Efficient User Revocation Mechanism for Privilege and Anonymity in Control Cloud Data Access

S.Ilakiya[1], P.Mayilvahanan[2]
[1]Research Scholor, Vels University, Pallavaram, TamilNadu, India.
[2]H.O.D. Department of MCA.Vels University, Pallavaram, Chennai, Tamil Nadu, India.
selvarajilakiya13@gmail.com, hodmca@velsuniv.ac.in

Abstract **-** The most engaging a part of the cloud computing is that the computation outsourcing, it's far beyond enough to only conduct Associate in Nursing access management. Users need to regulate the privileges of knowledge manipulation over alternative users or cloud servers,this is often as a result of once sensitive data or calculation is outsourced to the cloud servers or another user, that is out of user's management in most cases, privacy risks would raise dramatically as a result of the servers would possibly illicitly examine user's knowledge and access sensitive data, or alternative users is also able to infer responsive information from the out-sourced calculation. Therefore, not alone the access but collectively the operation have to be compelled to be controlled. So a control, theme AnonyControl and a fully-anonymous attribute-based privilege management theme AnonyControl-F is planned to agitate the user privacy draw back in an exceedingly very cloud storage server. Conjointly an efficient user revocation mechanism is additionally introduced at the side of this theme.

I. INTRODUCTION

Computing resources (hardware and software) are used in **cloud computing** and that are given as a service through the network (from the Internet). The name cloud computing comes from the cloud-shaped representation as an abstraction for the complex infrastructure it is mentioned in system diagrams. Cloud computing consign remote services with a user's information, code and computation. Cloud computing consists of hardware and code resources created offered on the web as managed third-party services. These services usually give access to advanced code applications and high-end networks of server computers.

The capacity of cloud computing is to use superior computing power, ordinarily employed by military and analysis facilities to perform many of many computations per second, in consumer-oriented applications like financial portfolios, to deliver individualized information, to provide info storage or to power big, immersive laptop games. The cloud computing uses networks of huge groups of servers sometimes running cheap shopper laptop computer technology with connections that are specialized to unfold data-processing stints across them. This shared IT infrastructure contains big pools of systems that unit of measurement connected on. Often, virtualization techniques unit of measurement accustomed maximize the flexibility of cloud computing.

Advantages:

- **Price:** user pay for their usage in cloud.
- **Security**: Cloud models are solitary in the network from other model for increased security.
- **Performance:** Instances is another instantly for improved performance. Shoppers have access to the overall resources of the Cloud's core hardware.
- **Scalability:** Auto-deploy cloud model once it required.
- **Uptime:** Uses multiple servers for maximum hypes. In case of server failure, instances can be created on another server automatically.
- **Control:** From any location the user can login. Server snapshot.
- **Traffic:** Deals with spike in traffic with fast readying of extra instances to handle the load.

Benefits of cloud computing:

- Succeed economies of scale
- Scale back defrayment on technology infrastructure.
- Widen your work force on a budget.
- Contour processes.
- Scale back capital prices.
- Recover accessibility.
- Less personnel coaching is required.
- Minimize licensing new package.
- Improve flexibility.

II. EXISTING

This scheme proposes a control scheme to control the privileges of the data manipulation over the users of other clouds. This is because whenever privacy is concerned not just the privacy of information but also the privacy of user's information should also be addressed. The existing system doesn't supports user revocation problem.

III. PROPOSED

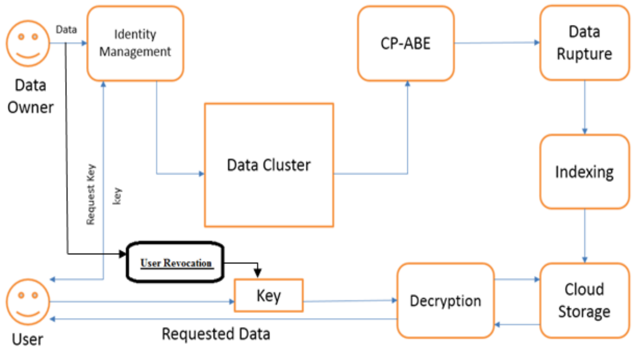

Figure 1

This proposes a control scheme Anony control to control and protect the privileges of user information. Using this scheme the privacy of users is protected. Also,whenever the admission is revoked the access permissions of the user should be revoked. This is addressed via user revocation problem.

User Revocation Based ABE ALGORITHM
The idea of attribute based encryption is one sort of open key encryption in which the client's mystery key and the figure content, both are qualities subordinate. In a framework, the decoding of a figure content is conceivable just if the arrangement of both qualities of the client key and the characteristics of the figure content matches, an essential security highlight is conspiracy resistance for Attribute-Based Encryption: An enemy that which holds different keys ought to just have the capacity to utilize information if no less than one single key gifts access.

