ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

A Survey on Hybrid Approach for Data Sharing in Untrusted Cloud Using Secure Mona Protocol

Korumilli Lavanya[1], Grandhi Satya Suneetha[2], Rayavarapu Sridivya[3]

M.Tech, Dept. of CSE, Pragati Engineering College, Kakinada, India [1]

Assistant Professor, Dept. of CSE, Pragati Engineering College, Kakinada, India [2]

Assistant Professor, Dept. of CSE, Pragati Engineering College, Kakinada, India [3]

ABSTRACT: Sharing social occasion resource among cloud customers is a significant effect, so appropriated figuring gives a preservationist and compelling course of action. In view of continues with change of sharing data, investment in a multi-proprietor path to an un trusted cloud is still a testing issue. Here in this paper, We propose a safe multi-proprietor data sharing arrangement, for dynamic(continuously changing) group in the cloud. By giving social affair mark and component show encryption methods, any cloud customer can protectively confer data to others. By then a meanwhile, the limit overhead and encryption count cost of the arrangement are free with the amount of denied customers. In other hand, we explore the security of this arrangement with intensive confirmations. OTP (One-Time Password) is one of the least complex and most prevalent types of confirmation that can be utilized for securing access to accounts. OTP are regularly alluded to as a safe and more grounded types of confirmation, and tolerating them to introduce over different machines. We give a numerous levels of security to share information among multi-proprietor process. Initially the client chooses the pre-chosen picture to login. At that point chooses a picture from the matrix of pictures. By utilizing this the OTP is produced consequently and sent to comparing email account.

KEYWORDS: Security, Broadcast Message, Encryption, Cloud computing.

I. INTRODUCTION

Distributed computing imagines exceedingly accessible, on-interest system access to a common pool of configurable figuring assets [1], [2], [3]. Clients can appreciate adaptable capacity limit and calculation ability without paying consideration on the development and support of these bases. While distributed computing acquires promising open doors, it likewise brings along new security and protection issues, which thwart the general population to embrace the cloud advancements. The information in travel or put away in distributed storage could be tempered by unapproved people or even the distributed storage supplier [4], [5], [6]. Various encryption methods are accessible to ensure the security of

Cloud information and administrations [7], [8], [9]. Be that as it may, as these encryption methods bring along new procedures, additional complexities must be conceived to oversee encoded information safely and productively.

For an individual distributed storage client, he/she stores his/her information and recovers part of the put away information later. Be that as it may, for big business clients, the put away information ought to be shared among gathering individuals. One sort of encryption plan called quality based encryption (ABE) could be utilized to apply fine-grained access control over the mutual information [10], [11], [12], [13], [14], [15]. Furthermore, the elements of gathering individuals and relating put away information ought to be considered to build a plausible fine-grained access control for the undertaking [16], [17], and [18].

Moreover, given the aggregate sum of information created and put away in the cloud, getting to information through route is tedious and annoying. Getting to cloud information through (watchword) hunt is thought to be commonsense and in unnecessary. Nonetheless, as the cloud information are secured through cryptographic methods, which acquire

DOI: 10.15680/IJIRCCE.2016. 0409181

high expenses when recovering through seeking. Searchable encryption was acquainted with empower clients to shroud the searchable watchwords (of a record) by encryption [19], [20], [21], [22], [23], [24]. Later, clients could produce proper tokens/trapdoors for particular watchwords to recover the encoded information containing these catchphrases. The clients looking capacity is additionally shared under fine-grain arrangements [25], [26], [27], [28] One client can produce searchable records for a document and indicate a subset of clients who can use these searchable files. Clients outside the predefined bunch can't look out this record. In any case, progression of gathering individuals and searchable records ought to be considered to yield a down to earth and vigorous searchable encryption [29], [30].

In this paper, we propose one novel distributed storage development empowering the administration of element searchable information for gathering coordinated effort. We make utilization of quality based encryption plan (ABE) and open key encryption with conjunctive catchphrase look (PECK) to outline our convention. We show that our plan remarkably incorporates crucial usefulness for big business clients, to be specific, the fine-grained access control for the searchable file and the substance of the information. Besides, we give security investigation and behavior broad execution assessment to demonstrate the achievability of our configuration for big business clients.
The following paper is structured as follows.

