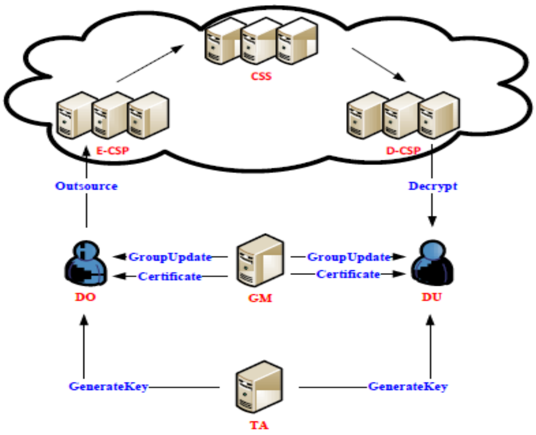

Figure 2.1 Architecture of Storage System

2.2.1 Performance Evaluation

Attribute Based Encryption Storage System build on Cipher Text Policy-Attribute Based Encryption scheme .Lets the parameters $|pars|$, $|msk|$, $|CT|$, $|L|$, $|T|$, $|SK|$, $|A|$ be the sizes of the parameters open parameter, ace private key, figure message, the attribute, the attached data , the decoding key and the entrance structure, separately . Connote l by the quantity of properties in a passageway structure, and k by the size of a credit set ascribed to a customer's confirmations. Table 1 takes a gander at the limit multifaceted nature of our structure. Clearly our structure is capable as far as the introduced accumulating overhead, which incorporates the essential Cipher Text Policy-Attribute Based Encryption parts to the system open parameter and 3 segments to the figure content set away by the insecure cloud server, with an additional private cloud taking care of 3 segments. Allow l is for the amount of attributes displayed in a passageway structure, and k is the size of a characteristic set related with the private key. Show y by the amount of existing names set away by the private cloud. The Table shows the quantity of mathematical exponent and paring exercises in our storing system. For example, it requires everything considered k + 2 exponential exercises what's more, 3k + 1 paring assignments to translate figure content. The above Table considers the computer related costs realized at the Data supplier the cloud, and the customer for one record storing our structure. It isn't inconvenient to see that the computational essential for the customer in our structure is twice that in the covered up Cipher Text Policy-Attribute Based Encryption Regarding the data provider, it requires 4 extra mathematical exponent assignments came about in view of the tag, name, affirmation and unauthorized access key despite the computational Cost of the concealed arrangement message in missing the mark on the capacity of secure de duplication. With respect to private cloud, our course of action takes 5 + (6l + 2) exponential exercises and 2y mixing exercises, among which 5 exponential assignments Are used to check the authenticity of the proof, 6l+2 exponential exercises are related to the figure content recuperation if vital additionally, 2y mixing exercises are resolved to check paying little heed to whether the normal text concealed in the redistributing sales has existed in the open cloud.

2.2.2 Variable attribute based Encryption:-

It shows cryptographic unrefined called versatile Cipher text Policy-ATTRIBUTE BASED ENCRYPTION, where a semi-accepted delegate is exhibited into the setting of Cipher Text Policy-Attribute Based Encryption. The middle person, given a system wide unauthorized access key, can change any figure message under one access methodology into figure writings of the comparable plaintext under some different access methodologies without adjusting any data related information about the plaintext during the technique of progress. Regardless, this strategy for using a lone unauthorized access key for all figure writings is extremely perilous, since if the single key is exchanged off, the security for the system will be totally broken. A badly arranged customer using the dealt unauthorized access key can recuperate a figure content into a passage Basic Model that? His/her characteristics satisfy, and thusly he/she can get the plaintext not expected for him/her. Also, the unauthorized access key is created by the AA who starting at now controls the unscrambling keys in the structure, so it is appealing to decrease its ability in controlling the encryption. Our framework is facilitated with the ultimate objective that each unauthorized access key must be used to change its contrasting figure content. As such, even in the end, a unauthorized access key is included; the mischief is limited to one message. At a raised level, our technique conveys another way to deal with creates adaptable CIPHER TEXT POLICY-ATTRIBUTE BASED ENCRYPTION outline works from a substitute viewpoint.