IV. INPUT DESIGN

The input style is that the link that connects the knowledge system and also the user. It contains the procedures for knowledge preparation and developing specification, those steps were necessary to place dealing knowledge into a usable kind for process is achieved by inspecting the pc to scan knowledge from a written or written document or it will occur by having individuals keying the info directly into the system. The look of input focuses on dominant the quantity of input needed, dominant the errors, avoiding delay, avoiding additional steps and keeping the method straightforward. The input is intended in such the simplest method so it provides security and simple use with holding the privacy. Input style thought-about the subsequent things:

- What information ought to be as input?
- How the info ought to be organized or coded?
- The dialog to guide the in operation personnel in providing input.
- Methods for getting ready input validations and steps to follow once error occur.

V. OBJECTIVES

Input vogue is that the strategy of adjusting a user-oriented description of the input into a computer-based system. This vogue is extremely vital to avoid errors among the {data} input methodology and show the proper direction to the management for getting correct data from the processed system.

It is achieved by making easy screens for the info entry to handle giant volume of knowledge. The goal of coming up with input is to create information entry easier and to be free from errors. The info entry screen is intended in such the simplest way that each one the info manipulates is often performed. It conjointly provides record viewing facilities.

When the knowledge is entered it will check for its validity. Data is also entered with the help of screens. Acceptable messages square measure provided as once needed that the user will not be in maize of instant. thus the target of input vogue is to make associate degree input layout that is easy to follow

VI. OUTPUT DESIGN

A quality output is one that meets the wants of the top user and presents the knowledge clearly. In any system results of process square measure communicated to the users and to alternative system through outputs. In output style it's determined however the knowledge is to be displaced for immediate would like and conjointly the text output. It’s the foremost necessary and direct supply data to the user. Economical and intelligent output style improves the system’s relationship to assist user decision-making. Designing pc output ought to proceed in AN organized, well thought out manner; the correct output should be developed whereas guaranteeing that every output component is intended in order that folks can notice the system will use simply and effectively. Once analysis style pc output, they ought to establish the precise output that's required to satisfy the wants.

- Select ways for presenting data.
- Produce document, report, or different formats that contain data created by the system.
- The output sort of Associate in nursing data system ought to accomplish one or a lot of the subsequent objectives:
- Convey data concerning past activities, current standing or projections of the
- Future.
- Signal necessary events, opportunities, problems, or warnings.
- Trigger Associate in nursing action.
- Confirm Associate in nursing action.

VII. MODULES

Giving access Privileges : Access privileges are given to various users based on their roles. Privileges are nothing but the rights given to the users based on their roles. They have limited access according to their roles. So to protect the privilege control a semi anonymous scheme called Anonycontrol is used.

n – Attribute based encryption: Based on their roles the user will encrypt the data and shares it. If he wants to send data then the particular data to be sent are encrypted but not the public one. This is done by using n- attribute based encryption.

Public and private data access: By using a semi-anonymous privilege control scheme AnonyControl which addresses not solely the info privacy, however additionally the user identity privacy in existing access management schemes. AnonyControl de-centralizes the central authority to limit the identity discharge and so achieves semi-anonymity. Besides, it additionally generalizes the file access management to the privilege management, by that privileges of all operations on the cloud knowledge will be managed during a fine-grained manner. Additionally AnonyControl-F, that absolutely prevents the identity leakage and to attain the total namelessness is additionally used.

User Revocation: During user revocation the privileges given to the user based on their role will be removed. If the privileges are not removed properly then the user will be able to access the data even after revocation. In this project privileges rights are maintained even after user revocation.

