International Journal of Research Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 07
June 2019

An Enhanced and Reliable Encrypted Cloud Storage Supporting Reduplication in Parallel Distribution System

K. Vijaya Kumar [1], V Lakshmi Chetana [2]

[1]Assistant Professor, Dep of CSE, PVSIT, Vijayawada.A.P
[2]Assistant Professor, Dept of CSE, Dvr & Dr Hs MICT, Vijayawada.A.P

Abstract:-The concept of storing data in the cloud allows them to user encrypt data by using cryptographic concepts and the Existed algorithm is Attribute-based encryption. In this Paper we propose the concept of sensor, it supports to maintain data from server side it allows to the user before storage the data the server will automatically get alert file along with the size the content will be compared with the block-wise and automatically detected the duplicated entry then cloud server administrator never allows to users for uploading the same file in the same storage device. The Parallel Network file system was only responsible for share the file from the user to a server and it is responsible for sensor alerts. We propose CP-ABE algorithm it generates different files having the different key that will never allow to an attacker for accessing files with wrong keys we are maintaining the hybrid cloud setting it allows to private cloud detecting for duplicate data and public cloud is responsible for maintaining storage. Key-Words:-ABE, CP-ABE, Parallel Distribution System, Storage, Sensors.

I.INTRODUCTION:-

Distributed computing enormously encourages information suppliers who need to re-appropriate their information to the cloud without uncovering their delicate information to outside gatherings and might want clients with specific accreditations to have the capacity to get to the information [1], [2], [3], [4], [5]. This expects information to be put away in scrambled frames with access control arrangements to such an extent that nobody aside from clients with characteristics (or qualifications) of explicit structures can decode the encoded information. An encryption procedure that meets this prerequisite is called quality based encryption (ABE) [6], where a client's private key is related with an property set, a message is encoded under an entrance strategy (or then again get to structure) over a lot of properties, and a client can unscramble a cipher text with his/her private key if his/her set of characteristics fulfills the entrance strategy related with this cipher text. Nonetheless, the standard ABE framework neglects to accomplish secure reduplication [7], which is a system to spare extra room and system data transfer capacity by dispensing with repetitive duplicates of the encoded information put away in the cloud. Then again, apparently, existing developments [8], [9], [10], [11] for secure reduplication are not based on quality based encryption. By the by, since ABE and secure reduplication have been generally connected in distributed computing, it is alluring to plan a cloud capacity framework having the two properties. We consider the accompanying situation in the structure of an property based capacity framework supporting secure reduplication of encoded information in the cloud, in which the cloud won't store a document more than once despite the fact that it might get different duplicates of a similar document scrambled under distinctive access approaches. An information supplier, Bob, means to transfer a fileM to the cloud, and shareM with clients having certain accreditations. So as to do as such, Bob encodes M under an entrance approach An over a lot of characteristics, and transfers the comparing cipher text to the cloud, to such an extent that as it were clients whose arrangements of characteristics fulfilling the entrance approach can unscramble the cipher text. Afterward, another information supplier, Alice, transfers a cipher text for the equivalent fundamental document M in any case, attributed to an alternate access arrangement A0. Since the document is transferred in an encoded structure, the cloud can't perceive that the plaintext comparing to Alice's cipher text is equivalent to that comparing to Bob's, and will store M twice. Clearly, such copied stockpiling squanders stockpiling space and correspondence data transfer capacity.

1.1 Network System:-

Over the last decade WSNs are increasingly used in several real-world applications [1], [2], [3], [4], such as wild habitat monitoring, volcano and fire monitoring, urban sensing, and military surveillance. In most cases, the sensor nodes form a multi-hop network while the base station (BS) acts as the central point of control. Typically, a sensor node has limitation in terms of computation capability and energy reserves. The BS wants to collect the sensed information from the network. One common way is to allow each sensor node to forward its reading to the BS, possibly via other intermediate nodes. Finally, the BS processes the received data. However, this strategy is restrictively costly as far as correspondence overhead.