II. Related Work:-

Cipher Text Policy-Attribute Based Encryption Schema with Verifiable Secure Decryption

We at first propose another Cipher Text Policy-Attribute Based Encryption plan utilizing Waters' Cipher Text Policy-Attribute Based Encryption plots, which is shown to be explicitly CPA-secure. By then, considering the arrangement, we propose a Cipher Text Policy-Attribute Based Encryption plot with re-appropriated unscrambling and exhibit that it is explicitly CPA-secure and undeniable in the standard model. Starting late, the first Cipher Text Policy-Attribute Based Encryption plan that practiced full security was proposed. Since the central structure of the Cipher Text Policy-Attribute Based Encryption .We use, one can change our advancement frameworks to the Cipher Text Policy-Attribute Based Encryption plan proposed to achieve totally secure Cipher Text Policy-Attribute Based Encryption contrive with verifiable redistributed unscrambling in the standard

model.

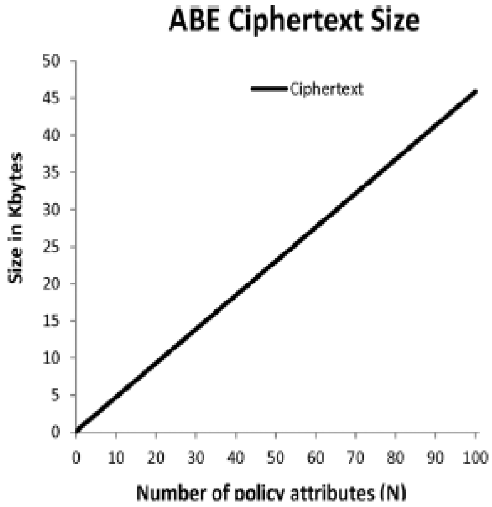

Figure 2.3.1(a) Calculating cipher text size

In a Cipher Text Policy-Attribute Based Encryption scheme, the complexity of cipher text arrangement impacts both the decryption time and the cipher text size. We create cipher text strategies in the form of (A_1,A_2……A_N) circumstance over the approach), where A_i is an Attribute.

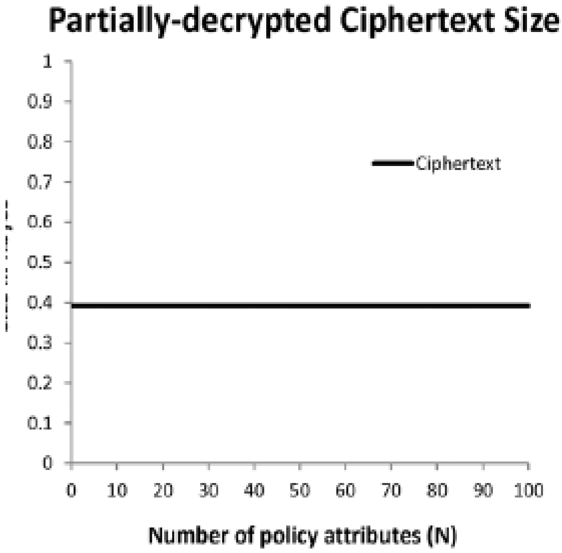

Figure 2.3.1(b) Partially Decrypted Cipher text size

The above Diagram represents the entire System will be depends upon the security if the secure decryption fails immediately the encrypted text doesn't support to decrypt properly.

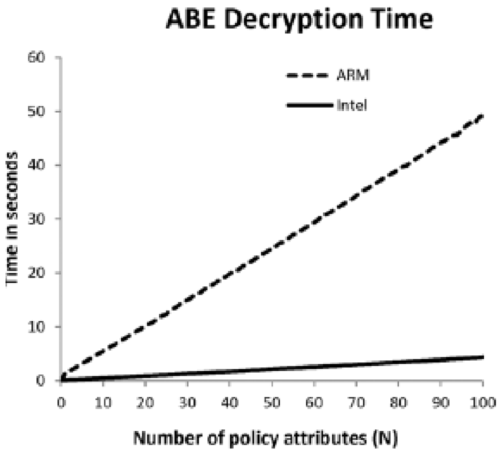

Figure 2.3.1 (C) Cipher Text Policy-Attribute Based Encryption Decryption Time

It shows the result of completely decrypted text time and the functions only allows to user after generated keys.