1. Related background is described in Section.
2. While targeted system models and two cryptographic building blocks are presented in Section.
3. Our novel construction is detailed in Section.
4. Then the security and performance analysis are shown in Section.
5. Finally, our contributions are reiterated and future direction is mentioned to conclude this paper.

II. ENCRYPTION

A. ATTRIBUTE-BASED ENCRYPTION

Property based Encryption (ABE) gives a fine-grained access control of shared information. ABE was begun from the work by Sahai and Waters [10]. Later, two tracks of ABE have been produced: figure content strategy ABE (CP-ABE) [13], [15] and key-approach ABE (KP-ABE) [12], [14]. In the CP-ABE plan, the client is conceded characteristic keys (connected with qualities), and the entrance arrangement could be authorized on the figure content. At that point the client possesses the property keys fulfilling the predetermined access arrangement, the client could unscramble the message. An opposite setting is called KP-ABE, which indicates decoding approach on the property keys and the figure content is labeled with an arrangement of traits.
Be that as it may, to send in handy applications, overseeing dynamic access approach is required to bolster steadily changing access bunch. At that point the property keys ought to be re-issued and figure content be re scrambled to consent to the present access control arrangement. In other hand, client repudiation ought to be done in a productive approach to control the harms. Some ABE proposed that the close time is added with the property when producing related trait keys [13], [17]. In any case, the exchange off between the granularity of "window of powerlessness" and the weight to upgrade the property keys ought to be considered. Boldyreva et al. [16] proposed an effective renouncement plan for IBE and KP-ABE, while Yu et al. [18] proposed an ABE plan with quality denial. They coordinated the intermediary re-encryption (PRE) with ABE, and empowered the power to appoint the greater part of the work for key redesign of the client to intermediary servers. Since part based access control (RBAC) [34] is regularly used to confining framework access to approved clients. CP-ABE, which is firmly identified with RBAC, is picked as a building piece of our plan for big business application situation.

B. SEARCHABLE ENCRYPTION

Searchable encryption empowers clients to conceal the searchable catchphrases (of a record) by encryption. Later, clients could create suitable tokens/trapdoors for particular catchphrases to recover the encoded information containing these watchwords. Senegal. [19] initially presented the idea of looking on encoded information and gave down to earth arrangements. Goh [20] then formalized the idea of security for this issue and built a more proficient plan utilizing Bloom channel. Taking after that, some examination [22], [23] was led to either enhance the proficiency or give more grounded security of searchable encryption. One shared characteristic of these works is that they all bolstered just single watchword inquiry in the symmetric key setting.

DOI: 10.15680/IJIRCCE.2016. 0409181

The idea of conjunctive catchphrase look in symmetric key setting was initially presented by Galle et al. [25]. They gave a security idea to conjunctive catchphrase look over scrambled information and developed a more productive plan contrasted and the one inconsequentially reached out from single watchword hunt plan. Later, Ballardet al. [26] enhanced by shortening the trapdoor size and diminishing calculation/stockpiling overhead. Be that as it may, because of the symmetric key setting, these plans just empower one client to store and recover his/her own private information. Sharing of file building and looking capacity can't be accomplished effortlessly.

Boneh et al. [21] initially tended to one sort of down to earth applications called email directing framework. The searchable file of a mail can be produced by utilizing the beneficiary's open key. The beneficiary can recover specific messages from the steering server by appointing related trapdoors. The relating messages can be gathered. What's more, Boneh et al. [35] proposed another application brought seeking over review log, where the organization can designate particular trapdoor to the examiner to assess just review related records. Be that as it may, these plans upheld just single catchphrase inquiry. There are different applications requiring more expressive hunt over conceivable watchwords.

