International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 29th Jan 2019. Link :
http://www.ijiemr.org/main/index.php?vol=Volume-08&issue=ISSUE-01

Title: **A LIGHT WEIGHT SECURE RECORDS STRUCTURE THEME FOR CLOUD COMPUTING**

Volume 08, Issue 01, Pages: 297–305.

Paper Authors

MS: SOUJANYA PIDATHALA, G.SANDHYA RANI

VIJAYA ENGINEERING COLLEGE

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A LIGHT WEIGHT SECURE RECORDS STRUCTURE THEME FOR CLOUD COMPUTING

MS: SOUJANYA PIDATHALA[1], G.SANDHYA RANI[2]
[1]PG SCHOLAR, VIJAYA ENGINEERING COLLEGE
[2]ASSISTANT PROFESSOR, VIJAYA ENGINEERING COLLEGE

ABSTRACT:

With the recognition of cloud computing, cell gadgets will shop/retrieve non-public statistics from anywhere at any time. Consequently, the information protection disadvantage in cell cloud turns into a variety of and plenty of excessive and forestalls extra development of cell cloud. There rectangular degree significant research which might be performed to reinforce the cloud protection. However, maximum of them don't seem to be applicable for cellular cloud because cell gadgets entirely have confined computing resources and strength. Solutions with low process overhead rectangular measure in exceptional want for cell cloud applications. At some point of this paper, we will be inclined to suggest a light-weight records sharing topic (LDSS) for mobile cloud computing. It adopts CP-ABE, accomplice diploma get admission to control technology hired in conventional cloud surroundings, however modifications the structure of get admission to management tree to form it suitable for cell cloud environments. LDSS movements an oversized portion of the manner in depth get right of entry to management tree transformation in CP-ABE from cellular devices to external proxy servers. Moreover, to cut back the person revocation fee, it introduces attribute description fields to enforce lazy-revocation, that could be a thorny difficulty in application-based CP-ABE systems. The experimental consequences show that LDSS will successfully reduce the overhead at the mobile device thing as soon as customers square measure sharing records in cell cloud environments.

1. INTRODUCTION:

With the event of cloud computing and conjointly the usual of excellent cell devices, humans stay vicinity unit of size united it by way of bit getting accustomed to a replacement technology of understanding sharing version during that the data is hold on the cloud and conjointly the cell gadgets sq. Measure accustomed retrieve the statistics from the cloud. Typically, cell devices by myself have constrained house for storing and computing strength. On the contrary, the cloud has Brobdingnagian amount of assets. In one of these, to obtain the satisfactory performance, it's critical to use the assets furnished by using the cloud carrier company (CSP) to store and percentage the facts. Nowadays, varied cloud cell packages square measure huge used. In these packages, humans (records proprietors) can switch their pics, movies, documents and completely exceptional files to the cloud and share these facts with folks (facts users) they like to proportion. CSPs further offer information control usefulness for facts homeowners. Since private statistics documents place unit sensitive, data householder's location unit allowed to make your mind up on whether or no longer or to not produce their facts documents public or can alone be shared with precise data users. Clearly, information private ness of the private sensitive facts can be a big difficulty for lots facts house owners. The innovative privilege control/get admission to management mechanisms supplied by means of the CSP area unit both no longer excellent or now not very convenient.

They'll not meet all the desires of knowledge householders. First, as soon as people transfer their information documents onto the cloud, they are attempt the information in Associate in Nursing extremely place in which is out in their control, and conjointly the CSP may undercover agent on user statistics for its industrial pastimes and/or exclusive motives. Second, person shave to be pressured to ship watchword to each data consumer if they on my own would like to share the encrypted information with sure users, it's implausibly bulky. To change the privilege control, the facts owner can divide understanding customers into completely unique corporations and send watchword to the organizations that they want to proportion the data. However, this method needs nice-grained access control. In every instance, watchword control is a large trouble. Apparently, to resolve the on excessive of troubles, private sensitive information want to be encrypted earlier than uploaded onto the cloud so as that the information is cosy towards the CSP. However, the statistics committal to writing brings new problems. The thanks to provide comparatively cheap get right of entry to management mechanism on ciphertext cryptography in order that alone the legal customers can get entry to the plaintext records is difficult. Similarly, system must provide information homeowners powerful person privilege management functionality, so they are going to grant/revoke facts get admission to privileges merely at the information customers. There rectangular degree considerable researches on the problem of expertise get entry to control over ciphertext. In those researches, they have got the subsequent commonplace assumptions. First, the CSP is considered honest and curious. Second, all the touchy facts area unit encrypted before uploaded to the Cloud. Third, person authorization on positive facts is finished thru encryption/decryption key distribution. In fashionable, we have a propensity to rectangular degree capable of divide those tactics into four categories: truthful ciphertext get entry to management, stratified get entry to control,

