IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 10, Issue 1, January 2020, ||Series -VI|| PP 01-05

Dynamic and Advanced Security Approach for Data Storage in Distributed Environment

E Yohoshva[1], Dr. N.K. Kameswara Rao[2]

[1]M.Tech, Department of IT SRKR Engineering College, Bhimavaram
[2] Professor, Department of IT SRKR Engineering College, Bhimavaram India

Received 03 January 2020; Accepted 17 January 2020

Abstract: With the implementation of data sourcing and other cloud services in real time environment, it describes efficient data transmission between different users parallel in distributed environment. Security or privacy is also important factor in data different users data sharing so that efficient and advanced cryptography system is required to do privacy for data from multiple users in cloud computing. Attribute based encryption is one of the basic advanced encryption system to provide efficient privacy between multiple users in distributed environment. Cipher text policy based attributed based encryption (CP-ABE) and Deffie- Hellman is one of the advanced secure approach proposed in this paper to multi user data sharing in distributed environment. In this scenario reduce the computational cost overhead in data sharing and other features in distributed environment. Performance evaluation of proposed approach describes efficient results in terms of encryption, decryption and other specification in cloud computing environment

Index Terms: Attribute based encryption, Cipher text policy based encryption, distributed computing,

I. INTROUDCTION

Cloud computing is the basic application to share data with different resources to accomplish equivalent economic scale to provide efficient data out sourcing in distributed environment. At the implementation of appropriate broadcast communication establishment between different organizations relates to cloud applications. Because of difficulties in data sharing of the cloud, i.e. security is the main security aspect in customers' ability to share data without any privacy aspects for distributed environment. Cloud resources are also major impact in data sharing between different users in cloud, for instance cloud client enter into application and then serve the resources like file sharing, and different types of security related approaches were introduced/developed to explore resource sharing between users in distributed environment. Various customers face different security concerns in storage of their data in distributed environment to explore access control issues with square different services in cloud for various applications.

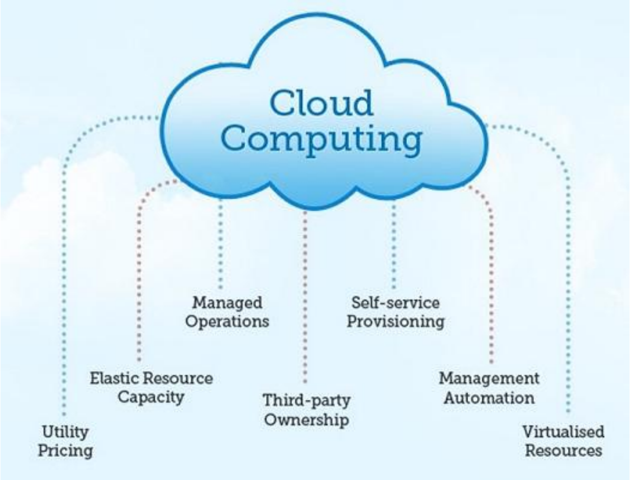

Figure 1: Different cloud computing services with respect to processing

As appeared in the above figure distributed computing gives three sorts of administrations with respect to cloud administration and different procedures present in conveyed registering tasks. The ABE plan can result the issue that data owner needs to utilize each endorsed client's locale key to verify data. Key-approach property based security (KP-ABE) plan planned the openness plan into the client's close to home key and portrayed the protected data with client's highlights. The KP-ABE plan can achieve the grained openness the executives and more edibility to the executives clients than ABE plan. Yet, the downside of KP-ABE is that the availability plan is planned into a client's close to home key, so data owner can't pick who can unscramble the data aside from choosing a lot of highlights which can clarify this data. What's more, it is unseemly in certain program on the grounds that a data owner needs to have faith in the key organization. CP-ABE plan structured the availability plan into the verified information; a lot of highlights is in a client's critical. The CP-ABE plan subtleties the issue of KP-ABE that data owner just confides in the key organization. To assess the proficiency of our ABE plan with demonstrated contracted unscrambling, we apply the CP-ABE plan with demonstrated contracted decoding and perform tests. In this paper we propose to create Advanced Attribute Based Encryption will be relevant for developing adaptable and adaptable and fine grained access control of out sourcing information in distributed computing. EABE extends the figure content strategy trait set-based security (CP-ASBE, or ASBE for short) plot by Bobba et al. [3] with an arranged structure of program clients, in order to achieve adaptable, adaptable and fine-grained availability the board. The cooperation of the report is multifold. Attribute based encryption is one of the basic advanced encryption system to provide efficient privacy between multiple users in distributed environment. Cipher text policy based attributed based encryption (CP-ABE) and Deffie- Hellman is one of the advanced secure approach proposed in this paper to multi user data sharing in distributed environment. In this scenario reduce the computational cost overhead in data sharing and other features in distributed environment. Performance evaluation of proposed approach describes efficient results in terms of encryption, decryption and other specification in cloud computing environment