To improve look expressions, Park et al. [27] proposed open key encryption with conjunctive catchphrase look (PECK). Boneh et al. [36] further gave a plan supporting the conjunction of subset and reach inquiries on figure content information. At that point their development utilized the bilinear gathering of Composite way, which yields less effective development. Furthermore, they considered just single-client setting, where sharing of searchable list is difficult to accomplish. Hwan get al. [28] gave one productive PECK and considered a conceivable expansion to multi-client settings [29], [30]. In this paper, we will advance consider the sharing of searchable list ought to be given to empower bunch coordinated effort.

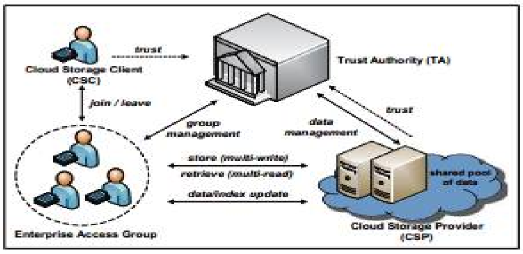
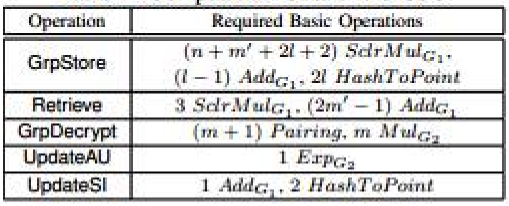


Fig. 1: Enterprise Cloud Storage Access Model

III. SECURITY AND PERFORMANCE

In this area, we show the security and execution of our convention. In this showing, just approved gathering individuals can 1) look/recover the gathering information and 2) unscramble the recovered gathering information put away in cloud stockpiles. The representative who leaves the gathering or is disavowed can't recover or decode the put away information in cloud stockpiles. Besides, we assess the calculation and correspondence costs for the CSC in our outline and finish up our configuration is successful and productive for the venture clients to share information and team up as a gathering

Table 2: Computation Cost of the CSC



Operation	Required Basic Operations
GrpStore	$(n + m' + 2l + 2)\ SclrMul_{G_1}$, $(l - 1)\ Add_{G_1}$, $2l\ HashToPoint$
Retrieve	$3\ SclrMul_{G_1}$, $(2m' - 1)\ Add_{G_1}$
GrpDecrypt	$(m + 1)\ Pairing$, $m\ Mul_{G_2}$
UpdateAU	$1\ Exp_{G_2}$
UpdateSI	$1\ Add_{G_1}$, $2\ HashToPoint$

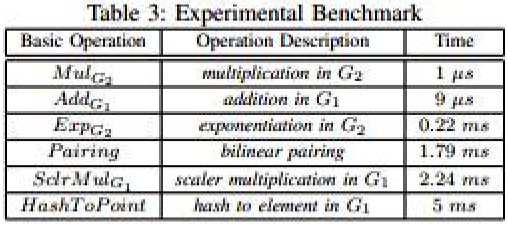
A. SECURITY ANALYSIS

The security of our convention depends on the fundamental ABEar [18] and muPECK [28]. From one viewpoint, the ABEar is turned out to be semantically secure under particular id picked plaintext assault (IND-s ID-CPA) accepting decisional bilinear Diffie-Hellman (DBDH) is hard. Taking into account these formal contentions, we can presume that the unapproved element (either CSC or CSP) can't fashion searchable records and searchable trapdoors since these activities are included in taking care of the difficult issue.

Then again, the muPECK is turned out to be semantically securing under multi-client figure content from arbitrary against picked watchword assaults (IND-mCR-CKA) expecting choice direct Daffier-Hellman (DLDH) is hard. In this manner, the unapproved substance can't compute characteristic keys for unscrambling, either in light of the fact that these activities are included in taking care of the DLDH difficult issue.

Concerning information flow, the information is re-scrambled to the same figure content space. The re-created key is likewise circulated consistently in the key space. Any foe can't increase any more preferences since he/she needs to manage the same difficult issues as the ones before information/key upgrade. What's more, the client flow is taken care of by including/evacuating one a player in searchable file of that client and issuing/redesigning the quality keys of that gathering. The mystery of the information encoded under indicated access approach can be ensured when bunch individuals join or leave, while the entrance control of inquiry ability of gathering individuals can be guaranteed.