II.Related Work:-

Attribute Based Encryption. Sahai and Waters [6] presented the thought of Attribute based encryption (ABE), and at that point Goyal et al. [16] formulated key-policy ABE (KP-ABE) what's more, cipher text-policy ABE (CP-ABE) as two complimentary types of ABE. The principal KP-ABE development given in [16] understood the monotonic access structures, the principal KP-ABE framework supporting the declaration of non-monotone equations was exhibited in [17] to empower increasingly feasible access policies, and the first large class KP-ABE system was presented by in the standard model in [18]. Nevertheless, we believe that KP-ABE is less flexible than CP-ABE because the access policy is determined once the user's attribute private keyis issued. Bettencourt, Sahai and Waters [19] proposed the first CP-ABE construction, but it is secure under the generic group model. Cheung and Newport [20] presented a CPABE scheme that is proved to be secure under the standard model, but it only supports the AND access structures. ACP-ABE system under more advanced access structures is proposed by Goyal et al. [21] based on the number theoretic assumption. In order to overcome the limitation that the size of the attribute space is polynomial bounded in the security parameter and the attributes are fixed ahead, Rouselakis and Waters [22] built a large universe CP-ABE system under the prime-order group. In this paper, the Rouselakis-Waters system is taken as the underlying scheme for the concrete construction.

Several researchers have studied problems related to data aggregation in WSNs.

A. Data Aggregation in a Trusted Environment

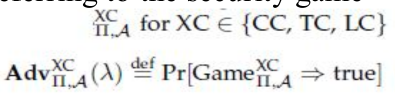
The Tiny Aggregation Service (TAG) to compute aggregates, such as Count and Sum, using tree-based aggregation algorithms were proposed in [5]. Similar algorithms to compute Count and Sum were proposed in [6]. Moreover, treebasedaggregation algorithms to compute an order-statistic(i.e., quantile) have been proposed in [14].To address the communication loss problem in tree-based algorithms an aggregation framework called synopsis diffusions designed in [8], which computes Count and Sum using a ring topology. Very similar algorithms are independently proposed in [7]. These works use duplicate-insensitive algorithms for computing aggregates based on [15]'s algorithm for counting distinct elements in a multi-set.

B. Secure Aggregation Techniques:-

Several secure aggregation algorithms have been proposed assuming that the BS is the only aggregator node in the network [18], [19], [20]. These works did not consider in network aggregation. Only recently, the research community has been paying attention to the security issues of hierarchical aggregation. The first attack-resilient hierarchical data aggregation protocol was designed in [16]. However, this scheme is secure when only one malicious nodes is present. A tree-based verification algorithm was designed in [17], [21] by which the BS can detect if the final aggregate, Count or Sum, is falsified. A few verification algorithms for computing Count and Sum within the synopsis diffusion approach were designed in [9],[12]. Recently, a few novel protocols have been proposed for 'secure outsourced aggregation' [22]; however, as noted by the authors, these algorithms are not designed for WSNs.

Existing Algorithm:-

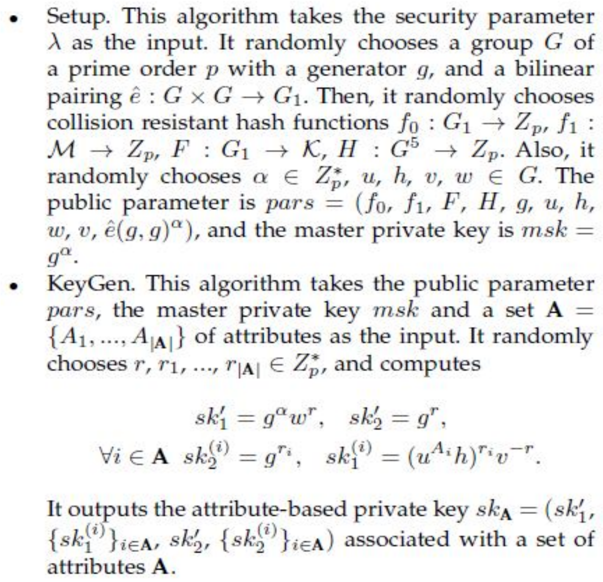
An attribute-based storage system for secure reduplications consistent if the advantage function referring to the security game



$$_{\Pi,\mathcal{A}}^{\mathrm{XC}} \text{ for XC} \in \{\text{CC, TC, LC}\}$$

$$\mathbf{Adv}_{\Pi,\mathcal{A}}^{\mathrm{XC}}(\lambda) \overset{\text{def}}{=} \Pr[\text{Game}_{\Pi,\mathcal{A}}^{\mathrm{XC}} \Rightarrow \text{true}]$$

is negligible in the security parameter _ for any PPT adversary
algorithm A.



