Journal of Research in Science, Technology, Engineering and Management (JoRSTEM)
Volume. 1, Issue: 2, December 2015

Advanced Secure Mona Protocol for Data Sharing in Untrusted Cloud Using Attribute Based Encryption

Mr. M. Sathish[1], Mr. P. A Hima Kiran[2]

[1] M.Tech Student, Dept. of cse, Malla Reddy Engineering College (Autonomous), Hyderabad, Telangana India.

[2] Associate Professor, Dept. of cse, Malla Reddy Engineering College (Autonomous), Hyderabad, Telangana India.

[1]sathishmarripally28@gmail.com
[2]andrewshimakiran@mrec.ac.in

Abstract— Sharing gathering asset among cloud clients is a noteworthy impact, so distributed computing gives a prudent and proficient arrangement. Because of proceeds with change of sharing information, enrollment in a multi-proprietor way to an un trusted cloud is still a testing issue. Here in this paper, We propose a safe multi-proprietor information sharing plan, for dynamic (continuously changing) bunch in the cloud. By giving gathering signature and element show encryption strategies, any cloud client can defensively impart information to others. At that point an in the mean time, the capacity overhead and encryption calculation expense of the plan are autonomous with the quantity of repudiated clients. In other hand, we break down the security of this plan with thorough verifications. OTP (One-Time Password) is one of the least difficult and most well known types of confirmation that can be utilized for securing access to accounts. OTP are regularly alluded to as a protected and more grounded types of validation, and tolerating them to introduce over different machines. We give a different levels of security to share information among multi-proprietor process. To start with the client chooses the pre-chosen picture to login. At that point chooses a picture from the lattice of pictures. By utilizing this the OTP is produced consequently and sent to relating email account.

Keywords— *Security, Broadcast Message, Encryption, Cloud computing.*

I. INTRODUCTION

Distributed computing imagines exceedingly accessible, on-interest system access to a mutual pool of configurable registering assets [1], [2], [3]. Clients can appreciate adaptable capacity limit and calculation ability without paying consideration on the development and upkeep of these foundations. While distributed computing gets promising open doors, it additionally brings along new security and protection issues, which ruin people in general to receive the cloud advances. 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 systems are accessible to ensure the security of Cloud information and administrations [7], [8], [9]. In any case, as these encryption methods bring along new procedures, additional complexities must be conceived to oversee scrambled information safely and effectively. For an individual distributed storage client, he/she stores his/her information and recovers some portion of the put away information later. Then again, for big business clients, the put away information ought to be shared among gathering individuals. One sort of encryption plan called characteristic based encryption (ABE) could be utilized to apply fine-grained access control over the common information [10], [11], [12], [13], [14], [15]. What's more, the flow of gathering individuals and comparing put away information ought to be considered to build a possible fine-grained access control for the venture [16], [17], and [18].

Besides, given the aggregate sum of information produced and put away in the cloud, getting to information through route is tedious and vexatious. Getting to cloud information through (catchphrase) inquiry is thought to be viable and in superfluous. Be that as it may, as the cloud information are secured through cryptographic systems, which acquire high expenses when recovering through seeking. Searchable encryption was acquainted with empower clients to shroud the searchable catchphrases (of a document) by encryption [19], [20], [21], [22], [23] [24]. Later, clients could create fitting tokens/trapdoors for particular catchphrases to recover the scrambled information containing these watchwords. The clients looking capacity is likewise shared under fine-grain arrangements [25], [26], [27], [28] One client can create searchable files for a document and indicate a subset of clients who can use these searchable records. Clients outside the predefined gathering can't hunt out this document. Then again, motion of gathering individuals and searchable files ought to be considered to yield a down to earth and powerful searchable encryption [29], [30].

In this paper, we propose one novel distributed storage development empowering the administration of element searchable information for gathering joint effort. We make utilization of characteristic based encryption plan (ABE) and open key encryption with conjunctive watchword pursuit (PECK) to outline our convention. We show that our plan exceptionally incorporates fundamental usefulness for big business clients, to be specific, the fine-grained access control for the searchable record and the substance of the information. Moreover, we give security examination 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 foundation is depicted in Section.
2. While focused on framework models and two cryptographic building squares are displayed in Section.
3. Our novel development is point by point in Section.
4. Then the security and execution investigation are appeared in Section.
5. Finally, our commitments are emphasized and future course is specified to close this paper.