get entry to control supported completely homomorphic committal to writing [1][2] and

get entry to management supported characteristic-based totally committal to writing (ABE). Of these proposals' region unit designed for non-mobile cloud surroundings. They eat large indefinite quantity of storage and computation assets, that are not gettable for cellular devices. Per the experimental finally ends up in [26], the vital ABE operations deem for a good deal longer time on cell devices than PC or desktop computer systems. It's miles a minimum of twenty-seven instances longer to execute on a smart phone than a personal pc (PC). This indicates that Associate in Nursing committal to writing operation that takes one minute on a computer laptop will take regarding zero.5 Associate in Nursing hour to complete on a mobile device. Moreover, present day solutions don't clear up the person privilege change drawback okay. Like operation could likely finish in very high revocation value. Normally this will be regularly now not relevant for mobile devices any. Clearly, there is not any accurate answer which could successfully clear up the relaxed statistics sharing disadvantage in mobile cloud. Due to the mobile cloud will become plenty of and masses of commonplace, presenting a cheap comfortable record sharing mechanism in mobile cloud is in urgent want. To handle this trouble, at some stage in this paper, we will be predisposed to tend to suggest a light-weight information Sharing theme (LDSS) for cellular cloud computing environment. The most contributions of LDSS vicinity unit as follows: (1) we have a propensity to tend to style Associate in Nursing algorithm remarked as LDSS-CP-ABE supported Attribute-Based committal to writing (ABE) method to supply reasonable get right of entry to management over ciphertext. (2) we have a propensity to tend to use proxy servers for committal to write and cryptography operations. In our method, technique intensive operations in ABE location unit carried out on proxy servers, that significantly prune the method overhead on client factor mobile devices. Meanwhile, in LDSS-CP-ABE, therefore on beware of understanding privacy, a model attribute is similarly delivered to the access shape. The cryptography key layout is changed so as that it's going to be sent to the proxy servers in Associate in Nursing extremely relaxed way. (three) we will be inclined to tend to introduce lazy re-encryption and description discipline of attributes to scale back the revocation overhead once dealing with the user revocation drawback. (4) Finally, we have a propensity to have a tendency to put into effect an information sharing instance framework supported LDSS. The experiments show that LDSS can substantially prune the overhead on the purchaser element, that on my own introduces a negligible additional cost on the server factor. Such Associate in Nursing approach is beneficial to enforce a realistic statistics sharing protection topic on mobile devices. The outcomes similarly show that LDSS has higher overall performance in comparison to the present day ABE primarily based get entry to control schemes over ciphertext. The relaxation of this paper is prepared as follows. Section a integrate of offers a few primary concepts in secure cell cloud information sharing and conjointly the safety premise. Section 3 provides the cautious type of LDSS. Section 4 and 5 offer the safety evaluation and performance evaluation, severally. Section vi provides linked works. Finally, Section seven concludes our work with the longer-term paintings.

2. RELATED WORK

In this segment, we have a propensity to specialize within the works of ciphertext get entry to control schemes that are closely related to our analysis. Access control is an important mechanism fact understanding facts privacy protection to confirm that facts will solely be nonheritable with the aid of valid users. There has been widespread analysis on the troubles of information access control within the cloud, mainly specializing in get admission to

Assume that p is a prime number, the secrete information to share is $k\varepsilon k = Z_p$.Divide k into n pieces through the following steps:

Randomly select one (t-1)-order polynomial The process to reconstruct h(x) out of t random shares through the Lagrange polynomial interpolation is as follows: in

$$h(x) = \sum_{s=1}^{t} y_{i_s} \prod_{\substack{j=1 \\ j\neq s}}^{t} (x - x_{i_j}) / (x_{i_s} - x_{i_j})$$

All these operations are done on Zp, namely, they are all p-mode operations. After obtaining h(x), we can get the secret k=aa_0 = h(0)

$$k = h(0) = \sum_{s=1}^{t} y_{i_s} \prod_{\substack{j=1 \\ j\neq s}}^{t} \frac{-x_{i_j}}{x_{i_s} - x_{i_j}}$$