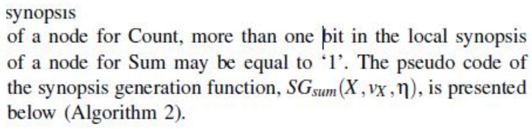
- Setup. This algorithm takes the security parameter λ as the input. It randomly chooses a group G of a prime order p with a generator g, and a bilinear pairing $\hat{e} : G \times G \rightarrow G_1$. Then, it randomly chooses collision resistant hash functions $f_0 : G_1 \rightarrow Z_p$, $f_1 : \mathcal{M} \rightarrow Z_p$, $F : G_1 \rightarrow \mathcal{K}$, $H : G^5 \rightarrow Z_p$. Also, it randomly chooses $\alpha \in Z_p^*$, u, h, v, $w \in G$. The public parameter is $pars = (f_0, f_1, F, H, g, u, h, w, v, \hat{e}(g,g)^{\alpha})$, and the master private key is $msk = g^{\alpha}$.
- KeyGen. This algorithm takes the public parameter $pars$, the master private key msk and a set $\mathbf{A} = \{A_1, ..., A_{|\mathbf{A}|}\}$ of attributes as the input. It randomly chooses $r, r_1, ..., r_{|\mathbf{A}|} \in Z_p^*$, and computes

$$sk_1' = g^{\alpha} w^{r}, \quad sk_2' = g^{r},$$
$$\forall i \in \mathbf{A} \;\; sk_2^{(i)} = g^{r_i}, \quad sk_1^{(i)} = (u^{A_i} h)^{r_i} v^{-r}.$$

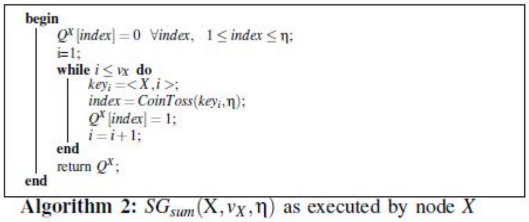
It outputs the attribute-based private key $sk_{\mathbf{A}} = (sk_1', \{sk_1^{(i)}\}_{i \in \mathbf{A}}, sk_2', \{sk_2^{(i)}\}_{i \in \mathbf{A}})$ associated with a set of attributes $\mathbf{A}$.

Proposed Algorithm:-

Iterative Filtering (IF) algorithms are an attractive option for WSNs because they solve both problems - data aggregation and data trustworthiness assess- ment - using a single iterative procedure. Such trustworthiness estimate of each sensor is based on the distance of the readings of such a sensor from the estimate of the correct values, obtained in the previous round of iteration by some form of aggregation of the readings of all sensors. Such aggregation is usually a weighted average; sensors whose readings signicantly dier from such estimate are assigned less trustworthiness and consequently in the aggregation process in the present round of iteration their readings are given a lower weight. Our goal is to enable BS to obtain the 'true' estimate of the aggregate (which BS would compute if there were no compromised nodes) even in the presence of the attack. More formally, goal (a) is to detect if ˆB, the synopsis received at BS is the same as the 'true' final synopsis B, and goal (b) is to compute B from ˆB and other received information. Without loss of generality, we present our algorithms in the context of Sum aggregate. As Count is a special case of Sum, where each node reports a unit value, these algorithms are readily applicable to Count aggregate also.



synopsis
of a node for Count, more than one bit in the local synopsis of a node for Sum may be equal to '1'. The pseudo code of the synopsis generation function, $SG_{sum}(X, v_X, \eta)$, is presented below (Algorithm 2).