II. ENHANCED SECURITY MODEL

We propose to create effective acknowledge adaptable and adaptable access control with respect to fine gained services re-appropriating in computing distributed environment, this section describe the proposed procedure to create Encryption based on Enhanced Attributes dependent on hierarchal trait set based security in out sourced information of distributed computing. the thinking figuring framework under thought comprises of five sorts of gatherings: a thinking bolster organization, data business visionaries, data clients, various area controllers, and a solid power. The cloud computation organizations deal with data outsourcing to support efficient data retrieval from distributed cloud environment with security. Data could be stored in cloud and then share them to multiple clients in cloud, to access multiple types of data from multiple clients with encryption and decryption in centralized cloud environment. Every data proprietor/buyer is administrated by a division control. A part power is overseen by its parent area control or the dependable power. [8][9] Data business visionaries, data clients, part controllers, and the solid power are composed in a various leveled way as appeared in figure 2.

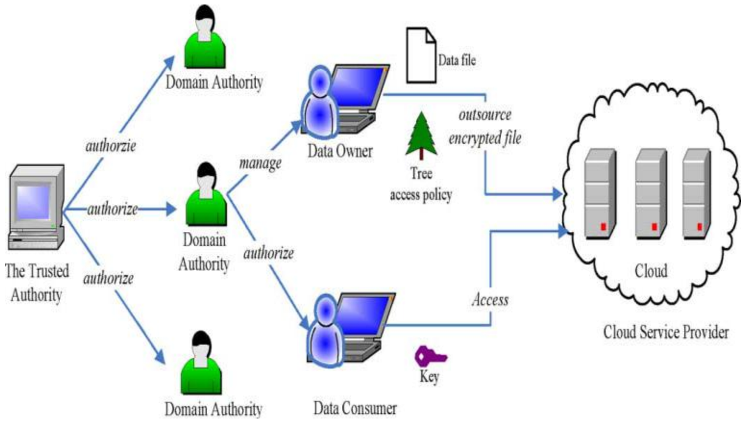

Figure 2 Procedure to explore different services in distributed environment

To provide efficient resource utilization with respect to top level segment in sharing of data to multi clients, each client share data with top level security which is matched with data original content cloud business organization explore their business in distributed environment. Data proprietors/purchasers may match to laborers in an organization [16] . Every segment power is responsible for taking care of the area controllers at the following stage or the data proprietors/customers in its part. In our framework, neither information business visionaries nor information clients will be consistently on the web. They please the web just when vital, while the thinking administration office, the dependable power, and segment controllers are consistently on the web. The thinking is accepted to have various extra room potential and computations control. Moreover, we accept that information clients can get to data for considering as it were.

III. PERFORMANCE EVALUATION

In this section, we initially assess theoretic figuring’s multifaceted nature of the recommended arrangement in each capacity. At that point we execute an EASBE device set as per the instrument set produced for CP-ABE. also, play out an arrangement of tests to assess productivity of our proposed arrangement [14]. In this area we process execution assessment and after that usage system for characteristic based encryption in distributed computing.

3.1. Execution Evaluation

We assess the figuring’s unpredictability for each program activity in our arrangement as pursues.

Framework Setup: When the program is set up, the solid specialist chooses a bilinear group and some one of a kind numbers. At the point when keys are created PK and MKo are delivered, there will be a few exponentiation capacities. So the computations unpredictability of Program Installation is O(1).

Top-Level Sector Power Grant: This activity is directed by the dependable power. The ace key of a segment power is as where is the key structure related with another area specialist, is the set . Give N a chance to be the quantity of traits in and M be the quantity of sets in , then the mix of the method comprises two exponential qualities for each property.