2.3.2 Cipher Text Policy-Attribute Based Encryption System with Outsourced Decryption

Consider a cloud based electronic therapeutic record structure in which patients' helpful records are guaranteed using Cipher Text Policy-Attribute Based Encryption plans with redistributed unraveling and are taken care of in the cloud. In order to beneficially get to patients' remedial Records on her mobile phone, a pro delivers and delegates a change key to a mediator in the cloud for re-appropriated translating; given a changed figure content from the middle person, the pro can scrutinize a patient's restorative record by just playing out a clear advance of count. If no check of the rightness of the change is guaranteed, in any case, the structure may continue running into the going with two issues:

1) With the ultimate objective of saving enlisting cost, the mediator could reestablish a medicinal record changed heretofore for a comparable authority

2) Because of system breakdown or malignant ambush, the go-between could send the helpful record of another patient or an archive of the correct structure in any case, passing on erroneously information.

The result of treating the patient subject to off kilter information could be extreme or on the other hand even disastrous. The above observation rouses us to inspect Cipher Text Policy-Attribute Based Encryption with apparent re-appropriated unscrambling in this paper. We highlight that an Cipher Text Policy-Attribute Based Encryption contrive with secure redistributed unraveling doesn't generally guarantee certain nature For example, the safe Cipher Text Policy-Attribute Based Encryption plans with re-appropriated disentangling.

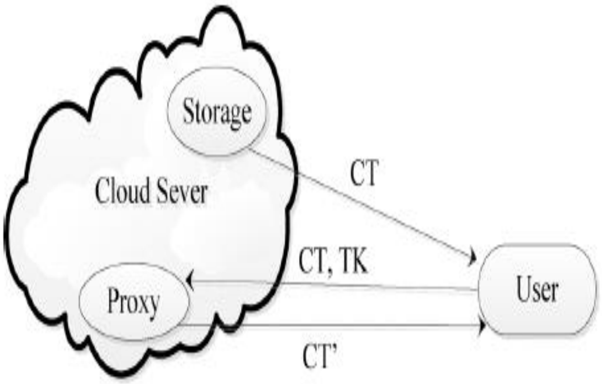

Figure 2.3.2 Cipher Text Policy-Attribute Based Encryption System with outsourced decryption

Intermediary re encryption: In Cipher Text Policy-Attribute Based Encryption with redistributed unscrambling, a customer outfits the cloud with a change key that allows the cloud to unravel a Cipher Text Policy-Attribute Based Encryption figure message on message into an essential figure message on the comparable, without grabbing anything about. This is reminiscent of the possibility of middle person re encryption.

Delegate re encryption allows a middle person, using are encryption key, to change an encryption of under Alice's open key into an encryption of the identical under Bob's open key without the mediator grabbing anything about the encoded

Message. We underscore that in the model of go-between encryption; proof of the mediator's change can't be cultivated. This can be immediately explained as seeks after. A mediator could replace the encryption of under Alice's open key with the encryption of another message under Alice's open key and after that usage its re encryption key to change the last into an encryption of under Bob's open key. Plainly, without participation with Alice, Bob can't perceive this threatening behavior of the middle person.

2.3.3 Cipher Text Policy- Attribute Based Encryption with outsourced Decryption

In the first model characterized in, a Cipher Text Policy-Attribute Based Encryption conspire with re-appropriated decoding comprises of five calculations: furthermore, . A trusted gathering utilizes the calculation to produce the open parameters also, an ace mystery key, and uses to produce a private key and a change key for a client. Taking as input the change key given by a client and a cipher text, the cloud can utilize the calculation to change the cipher text into a straightforward cipher text if the client's quality fulfills the entrance structure related with the cipher text; at that point the client utilizes the calculation to recuperate the plaintext from the changed cipher text, the contribution to the calculation incorporates just the private key of the client and the changed cipher text, yet does exclude the first cipher text. As a result of this oversight of the first cipher text, it is preposterous to expect to develop a Cipher Text Policy-Attribute Based Encryption Plot with evident redistributed unscrambling under the definition. This can be clarified as pursues. A pernicious cloud could supplant the cipher text it assumes to change with a cipher text of an alternate message, and after that change the last into a straightforward cipher text utilizing its change key. Clearly, the client can't recognize this vindictive conduct of the cloud since the contribution to the calculation doesn't incorporate the first cipher text required to be changed. In request to accomplish certainty, we have to adjust the model of Cipher Text Policy-Attribute Based Encryption with re-appropriated decoding. We now officially depict our new model. A Cipher Text Policy-Attribute Based Encryption conspires with re-appropriated unscrambling comprises of the accompanying seven calculations.