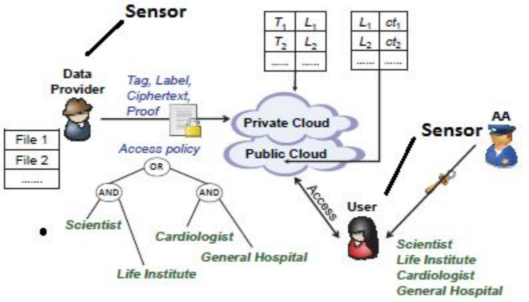


```
begin
    $Q^X[index] = 0 \;\; \forall index, \;\; 1 \le index \le \eta$;
    i=1;
    while $i \le v_X$ do
        $key_i = <X, i>$;
        $index = CoinToss(key_i, \eta)$;
        $Q^X[index] = 1$;
        $i = i + 1$;
    end
    return $Q^X$;
end
```

Algorithm 2: $SG_{sum}(\mathrm{X}, v_X, \eta)$ as executed by node X

Architecture Diagram:-

Concerning the ill-disposed model of our stockpiling framework, we expect that the private cloud is "interested however fair" with the end goal that it will endeavor to acquire the encoded messages in any case, it will sincerely pursue the conventions, while the general population cloud is questioned to such an extent that it may alter the name also, cipher text sets re-appropriated from the private cloud (note that such a mischief will be identified by either the private cloud or the client through the went with mark). Another contrast between the private cloud and general society cloud is that the previous can not conspire with users[4], however the last could conspire with clients. This supposition that is in line with this present reality practice where the private cloud is confided in more than the open cloud. We accept that information clients may attempt to get to information past their approved benefits. Notwithstanding endeavoring to acquire plaintext information from the cloud, malignant outcasts may likewise submit copy faking assaults as portrayed previously.



III.Literature Survey:-

1)Fast and secure laptop backups with encrypted de-duplication

AUTHORS: P. Anderson and L. Zhang

Many people now store large quantities of personal and corporate data on laptops or home computers. These often have poor or intermittent connectivity, and are vulnerable to theft or hardware failure. Conventional backup solutions are not well suited to this environment, and backup regimes are frequently inadequate. This paper describes an algorithm which takes advantage of the data which is common between users to increase the speed of backups, and reduce the storage requirements. This algorithm supports client-end per-user encryption which is necessary for confidential personal data.

2) Message-locked encryption and secure deduplication.

AUTHORS: M. Bellare, S. Keelveedhi, and T. Ristenpart

We formalize a new cryptographic primitive, Message-Locked Encryption (MLE), where the key under which encryption and decryption are performed is itself derived from the message. MLE provides a way to achieve secure deduplication (space-efficient secure outsourced storage), a goal currently targeted by numerous cloud-storage providers. We provide definitions both for privacy and for a form of integrity that we call tag consistency. Based on this foundation, we make both practical and theoretical contributions. On the practical side, we provide ROM security analyses of a natural family of MLE schemes that includes deployed schemes. On the theoretical side the challenge is standard model solutions, and we make connections with deterministic encryption, hash functions secure on correlated inputs and the sample-then-extract paradigm to deliver schemes under different assumptions and for different classes of message sources. Our work shows that MLE is a primitive of both practical

3. Security proofs for identity-based identification and signature schemes.

AUTHORS: M. Bellare, C. Namprempre, and G. Neven

This paper provides either security proofs or attacks for a large number of identity-based identification and signature schemes defined either explicitly or implicitly in existing literature. Underlying these is a framework that on the one hand helps explain how these schemes are derived and on the other hand enables modular security analyses, thereby helping to understand, simplify, and unify previous work. We also analyze a generic folklore construction that in particular yields identity-based identification and signature schemes without random oracles.