Table 3: Experimental Benchmark



Basic Operation	Operation Description	Time
Mul_{G_2}	*multiplication in* G_2	$1\ \mu s$
Add_{G_1}	*addition in* G_1	$9\ \mu s$
Exp_{G_2}	*exponentiation in* G_2	$0.22\ ms$
$Pairing$	*bilinear pairing*	$1.79\ ms$
$SclrMul_{G_1}$	*scaler multiplication in* G_1	$2.24\ ms$
$HashToPoint$	*hash to element in* G_1	$5\ ms$

One approved client, while Update SI relies on upon 2 Hashand 1 increases in G1for the incorporation/rejection of one single searchable list. If you don't mind allude to Table. 2. with respect to correspondence cost, the CSC needs to start a solicitation for Grp Store, Retrieve, Update AK, Update CT, Update AU, and Update SI. At that point the CSC gets the reaction from the CSP. One and only round of correspondence is required.

The trial benchmark is directed utilizing neighborhood server with Intel Xeon processor E5620 at 2. 40GHz running Ubuntu 11.10. We utilize GNU numerous accuracy number juggling library (GMP) [37] and blending based cryptography library (PBC) [38] libraries. We select one super solitary bend overb one base field of size 512 bits and the implanting degree is 2. In this way the security level is set to be ECC-160 bits. The measure of one gathering component in G1 is 1024 bits. The expense of one expansion in G1 costs9 µs, while one increase in G1 requires 2. 24ms. One increase in G 2 requires 1 µs, while one exponentiation in G2 costs0. 22ms. At last, the bilinear matching needs 1. 79ms, and hash to G 1 component expends 5. 00ms. (See Table 3)

IV. PROPOSED SYSTEM

Secure situations ensure their assets against unapproved access by upholding access control components. So the quickly expanding security is an issue content based passwords are insufficient to counter such issues. At that point the requirement for something more secure alongside being easy to use is required. At that point this is the place Image Based Authentication (IBA) becomes an integral factor. This takes out storm assault, shoulder assault. Utilizing the texting administration accessible in web, client will acquire the OTP after picture checking. At that point this OTP then can be utilized by client to get to their own records. The picture construct verification strategy depends in light of the client's capacity to perceive pre-picked classifications from a matrix of pictures. In this paper I incorporates Image based validation and one time watchword to accomplish abnormal state of security in verifying the client over the web.

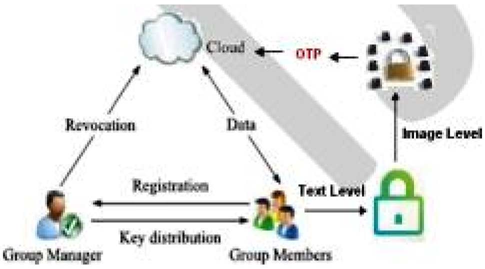


Fig.2 System Architecture.

The fundamental Objective of 3 Level Security framework is a one of a kind and an exclusive investigation of utilizing pictures as secret key and execution of a to a great degree secured framework, distinguishing 3 levels of security.
Level 1: Security at level 1 has been forced by basic content –based secret word.
Level 2: Security at this level has been forced by utilizing picture based validation (IBA) which wipes out shoulder assault, whirlwind assault. Client needs to choose three pictures from that point sportive lattice.
Level 3: After the viable elbowroom of the above two levels, the Level 3 Security System will then deliver a one-time numeric mystery word that would be true blue just for that login session. The check customer will be instructed of this one time mystery word on his email id.

V. CONCLUSION

In this paper, we propose a novel distributed storage development empowering the administration of searchable element information for gathering cooperation. Our commitments are abridged in the accompanying three noteworthy components of our convention: (1) expressly tending to big business application situation of cloud stockpiles as far as framework design and usefulness. (2) A novel access-control plan for the endeavor clients to share the dynamic information and work together as a gathering, and (3) A practical configuration as far as the venture client's stockpiling, calculation and correspondence while (2) is accomplished. For the future work, we might want to facilitate incorporate other vital functionalities for the undertaking, for example, open examining and secure cloud information calculation, to empower completely fledged distributed storage for future venture applications.