New User/Domain Power Allow. In this capacity, another client or new area specialist is related with a characteristic set, which is the arrangement of that of the in the space expert. The essential computations cost of this activity is rerandomizing the key.

Document information with new user version: It describes the basic parameters relates to user and describe the used parameters and generate the key for them to provide efficient communication in data outsourcing. In proposed approach, each document depends on document size with privacy prediction.

Document Revocation by User: In this scenario, each user stores data if is satisfied his/her conditions in sharing and storing data between different users in distributed environment. If any user perform wrong prediction in data sharing then automatically that user revoke permissions to other users in distributed environment. Generate secure key for each file and then if key satisfy with other user’s data then it automatically revoked from cloud.

Access control to Document: This function verified by the different users in cloud, which are the users are reliable to share and access data, check every time this condition at each user. If any user share document to one of the user present in cloud with encryption and then that particular user access and check permission every time with operations in cloud. Every check the secure keys in data sharing to all the users in cloud with feasible operations..

Record Removal: This capacity is actualized at the interest of a data owner. On the off chance that the thinking can affirm the requestor is the proprietor of the data document, the thinking expels the PC data record. So the calculation unpredictability is O (1).

3.2. Implementation

We have applied a staggered EABE device set as per the cpabe apparatus set from (http://acsc.csl.sri.com/cpabe/) produced for CP-ABE which uses the cryptography with description of parameters (http://crypto.stanford.edu/pbc/). At that point exhaustive tests are performed on a PC with double center 2.10-GHz CPU and 2-GB RAM, working Ie8 10.04. We make an examination on the preliminary data and gives the numerical data.

EABE-arrangement: Produces a network key master key MK0 with public key representations .

EABE-keygen: Generate public key for all the users with master key MK0, network key system for different users in data outsourcing is fulfilled.

EABE-keydel: Given PK and MKi of DA , assigns a few territories of DA 's individual significant elements to another client or DA in its segment. The alloted key is similar to creating private significant factors by the principle control.

EABE-keyup: Given PK , the individual key, the new property and the part, creates another individual key which contains the new include.

EABE-enc: Given PK, scrambles a PC document under an openness tree approach indicated in an arrangement wording. EABE-dec: Given an individual key, unscrambles a PC document.

EABE-rec: Given PK , an individual key and a verified PC document, re-encode the PC record. See that the individual key ought to have the option to decode the verified document.

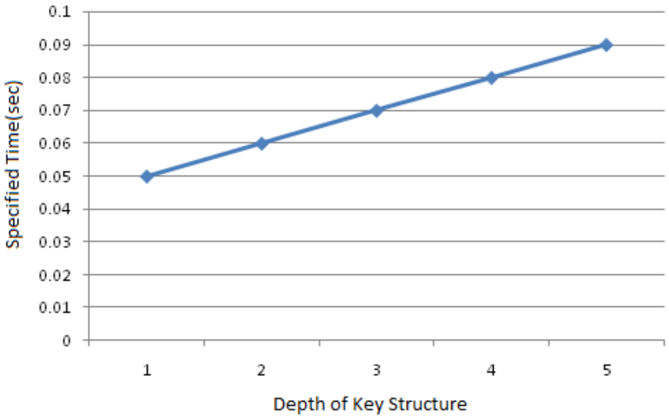

Figure 3 Encryption time for processing key structure in distributed environment

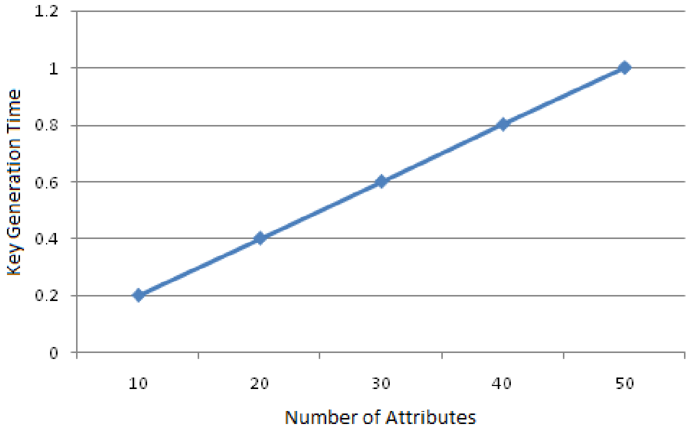

Figure 4 Key level based encryption with respect to different users in distributed environment.