4. A reverse deduplication storage system optimized for reads to latest backups

AUTHORS: C. Ng and P. Lee. Revdedup

Deduplication is known to effectively eliminate duplicates, yet it introduces fragmentation that degrades read performance. We propose RevDedup, a deduplication system that optimizes reads to the latest backups of virtual machine (VM) images using reverse deduplication. In contrast with conventional deduplication that removes duplicates from new data, RevDedup removes duplicates from old data, thereby shifting fragmentation to old data while keeping the layout of new data as sequential as possible. We evaluate our RevDedup prototype using a 12-week span of real-world VM image snapshots of 160 users. We show that RevDedup achieves high deduplication efficiency, high backup throughput, and high read throughput.

5. Secure deduplication with efficient and reliable convergent key management

AUTHORS: P. Lee, and W. Lou

Data deduplication is a technique for eliminating duplicate copies of data, and has been widely used in cloud storage to reduce storage space and upload bandwidth. Promising as it is, an arising challenge is to perform secure deduplication in cloud storage. Although convergent encryption has been extensively adopted for secure deduplication, a critical issue of making convergent encryption practical is to efficiently and reliably manage a huge number of convergent keys. This paper makes the first attempt to formally address the problem of achieving efficient and reliable key management in secure deduplication. We first introduce a baseline approach in which each user holds an independent master key for encrypting the convergent keys and outsourcing them to the cloud. However, such a baseline key management scheme generates an enormous number of keys with the increasing number of users and requires users to dedicatedly protect the master keys. To this end, we propose Dekey, a new construction in which users do not need to manage any keys on their own but instead securely distribute the convergent key shares across multiple servers. Security analysis demonstrates that Dekey is secure in terms of the definitions specified in the proposed security model. As a proof of concept, we implement Dekey using the Ramp secret sharing scheme and demonstrate that Dekey incurs limited overhead in realistic environments.

IV.Conclusion:-

Attribute based encryption (ABE) has been generally utilized in distributed computing where information suppliers re-appropriate their scrambled information to the cloud and can impart the information to clients having indicated qualifications. Then again, deduplication is a significant procedure to spare the capacity space and system transmission capacity, which takes out copyDuplicates of indistinguishable information. Notwithstanding, the standard

ABE frameworks try not to help secure deduplication, which makes them exorbitant to be connected in some business stockpiling administrations. In this paper, we displayed a novel way to deal with understand an Quality based capacity framework supporting secure deduplication. Our capacity framework is worked under a half breed cloud engineering, where a private cloud controls the calculation furthermore, an open cloud deals with the capacity. The private cloud is given a trapdoor key related with the comparing cipher text, with which it can exchange the ciphertext more than one access arrangement into cipher texts of the equivalent plaintext under some other access arrangements without being mindful of the hidden plaintext. In the wake of accepting a capacity demand, the private cloud first checks the legitimacy of the transferred thing through the appended evidence. On the off chance that the evidence is substantial, the private cloud runs a label coordinating calculation to see whether similar information basic the cipher text has been put away. Provided that this is true, at whatever point it is fundamental, it recovers the cipher text into a cipher text of the equivalent plaintext over an get to arrangement which is the association set of both access strategies. The proposed stockpiling framework appreciates two noteworthy focal points. Right off the bat, it very well may be utilized to privately impart information to other clients by determining an entrance strategy as opposed to sharing the unscrambling key. Besides, it accomplishes the standard thought of semantic security while existing deduplication plans just accomplish it under a flimsier security idea.

V.References:-

[1] D. Quick, B. Martini, and K. R. Choo, Cloud Storage Forensics. Syngress Publishing/Elsevier,2014.[Online].Available :http://www.elsevier.com/books/cloud-storageforensics/quick/978-0-12-419970-5

[2] K. R. Choo, J. Domingo-Ferrer, and L. Zhang, “Cloud cryptography: Theory, practice and future research directions,” Future Generation Comp. Syst., vol. 62, pp. 51–53, 2016.

[3] K. R. Choo, M. Herman, M. Iorga, and B. Martini, “Cloud forensics: State-of-the-art and future directions,” Digital Investigation, vol. 18, pp. 77–78, 2016.

[4] Y. Yang, H. Zhu, H. Lu, J.Weng, Y. Zhang, and K. R. Choo, “Cloud based data sharing with fine-grained proxy re-encryption,” Pervasive and Mobile Computing, vol. 28, pp. 122–134, 2016.