REFERENCES

1. P. Mell and T. Grance, “The nist definition of cloud computing (draft) recommendations of the national institute of standards and technology,” Nist Special Publication , vol. 145, no. 6, p. 7, 2011.
2. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” EECS Department, University of California, Berkeley, Tech. Rep., Feb 2009.
3. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility,”Future Generation Computer Systems, vol. 25, no. 6, pp. 599 – 616, 2009.
4. Nist, “Fips pub 197: Announcing the advanced encryption standard (aes),” NIST, 2001.
5. J. Jonsson and B. Kaliski, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,” no. 3, February 2003. [On line]. Available: http://www.ietf.org/rfc/rfc3447
6. D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” SIAM J. of Computing, vol. 32, no. 3, pp. 586–615, 2003, extended abstract in Crypto’01.
7. N. Virvilis, S. Dritsas, and D. Gritzalis, “Secure cloud storage: Available infrastructures and architectures review and evaluation,” in Trust, Privacy and Security in Digital Business, ser. Lecture Notes in Computer Science, S. Furnell, C. Lambrinoudakis, and G. Pernul, Eds. Springer, 2011, vol. 6863, pp. 74–85.
8. K. Yang and X. Jia, “Data storage auditing service in cloud computing: challenges, methods and opportunities,” World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.
9. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” Commun. ACM, vol. 53, pp. 50–58, Apr. 2010.
10. A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology - EUROCRYPT 2005 , ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer, 2005, vol. 3494, pp.557–557.
11. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute-based systems,” in Proceedings of the 13th ACM conference on Computer and communications security, ser. CCS ’06. New York, NY, USA: ACM, 2006, pp. 99–112.
12. 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, ser. CCS ’06. New York, NY, USA: ACM, 2006,pp. 89–98.

13. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in Proceedings of the 2007 IEEE Symposium on Security and Privacy , ser. SP ’07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334.

14. R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” in Proceedings of the 14th ACM conference on Computer and communications security, ser. CCS ’07. New York, NY, USA: ACM, 2007, pp. 195–203.

15. B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography - PKC 2011 , ser. Lecture Notes in Computer Science, D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, Eds. Springer, 2011, vol. 6571, pp. 53–70.

16. A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” inProceedings of the 15th ACM conference on Computer and communications security, ser. CCS ’08. New York, NY, USA: ACM, 2008, pp. 417–426. [Online]. Available: http://doi.acm.org/10.1145/1455770.1455823

17. R. Bobba, H. Khurana, and M. Prabhakaran, “Attribute-sets: A practically motivated enhancement to attribute-based encryption,” in Computer Security â A¸S ESORICS 2009, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds. Springer, 2009, vol. 5789, pp.
587–604.

18. S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS ’10. New York, NY, USA: ACM, 2010, pp. 261–270. [Online]. Available: http://doi.acm.org/10.1145/1755688.1755720

19. D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Security and Privacy, 2000. S P 2000.Proceedings. 2000 IEEE Symposium on, 2000, pp. 44 –55.

20. E.-J. Goh, “Secure indexes,” IACR Cryptology ePrint Archive , vol.2003, p. 216, 2003.

BIOGRAPHY

KORUMILLI LAVANYA: M.Tech, CSE Dept, Pragati Engineering College, Surampalem.She completed Master of Computer Applications at Sai Aditya P.G college,Kakinada.

Grandhi Satya Suneetha: is working as an Assistant Professor in department of Computer Science and Engineering, Pragati Engineering College.She is a postgraduate in Computer Science and Technology and had 12 years of teaching experience. Her areas of interest include BigData and Cloud Computing.

RAYAVARAPU SRIDIVYA: is working as an Assistant Professor in department of Computer Science and Engineering, Pragati Engineering College. She is a postgraduate in Computer Science and Technology and had 6 years of teaching experience.

DOI: 10.15680/IJIRCCE.2016. 0409181