Based on above figure our proposed approach gives better efficiency with respect to key generation and encryption for different users in distributed environment.

IV. CONCLUSION

In In this paper, present and introduce encryption based on enhanced attribute procedure using the encryption and decryption procedure i.e. Deffie-Hellman procedure for secure data sharing in distributed environment. Encryption based on user attributes is performed in this region to maintain hierarchy structure with different labels in cloud computing. This procedure provides efficient and scalable data sharing between different users in distributed environment. In conclusion, we executed the recommended arrangement, and performed extensive execution research and evaluation, which uncovered its effectiveness and favorable circumstances over ebb and flow strategies. Further improvement of our recommended work will be created in numerous client openness the board strategy with continuous database incorporation in thinking preparing.

REFERENCES

[1]. [1] B. Xu et al., "Ubiquitous data accessing method in IoT-based information system for emergency medical services", IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1578-1586, May 2014

[2]. [2] M. B. Mollah, M. A. K. Azad, A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted Internet of Things", IEEE Cloud Comput., vol. 4, no. 1, pp. 34-42, Jan./Feb. 2017

[3]. [3] A. Castiglione, K.-K. R. Choo, M. Nappi, S. Ricciardi, "Context aware ubiquitous biometrics in edge of military things", IEEE Cloud Comput., vol. 4, no. 6, pp. 16-20, Nov./Dec. 2017

[4]. [4] A. Kumari et al., "Multimedia big data computing and Internet of Things applications: A taxonomy and process model", J. Netw. Comput. Appl., vol. 124, pp. 169-195, Dec. 2018.

[5]. [5] S.-H. Seo, M. Nabeel, X. Ding, and E. Bertino, “An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds,” IEEE Trans. Knowledge and Data Engineering, vol. 26,

[6]. no. 9, 2014, pp. 2107–2119.

[7]. [6] H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari,and X. Yi, “Secure Data Analytics for CloudIntegrated Internet of Things Applications,” IEEE Cloud Computing, vol. 3, no. 2, 2016, pp.46–56.

[8]. [7] J.B. Bernabe, J.L.H. Ramos, and A.F.S. Gomez, “TACIoT: Multidimensional Trust-Aware Access Control System for the Internet of Things,” Soft Computing, vol. 20, no. 5, 2016, pp. 1763–1779..

[9]. [8] U. Feige and J. Kilian, “Making games short (extended abstract),” in Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, ser. STOC ’97. New York, NY, USA: ACM, 1997, pp. 506–516.

[10]. [9] S. Hohenberger and A. Lysyanskaya, “How to securely outsource cryptographic computations,” in Proceedings of the Second international conference on Theory of Cryptography, ser. TCC’05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 264–282.

[11]. [10] R. Canetti, B. Riva, and G. Rothblum, “Two protocols for delegation of computation,” in Information Theoretic Security, ser. Lecture Notes in Computer Science, A. Smith, Ed. Springer Berlin / Heidelberg, 2012, vol. 7412, pp. 37–61.

[12]. [11] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, “New and secure outsourcing algorithms of modular exponentiations,” in 17th European Symposium on Research in Computer Security (ESORICS), 2012.

[13]. [12] M. J. Atallah and K. B. Frikken, “Securely outsourcing linear algebra computations,” in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS ’10. New York, NY, USA: ACM, 2010, pp. 48–59.

[14]. [13] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in Cryptology – CRYPTO, ser. Lecture Notes in Computer Science, G. Blakley and D. Chaum, Eds. Springer Berlin / Heidelberg, 1985, vol. 196, pp. 47–53.

[15]. [14] C. Cocks, “An identity based encryption scheme based on quadratic residues,” in Cryptography and Coding, ser. Lecture Notes in Computer Science, B. Honary, Ed. Springer Berlin / Heidelberg, 2001, vol. 2260, pp. 360–363.

E Yohoshva, et.al. "Dynamic and Advanced Security Approach for Data Storage in Distributed Environment". *IOSR Journal of Engineering (IOSRJEN)*, 10(1), 2020, pp. 01-05.