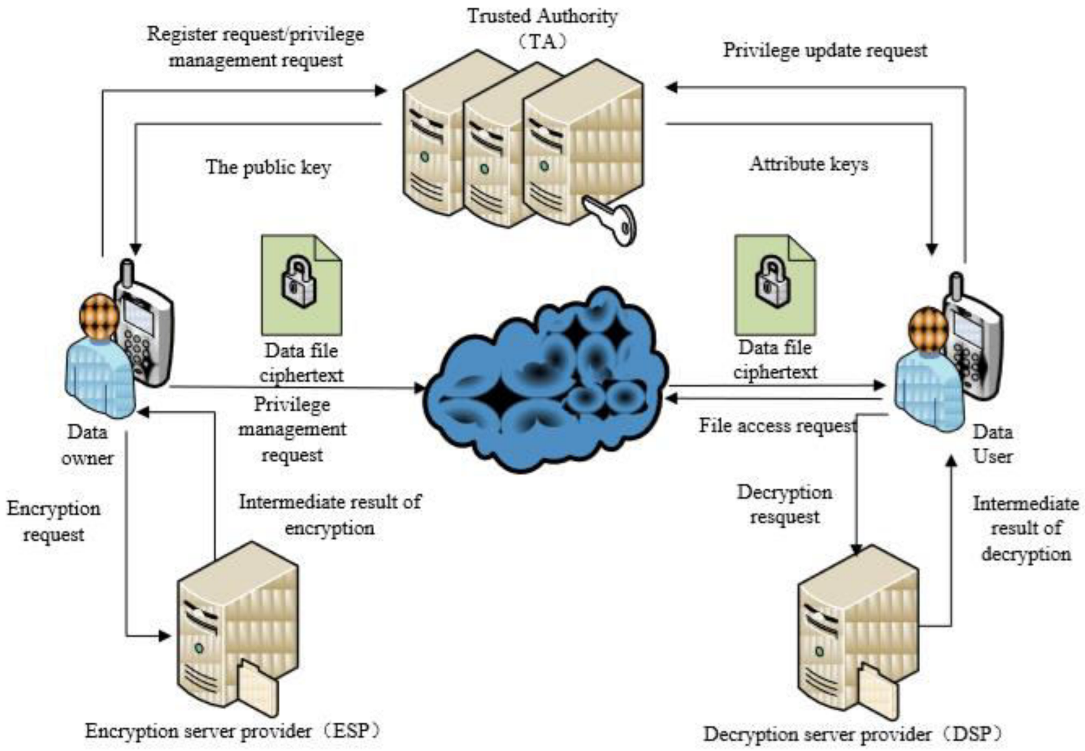
Since n x xx ,...,, 1 2 is public, we can get Lagrange coefficients in advance

$$\lambda_s = \prod_{\substack{j=1 \\ j\neq s}}^{t} \frac{-x_{i_j}}{x_{i_s} - x_{i_j}}$$

Thus, the formula to recover the secret k can be put in a simpler way:

$$k = \sum_{s=1}^{t} \lambda_s y_{i_s}$$

management over ciphertext. Typically, the cloud is taken into consideration honest and curious. Sensitive know-how needs to be encrypted before causing to the cloud. User authorization is carried out through key distribution. The analysis may be usually divided into 4 regions: smooth ciphertext get entry to control, ranked get entry to control, get right of entry to management supported homomorphic mystery writing [1][2] and get right of entry to management supported attribute-based totally mystery writing (ABE). Clean ciphertext access control refers to it once document mystery writing, the secret writing keys are dispensed all through a comfy way to prevail authorization for straightforward customers [3]. To reduce the overhead of big user key distribution, Skillen and Mannan [4] designed a system called Mobiflage that allows PDE (plausibly confusable encryption) on cellular devices by using concealment encrypted volumes through random know-how on a tool's auxiliary storage.