II. ENCRYPTION

2.1 Attribute-based Encryption

Attribute based Encryption (ABE) gives a fine-grained access control of shared information. ABE was started from the work by Sahai and Waters [10]. Later, two tracks of ABE have been produced: figure content arrangement ABE (CP-ABE) [13], [15] and key-strategy ABE (KP-ABE) [12], [14]. In the CP-ABE plan, the client is allowed trait keys (connected with qualities), and the entrance approach could be upheld on the figure content. At that point the client claims the trait keys fulfilling the predetermined access approach, the client could unscramble the message. An opposite setting is called KP-ABE, which determines decoding arrangement on the trait keys and the figure content is labeled with an arrangement of qualities.

In any case, to send in down to earth applications, overseeing element access approach is required to bolster perpetually changing access bunch. At that point the trait keys ought to be re-issued and figure content be re scrambled to consent to the present access control arrangement. In other hand, client renouncement ought to be did in a productive approach to control the harms. Some ABE proposed that the lapse time is added with the quality when creating related property keys [13], [17]. On the other hand, the exchange off between the granularity of "window of defenselessness" and the weight to upgrade the quality keys ought to be considered. Boldyreva et al. [16] proposed an effective denial plan for IBE and KP-ABE, while Yu et al. [18] proposed an ABE plan with property disavowal. They incorporated the intermediary re-encryption (PRE) with ABE, and empowered the power to designate a large portion of the work for key overhaul of the client to intermediary servers. Since part based access control (RBAC) [34] is normally used to limiting framework access to approved clients. CP-ABE, which is firmly identified with RBAC, is picked as a building square of our plan for big business application situation.

2. 2 Searchable Encryption

Searchable encryption empowers clients to conceal the searchable watchwords (of a document) by encryption. Later, clients could create suitable tokens/trapdoors for particular catchphrases to recover the scrambled 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 developed a more effective plan utilizing Bloom channel. Taking after that, some exploration [22], [23] was led to either enhance the effectiveness or give more grounded security of searchable encryption. One shared trait of these works is that they all upheld just single watchword hunt in the symmetric key setting.

The idea of conjunctive catchphrase look in symmetric key setting was initially presented by Galle et al. [25]. They gave a security thought to conjunctive watchword look over encoded information and built a more proficient plan contrasted and the one insignificantly stretched out from single catchphrase pursuit plan. Later, Ballardet al. [26] enhanced by shortening the trapdoor size and lessening 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 particular private information. Sharing of file building and looking ability can't be accomplished effortlessly.

Boneh et al. [21] initially tended to one sort of reasonable applications called email steering framework. The searchable list of a mail can be created by utilizing the beneficiary's open key. The beneficiary can recover specific messages from the delegating so as to steer server related trapdoors. The relating messages can be gathered. What's more, Boneh et al. [35] proposed another application brought looking over review log, where the organization can appoint particular trapdoor to the evaluator to examine just review related records. Be that as it may, these plans upheld just single watchword pursuit. There are different applications requiring more expressive pursuit over conceivable watchwords.

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

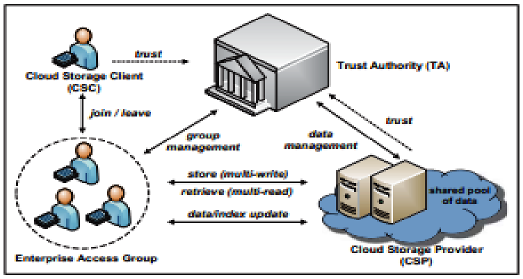
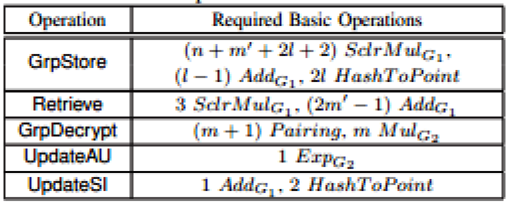


Fig. 1: Enterprise Cloud Storage Access Model

III. SECURITY AND PERFORMANCE

In this area, we show the security and execution of our convention. In this exhibit, just approved gathering individuals can 1) Search/recover the gathering information and 2) unscramble the recovered gathering information put away in cloud stockpiles. The worker who leaves the gathering or is denied can't recover or decode the put away information in cloud stockpiles. In addition, we assess the calculation and correspondence costs for the CSC in our configuration and close our outline is powerful and proficient 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	$1\ Add_{G_1}$, $2\ HashToPoint$