[5] D. Quick and K. R. Choo, “Google drive: Forensic analysis of data remnants,” J. Network and Computer Applications, vol. 40, pp. 179– 193, 2014.

[6] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology - EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005, Proceedings, ser. Lecture Notes in Computer Science, vol. 3494. Springer, 2005, pp. 457–473.

[7] B. Zhu, K. Li, and R. H. Patterson, “Avoiding the disk bottleneck in the data domain deduplication file system,” in 6th USENIX Conference on File and Storage Technologies, FAST 2008, February 26- 29, 2008, San Jose, CA, USA. USENIX, 2008, pp. 269–282.

[8] M. Bellare, S. Keelveedhi, and T. Ristenpart, “Message-locked encryption and secure deduplication,” in Advances in Cryptology - EUROCRYPT 2013, 32nd

Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, ser. Lecture Notes in Computer Science, vol. 7881. Springer, 2013, pp. 296–312.

[9] M. Abadi, D. Boneh, I. Mironov, A. Raghunathan, and G. Segev, "Message-locked encryption for lock-dependent messages," in Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I, ser. Lecture Notes in Computer Science, vol. 8042. Springer, 2013, pp. 374–391.

[10] S. Keelveedhi, M. Bellare, and T. Ristenpart, "Dupless: Serveraided encryption for deduplicated storage," in Proceedings of the 22th USENIX Security Symposium, Washington, DC, USA, August 14-16, 2013. USENIX Association, 2013, pp. 179–194.

[11] M. Bellare and S. Keelveedhi, "Interactive message-locked encryption and secure deduplication," in Public-Key Cryptography – PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 – April 1, 2015, Proceedings, ser. Lecture Notes in Computer Science, vol. 9020. Springer, 2015, pp. 516–538.

[12] S. Bugiel, S. N¨ urnberger, A. Sadeghi, and T. Schneider, "Twin clouds: Secure cloud computing with low latency - (full version)," in Communications and Multimedia Security, 12th IFIP TC 6 / TC 11 International Conference, CMS 2011, Ghent, Belgium, October 19- 21,2011. Proceedings, ser. Lecture Notes in Computer Science, vol. 7025. Springer, 2011, pp. 32–44.

[13] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems (extended abstract)," in Proceedings of the 17th Annual ACM Symposium on Theory of Computing, May 6-8, 1985, Providence, Rhode Island, USA. ACM, 1985, pp. 291–304.

[14] M. Fischlin and R. Fischlin, "Efficient non-malleable commitment schemes," in Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings, ser. Lecture Notes in Computer Science, vol. 1880. Springer, 2000, pp. 413–431.

[15] S. Goldwasser and S. Micali, "Probabilistic encryption," J. Comput. Syst. Sci., vol. 28, no. 2, pp. 270–299, 1984.

[16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, Ioctober 30 - November 3, 2006, ser. Lecture Notes in Computer Science, vol. 5126. Springer, 2006, pp. 89–98.

[17] R. Ostrovsky, A. Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007. ACM, 2007, pp. 195–203.

[18] A. B. Lewko and B. Waters, "Unbounded HIBE and attribute based encryption," in Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings, ser. Lecture Notes in Computer

Science, vol. 6632. Springer, 2011, pp. 547–567.

[19] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute-based encryption," in 2007 IEEE Symposium on Security and Privacy (S&P 2007), 20-23 May 2007, Oakland, California, USA. IEEE Computer Society, 2007, pp. 321–334.

[20] L. Cheung and C. C. Newport, "Provably secure cipher text policy ABE," in Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, Virginia, USA, October 28-31, 2007. ACM, 2007, pp. 456–465.

[21] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded cipher text policy attribute based encryption," in Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik.

Author Details:

Author 1:

K. Vijaya Kumar Assistant Professor, Department of Computer Science & Engineering, Prasad V Potluri Siddhartha Institute of Technology.
Email:kvkumar@pvpsiddhartha.ac.in

Author 2:

V Lakshmi hetana, Asst.Prof. Department of CSE, DVR& Dr HS MIC College of Technology,
Email:mailtochetana@gmail.com