Trusted Authority (TA)
Register request/privilege management request
Privilege update request
The public key
Attribute keys
Data file ciphertext
Data file ciphertext
Privilege management request
File access request
Data owner
Data User
Encryption request
Intermediate result of encryption
Decryption resquest
Intermediate result of decryption
Encryption server provider（ESP）
Decryption server provider（DSP）

However, the device must collect extraordinary amount of facts of keys. [5] borrows the access control technique utilized in regular dispensed storage [4][6][7][8], keeping apart users into totally extraordinary unique teams in keeping with get right of entry to rights and assign exclusive keys to teams. This reduces the overhead of key control; however, it cannot satisfy the call for for pleasant-grained access management. Ranked get right of entry to control has clever performance in decreasing the overhead of key distribution in ciphertext access management [9]. As a result, there are widespread analysis on ciphertext get admission to management [10][11][12][13] supported ranked get entry to control method. In ranked get entry to control approach, keys may be derived from personal keys and a public token table. However, the operation on token desk is state-of-the-art and generates high fee. Besides, the token table is hold in the cloud. Its privateers and safety cannot be secured [14]. Full homomorphic secret writing algorithmic software will perform without delay on the ciphertext. It's in operation consequences are equal with in operation on plaintext so encrypting the facts. [15] makes use of full homomorphic secret writing algorithmic program to try to to operations like retrieval and calculation without delay on ciphertext. It will solve the matter that the cloud is untrusty basically because of all information replace Operations and person privilege amendment operations could also be completed at once on ciphertext. However, this coding theme is simply too complicated to place into result in sensible applications.

Attribute-primarily primarily based coding rule comes from identity-primarily based coding. It embeds cryptography rules among the coding set of rules, that avoids frequent key distribution. Lai et al [14] and Bethen court et al [17] planned key-policy attribute-based coding (KP-ABE) and ciphertext-policy attribute-based wholly coding (CPABE).

In smart programs, CP-ABE has been drastically studied [18][19][20] after you consider that it's miles very like role based get admission to govern (RBAC) theme [21]. In CP-ABE, the possession of 1 characteristic key means that the key man of affairs owns corresponding attribute, and characteristic keys cannot be saved as shortly as they are distributed. As a result, while a statistics user's characteristic is revoked, a way to check that statistics privacy can become a troublesome problem [14]. Liang et al [18] propose characteristic-based proxy re-encryption (ABPRE) theme to clear up this bother. However, in their answer, whereas a person's attribute is revoked, all alternative users UN agency own this attribute can lose this characteristic at the identical time, that cannot fulfil quality-grained get admission to manage desires. Tian et al [22] integrate CP-ABE and public key cryptography to achieve ciphertext get right of entry to govern. However, it brings excessive value to statistics proprietors. Di Vimercati et al [23] add a time stamp to attributes to restriction the utilization of characteristic keys to influence attribute revocation problem. However, during this scenario, statistics customers got to sporadically follow for characteristic keys and therefore the customers' characteristic cannot be revoked ahead of the time stamp expires. Yu et al [24] counsel some work of revocation will be outsourced to CSP, whereas CSP should have a positive quality, and access manage policy that has "or" geological dating or "threshold" relationship isn't supported. Yu et al [25] to boot planned a theme to address the cloud computing arduous that preserve sensitive user statistics non-public against untrusted servers by victimization exploiting

and unambiguously combining techniques of characteristic-based coding (ABE), proxy re-encryption, and lazy re-encryption. Yang et al. [26] planned a

singular theme that sanctioning inexperienced get entry to govern with dynamic policy change for giant records within the cloud that specializing in developing AN outsourced

policy change technique for ABE structures. It to boot designed policy change algorithms for extraordinary forms of get admission to policies. All the higher than works consciousness on the matter of facts get admission to regulate within the cloud. they're particularly for non-cell gadgets and cannot be enforced for records sharing in cell cloud atmosphere. relating to to facts private ness in cell cloud, some works had been finished during this space[25]. Huang et al [26] endorse Mobi Cloud, within which typical Mobile Ad-hoc NET works (MANETs) is born-again into service-orientated language design. during