2.3.4 Verifiable Delegation Technique

Verifiable Delegation (VD) is utilized to ensure approved clients from being misdirected during the assignment. The information proprietor scrambles his message M under get to arrangement f, at that point registers the supplement circuit if, which yields the contrary piece of the yield of f, and scrambles an arbitrary component R of the equivalent length to M under the arrangement. The clients can at that point redistribute their unpredictable access control approach choice what's more, part procedure of unscrambling to the cloud. Such expanded encryption guarantees that the clients can get either the message M or the irregular component R, which maintains a strategic distance from the situation when the cloud server misdirects the clients that they are not fulfilled to the entrance strategy, be that as it may, they meet the entrance arrangement really. In Cipher Text Policy-Attribute Based Encryption we utilize a half breed variation for two reasons: one is that the circuit Cipher Text Policy-Attribute Based Encryption is a piece encryption, and the other is that the validation of the assigned cipher text ought to be ensured. The cipher text of the half breed VD-CP Cipher Text Policy-Attribute Based Encryption framework is separated into two segments: the Cipher Text Policy-Attribute Based Encryption for circuits it makes up the key exemplification component part, and a symmetric encryption in addition to the encode make up the verified encryption component (AC) part. Each KEM encodes an irregular bunch component and afterward maps it by means of key determination capacities into a symmetric encryption key and a once checked key vk. At that point the irregular encryption key dk is utilized to encode the message of any length. vk and the information proprietor's ID are utilized to check the Macintosh of the cipher text. Just when the server portion not produce the first cipher text and react a right halfway unscrambled cipher text, the client might appropriately approve the MAC. For usage, the ongoing work on multi linear maps over the numbers is applied to reproduce conspire in the GMP library in VC 6.0. Despite the fact that the activity time for the matching in the multi linear guide is considerably more than the one in the bilinear guide, we could accomplish the most grounded general circuits get to approach up to now. Moreover, by utilizing undeniable assignment, the activity time for the client is short and autonomous of the unpredictability of the circuit. For the security, we demonstrate that the IND-CPA secure KEM consolidates with the IND-CCA secure verified (symmetric) encryption plan yields our IND-CPA secure mixture VD-CP Cipher Text Policy-Attribute Based Encryption plot.

2.3.5 Security Model

In our passage control system, the cloud is believed to be "straightforward however inquisitive", which resembles by far most of the related compositions in the subject of cloud secure amassing: On one hand, it offers reliable accumulating organization and viably executes every computation key various components; On the other hand, it may endeavor to increment unapproved information for its very own advantages. Past the cloud, the whole structure includes one CA, various owners and customers, wherein CA is believed to be totally trust, while customers can be dangerous. CA is responsible for key course and time token disseminating. We acknowledge that a dangerous customer may endeavor to unscramble the figure content to gain UN affirmed data unquestionably, consolidating plotting with different customers. The proposed TAFC can comprehend a fine-grained and coordinated discharge get to control system: Only a customer with satisfied property set can get to the data after the allocate time.

III. Literature Survey:-

1) A technique for computer detection and correction of spelling errors AUTHORS: F. J. Damerau

The method described assumes that a word which cannot be found in a dictionary has at most one error, which might be a wrong, missing or extra letter or a single transposition. The unidentified input word is compared to the dictionary again, testing each time to see if the words match—assuming one of these errors occurred. During a test run on garbled text, correct identifications were made for over 95 percent of these error types.

2) LIBSVM: A library for support vector machines

AUTHORS: C.-C. Chang and C.-J. Lin

LIBSVM is a library for Support Vector Machines (SVMs). We have been actively developing this package since the year 2000. The goal is to help users to easily apply SVM to their applications. LIBSVM has gained wide popularity in machine learning and many other areas. In this article, we present all implementation details of LIBSVM. Issues such as solving SVM optimization problems theoretical convergence multiclass classification probability estimates and parameter selection are discussed in detail.

3) Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs

AUTHORS: J. Ma, L. K. Saul, S. Savage, and G. M. Voelker

Malicious Web sites are a cornerstone of Internet criminal activities. As a result, there has been broad interest in developing systems to prevent the end user from visiting such sites. In this paper, we describe an approach to this problem based on automated URL classification, using statistical methods to discover the tell-tale lexical and host-based properties of malicious Web site URLs. These methods are able to learn highly predictive models by extracting and automatically analyzing tens of thousands of features potentially indicative of suspicious URLs. The resulting classifiers obtain 95-99% accuracy, detecting large numbers of malicious Web sites from their URLs, with only modest false positives.

4) Design and evaluation of a real-time URL spam filtering service

AUTHORS: K. Thomas, C. Grier, J. Ma, V. Paxson, and D. Song

On the heels of the widespread adoption of web services such as social networks and URL shorteners, scams, phishing, and malware have become regular threats. Despite extensive research, email-based spam filtering techniques generally fall short for protecting other web services. To better address this need, we present Monarch, a real-time system that crawls URLs as they are submitted to web services and determines whether the URLs direct to spam. We evaluate the viability of Monarch and the fundamental challenges that arise due to the diversity of web service spam. We show that Monarch can provide accurate, real-time protection, but that the underlying characteristics of spam do not generalize across web services. In particular, we find that spam targeting email qualitatively differs in significant ways from spam campaigns targeting Twitter. We explore the distinctions between email and Twitter spam, including the abuse of public web hosting and redirector services. Finally, we demonstrate Monarch's scalability, showing our system could protect a service such as Twitter--which needs to process 15 million URLs/day--for a bit under $800/day.

5) Detecting spammers on social networks

AUTHORS: G. Stringhini, C. Kruegel, and G.

Social networking has become a popular way for users to meet and interact online. Users spend a significant amount of time on popular social network platforms (such as Facebook, MySpace, or Twitter), storing and sharing a wealth of personal information. This information, as well as the possibility of contacting thousands of users, also attracts the interest of cybercriminals. For example, cybercriminals might exploit the implicit trust relationships between users in order to lure victims to malicious websites. As another example, cybercriminals might find personal information valuable for identity theft or to drive targeted spam campaigns.In this paper, we analyze to which extent spam has entered social networks. More precisely, we analyze how spammers who target social networking sites operate. To collect the data about spamming activity, we created a large and diverse set of "honey-profiles" on three large social networking sites, and logged the kind of contacts and messages that they received. We then analyzed the collected data and identified anomalous behavior of users who contacted our profiles. Based on the analysis of this behavior, we developed techniques to detect spammers in social networks, and we aggregated their messages in large spam campaigns. Our results show that it is possible to automatically identify the accounts used by spammers, and our analysis was used for take-down efforts in a real-world social network. More precisely, during this study, we collaborated with Twitter and correctly detected and deleted 15,857 spam profiles.

Proposed Algorithm:-

IV. Conclusion:-

In recent years, many studies on access control in cloud are based on attribute-based encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resources. In this paper, we Trapdoor creates encryption strategies that use cipher text policy attributes when the software uploads and saves the time if the key is not correctly identified as an incorrect user. With the arrangement A, a trapdoor key is given to the private cloud that is produced by an information supplier alongside the figure material c. For Strategy A and other Figure C material a new A0 entrance strategy without understanding the fundamental message M can be used for the private cloud to turn over the Figure c content. It helps the private cloud to retrieve figural material for the corresponding secret document by means of an entry technique, when two suppliers of information pass two figures relating to a similar record, but under different access arrangements An and A0. The Trapdoor Schussed and the figure message are located in the general public cloud rather than the previous one. The key test for secure de-duplication is to insure that a legitimately generated message is not misrepresented substituted by a fake copy attack. In such an attack, the malicious customer will block a re- appropriation request and alter the figure content afterwards.

propose LDSS to address this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud. The experimental results show that LDSS can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud. In the future work, we will design new approaches to ensure data integrity. To further tap the potential of mobile cloud, we will also study how to do ciphertext retrieval over existing data sharing schemes.

V.REFERENCES

[1] Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.

[2] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA: IEEE press, pp. 97-106, Oct. 2011.

[3] Qihua Wang, Hongxia Jin. "Data leakage mitigation for discertionary access control in collaboration clouds". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.

[4] Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Distributed System Security Symposium (NDSS), Feb. 2013.

[5] Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66, 2009.