3.1 Security Analysis

The security of our convention depends on the basic ABEar [18] and muPECK [28]. From one perspective, the ABEar is ended up being semantically secure under specific id picked plaintext assault (IND-s ID-CPA) accepting decisional bilinear Diffie-Hellman (DBDH) is hard. In light of these formal contentions, we can presume that the unapproved substance (either CSC or CSP) can't manufacture 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 catchphrase assaults (IND-mCR-CKA) accepting choice straight Daffier-Hellman (DLDH) is hard. In this way, the unapproved element can't compute quality keys for decoding, either in light of the fact that these activities are included in taking care of the DLDH difficult issue.

With respect to information elements, the information is re-encoded to the same figure content space. The re-created key is likewise appropriated consistently in the key space. Any enemy can't increase any more points of interest since he/she needs to manage the same difficult issues as the ones before information/key upgrade. What's more, the client elements is taken care of by including/evacuating one piece of searchable file of that client and issuing/upgrading the property keys of that gathering. The mystery of the information encoded under determined access strategy can be ensured when bunch individuals join or leave, while the entrance control of pursuit capacity 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 authorized user, while Update SI depends on 2 Hashand 1 additions in G1for the inclusion/exclusion of one single searchable index. Please refer to Table. 2. as for communication cost, the CSC has to initiate a request for Grp Store, Retrieve, Update AK, Update CT, Update AU, and Update SI. Then the CSC receives the response from the CSP. Only one round of communication is required.

The experimental benchmark is conducted using local server with Intel Xeon processor E5620 at 2. 40GHz running Ubuntu 11.10. We use GNU multiple precision arithmetic library (GMP) [37] and pairing-based cryptography library (PBC) [38] libraries. We select one super singular curve overb one base field of size 512 bits and the embedding degree is 2. Thus the security level is set to be ECC- 160 bits. The size of one group element in G1 is 1024 bits. The cost of one addition in G1 costs9 µs, while one multiplication in G1 requires 2. 24ms. One multiplication in G 2 requires 1 µs, while one exponentiation in G2 costs0. 22ms. Finally, the bilinear pairing needs 1. 79ms, and hash to G 1 element consumes 5. 00ms. (See Table 3)

IV. PROPOSED SYSTEM

Secure environments protect their resources against unauthorized access by enforcing access control mechanisms. So the rapidly increasing security is an issue text based passwords are not enough to counter such issues. Then the need for something more secure along with being user friendly is needed. Then this is where Image Based Authentication (IBA) comes into play. This helps to eliminate tempest attack, shoulder attack. Using the instant messaging service available in internet, user will obtain the OTP after image checking. Then this OTP then can be used by user to access their personal accounts. The image based authentication method relies on the user’s ability to recognize pre-chosen categories from a grid of pictures. In this paper I integrates Image based authentication and one time password to achieve high level of security in authenticating the user over the internet.

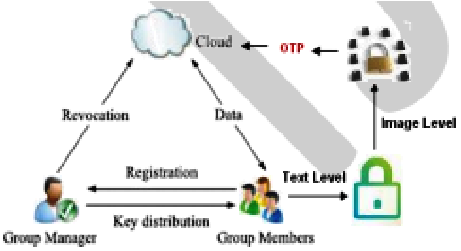


Fig.2 System Architecture.

The principle Objective of 3 Level Security framework is an extraordinary 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 straightforward content –based secret key.

Level 2: Security at this level has been forced by utilizing picture based verification (IBA) which disposes of shoulder assault, storm assault. Client needs to choose three pictures from that point sportive matrix.

Level 3: After the fruitful freedom of the above two levels, the Level 3 Security System will then produce an one-time numeric secret word that would be substantial only for that login session. The check client will be educated of this one time secret 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 joint effort. Our commitments are compressed in the accompanying three noteworthy components of our convention: (1) unequivocally tending to big business application situation of cloud stockpiles regarding framework structural planning and usefulness. (2) A novel access-control plan for the undertaking clients to share the dynamic information and team up as a gathering, and (3) A practical outline regarding the venture client's capacity, calculation and correspondence while (2) is accomplished. For the future work, we might want to further incorporate other imperative functionalities for the venture, for example, open reviewing and secure cloud information calculation, to empower completely fledged distributed storage for future enterprise 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.