this design, every mobile device is appeared as a carrier node, and therefore the operations ar outsourced to the cloud. However, in Mobi Cloud, customers got to fully settle for as true with the cloud, that isn't the case indeed. Livshits and Jung [27] designed and administered a graph a prioris rule to space mediation activates that protect every resource access, whereas avoiding repetitive prompting and prompting in background tasks or third-party libraries, for the matter of mediating resource accesses in mobile applications. Chou dynasty et al [28] projected AN ABDS theme to attain secure knowledge storage within the cloud. However, this theme is n't appropriate for knowledge sharing and has no clear answer for attribute revocation. Tysowski et al. [29] thought of a selected cloud computing atmosphere wherever knowledge area unit accessed by resource-constrained mobile devices, and projected novel modifications to ABE, that allotted the upper procedure overhead of scientific discipline operations to the cloud supplier and lowered the overall communication price for the mobile user. In summary, current proposals on knowledge access management within the cloud area unit largely for non-mobile terminals, that isn't appropriate for mobile devices. Besides, current solutions don't solve the matter of user privilege modification eventualities fine since the y carry high revocation price. this is often not applicable for mobile devices that solely have restricted computing cap ability and power. Existing studies on mobile cloud don't have a decent answer to secure knowledge'sharing once servers aren't cre dible. In a word, there's no correct answer which will solve the matter of secure knowledge sharing in mobile cloud. during this paper, we have a tendency to propose a light-weight knowledge sharing theme (LDSS) for mobile cloud applications. It adopts CP-ABE, a technology utilized in access management within the traditional cloud atmosphere, however chang es the structure of access management tree to form it appropriate for mobile cloud. LDSS is demonstrably secure, and is incontestable to be additional economical and scalable than state of-the-art ABE schemes

3. EXPERIMENTAL REVIEW:

Int the occasion of distributed computing and in the way the nature of sensible mobile phones, people simple measurestraight ordered getting familiar with a substitution time interval of data sharing model inside which the data is keptin the cloud and along with the lines of the cell phones square measure acclimated stored or recovered the data from the cloud. daily, cell phones exclusively have confined cabinet space and figuring power. Despite what might be expected, the cloud has tremendous amount of assets. In such a circumstance, to understand the execution, it's basic to utilize the assets given by the cloud benefit provider to store and offer the data. firstly, to determine the on major of issues, individual information must be constrained to be encoded before passing onto the cloud randomly the information is secure against the CSP. Thus , the information mystery brings new issue's. The of give access for one account administration system on figure content cryptography along with these lines totally the certify clients can get to the plain text information is troublesome. Secondly, to start framework should give information householders successful client benefit administration capacity, so as that they will give/disavow information for getting benefits just on learning clients. Thereis zone unit which examines on the matter of information get to administration over picture content. In these explores, they have the accompanying normal suppositions. In the first place, the CSP is mulled over genuine and inquisitive. Thirdly, all the delicate information unit of estimation scrambled before passed to the Cloud. fourthly, client approval on positive information is accomplished through encryption/decryption key conveyance. When all is said in done, we do partition these methodologies into four classifications: basic image content access administration, various levels get to administration for uphold entire homomorphic mystery composing and access administration bolstered property based mystery composing (ABE) out of these recommendations unit of estimation intended for non-portable cloud environment.

4. CONCLUSION:

As of late, a few examinations on access administration in cloud square measure bolstered property-based mystery composing algorithmic program (ABE). Be that as it may, antiquated ABE isn't proper for versatile cloud because of its computationally escalated and cell phones exclusively have limited assets. amid this paper, we tend to propose LDSS to manage this issue. It presents a totally novel LDSS-CP-ABE algorithmic program to move significant calculation overhead from cell phones onto intermediary servers, along these lines it will comprehend the protected data sharing drawback in versatile cloud. The trial results demonstrate that LDSS will ensure data security in versatile cloud and scale back the overhead on clients' feature in portable cloud. inside the future work, we will style new ways to deal with affirm data respectability. To extra spigot the capability of portable cloud, we are going to also ponder an approach to do ciphertext recovery over existing data sharing plans

5. 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, HongxiaJin. "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, Bo Zhang, RuitaoXie: DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics

[8] 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.

[9] 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.

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

[11] 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. 350364

[12] Cong Wang, Kui Ren, Shucheng Yu, and Karthik MahendraRajeUrs. Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012

[13] 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

[14] Kan Yang, Xiaohua Jia, Kui Ren, Bo Zhang, RuitaoXie: 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

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

[22] 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

[23] 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.

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

[25] 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.

[26] 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.

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

[28] 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.

[29] 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

Author 1

PG Scalar

PIDATHALA.SOUJANYA,
B. tech: Swarna Bharathi institute of Science and technology,
M.tech : Vijaya engineering college
mondru.sj@gmail.com.

Author 2

Guide details:

G.SANDHYA RANI (ASSISTANT professor)
EMAIL:mvlsandhya@gmail.com