[6] Maheshwari U, Vingralek R, Shapiro W. How to build a trusted database system on untrusted storage. in: Proceedings of the 4th conference on Symposium on Operating System Design & Implementation-Volume 4. USENIX Association, pp. 10-12, 2000.

[7] Kan Yang, Xiaohua Jia, Kui Ren: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.

[8] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control. in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006.

[9] Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data. in: Proceedings of Symposium on Security and Privacy (SP), IEEE press, 2007. 350- 364

[10] Cong Wang, Kui Ren, Shucheng Yu, and Karthik Mahendra Raje Urs. Achieving Usable

and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012

[11] Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010

[12] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, Ruitao Xie: DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.

[13] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer press, pp.377-394, 2010.

[14] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fully secure keypolicy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.

[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute based encryption in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.

[16] Liang Xiaohui, Cao Zhenfu, Lin Huang, et al. Attribute based proxy re-encryption with delegating capabilities. in: Proceedings of the 4th International Symposium on Information, Computer and Communications Security. New York, NY, USA: ACM press, pp. 276-286, 2009.

[17] Pirretti M, Traynor P, McDaniel P, et al. Secure atrribute-based systems. in: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York, USA: ACM press, pp. 99-112, 2006.

[18] Yu S., Wang C., Ren K., et al. Attribute based data sharing with attribute revocation. in: Proceedings of the 5th International Symposium on Information, Computer and Communications Security (ASIACCS), New York, USA: ACM press pp. 261-270, 2010.

[19] Sandhu R S, Coyne E J, Feinstein H L, et al. Role-based access control models. Computer, 29(2): 38-47, 1996.

[20] Tian X X, Wang X L, Zhou A Y. DSP RE-Encryption: A flexible mechanism for access control enforcement management in DaaS. in:

Proceedings of IEEE International Conference on Cloud Computing. IEEE press, pp.25-32, 2009

[21] Di Vimercati S D C, Foresti S, Jajodia S, et al. Over-encryption: management of access control evolution on outsourced data. in: Proceedings of the 33rd international conference on Very large data bases. Vienna, Austria: ACM, pp. 123-134, 2007.

[22] Kan Yang, Xiaohua Jia, Kui Ren, Ruitao Xie, Liusheng Huang: Enabling efficient access control with dynamic policy updating for big data in the cloud. INFOCOM 2014, pp.2013-2021, 2014.

[23] Jia W, Zhu H, Cao Z, et al. SDSM: a secure data service mechanism in mobile cloud computing. in: Proceedings of 30th IEEE International Conference on Computer Communications. Shanghai, China: IEEE, pp. 1060-1065, 2011.

[24] D. Huang, X. Zhang, M. Kang, and J. Luo. Mobicloud: A secure mobile cloud framework for pervasive mobile computing and communication. in: Proceedings of 5th IEEE International Symposium on Service-Oriented System Engineering. Nanjing, China: IEEE, pp. 90-98, 2010.

[25] Benjamin Livshits, Jaeyeon Jung. Automatic Mediation of Privacy-Sensitive Resource Access in Smartphone Applications. USENIX Security, pp.113-130, Aug. 2013.

[26] Zhou Z, Huang D. Efficient and secure data storage operations for mobile cloud computing. in: Proceedings of 8th International Conference on Network and Service Management (CNSM 2012), Las Vegas, USA: IEEE, pp. 37-45, 2012.

[27] P. K. Tysowski and M. A.Hasan. Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds. IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 172-186, Nov. 2013.

[28] Boneh D, Franklin M. Identity-based encryption from the Weil pairing. in: Proceedings of the Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, pp. 213−229, 2001.

[29] Sahai A, Waters B. Fuzzy identity based encryption. in: Proceedings of the Advances in Cryptology. Aarhus, Denmark: Springer-Verlag, pp.457-473, 2005.

[30] Shamir A. How to share a secret. Communications of the ACM,1979, 22 (11): 612-613.

Vaka Uma Devi is a student of Sri Vasavi Institute of Engineering & Technology, Nandamuru.she is student of M.tech[CSE] and also received B.tech degree from JNTUK.

N.Anil Kumar is an Associate Professor in Sri Vasavi Institute of Engineering & Technology, Nandamuru. He Received Master Degrees from different Universities and also Having 22 years of Experience as a faculty and Guide for Different Domain