VIII. PERFORMANCE EVALUATION

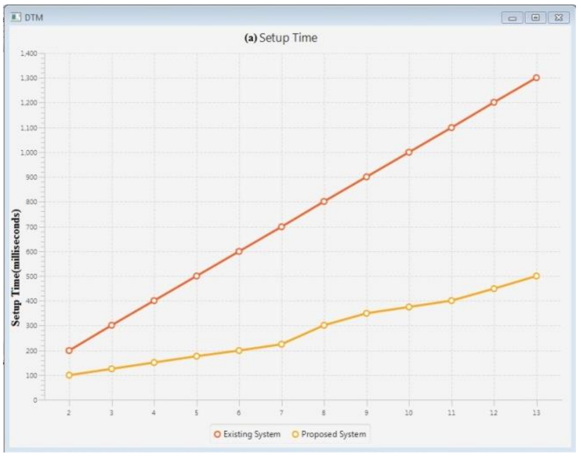

Fig. (a) Setup Time

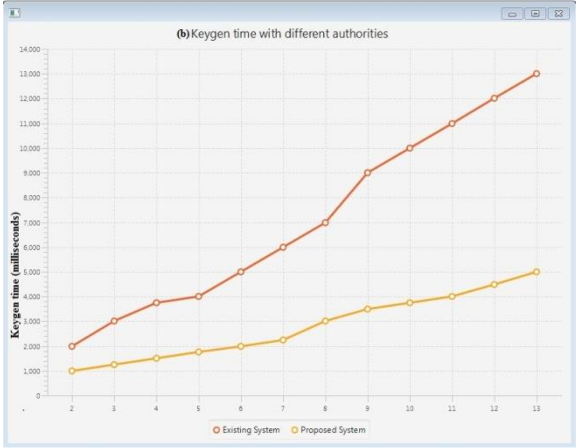

Fig. (b) Keygen time with different authorities

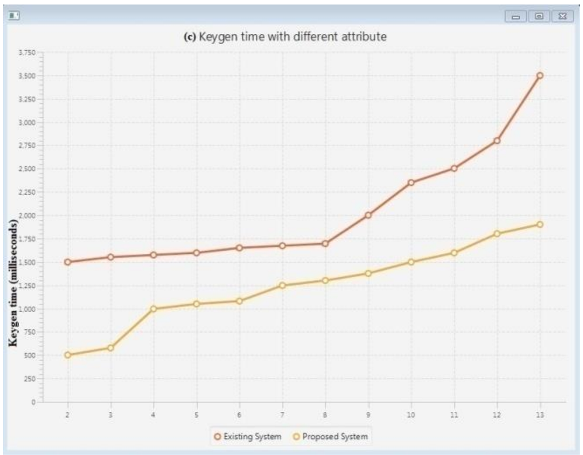

Fig. (c) Keygen time with different attribute

IX. CONCLUSION

Now we currently were using this mechanism in small data in cloud computing. Different encryption scheme like IBE, ABE, KP-ABE, CP-ABE, Anonycontrol and AnonyControl-F is mentioned with their advantage and disadvantage. The different variation of this scheme are compared and discussed with the existing scheme according to the rise in the security issues in cloud computing. The comparisons and study of those encryption scheme are done according to the problems arises and the solution on those the problem are mentioned. Direction for future work is to allow multi authority servers to update user secret key without disclosing user attribute information. Also in AnonyControl system we worked with multi authority system, so it will be interesting to work with load balancing techniques to handle overhead. The system has been developed keeping in mind all the requirements of the client Although the system is developed with the embody it is workable that it might not able to provide with all the facilities Hence it is always requisite to improve the system and provide with facilities as when the user requires it .one of the promising future works is to present the efficient user revocation mechanism on top of our anonymous ABE. In future we will pass huge amount of data in Hadoop environment.

Reference

[1] F. Li, Y. Rahulamathavan, M. Rajarajan, and R. C.-W. Phan, “Low Complexity multi-authority attribute based encryption scheme for mobile Cloud computing,” in *Proc. IEEE 7th SOSE*, Mar. 2013, pp. 573–577.

[2] K. Yang, X. Jia, K. Ren, and B. Zhang, “DAC-MACS: Effective data Access control for multi-authority cloud storage systems,” in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2895–2903.

[3] H. Ma, G. Zeng, Z. Wang, and J. Xu, “Fully secure multi-authority Attribute-based traitor tracing,” *J. Comput. Inf. Syst.*, vol. 9, no. 7, pp. 2793–2800, 2013.

[4] T. Jung, X. Mao, X.-Y. Li, S.-J. Tang, W. Gong, and L. Zhang, “Privacypreserving Data aggregation without secure channel: Multivariate polynomial Evaluation,” in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2634–2642.

[5] L. Zhang, X.-Y. Li, Y. Liu, and T. Jung, “Verifiable private multiparty computation: Ranging and ranking,” in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 605–609.

[6] *Ciphertext-Policy Attribute-Based Encryption Toolkit*. [Online]. Available: http://acsc.csl.sri.com/cpabe/, accessed 2014.

[7] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, “Scalable and secure Sharing of personal health records in cloud computing using attribute based Encryption,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[8] S. Hohenberger and B. Waters, “Attribute-based encryption with Fast decryption,” in *Public-Key Cryptography*. Berlin, Germany: Springer-Verlag, 2013, pp. 162–179.

[9] J. Hur, “Attribute-based secure data sharing with hidden policies in smart Grid,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 11, pp. 2171–2180, Nov. 2013.

[10] Y. Zhang, X. Chen, J. Li, D. S. Wong, and H. Li, “Anonymous attributebased Encryption supporting efficient decryption test,” in *Proc. 8th ASIACCS*, 2013, pp. 511–516.

[11] X.-Y. Li and T. Jung, “Search me if you can: Privacy-preserving location Query service,” in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2760–2768.

[12] *Tor: Anonymized Network*. [Online]. Available: https://www.torproject.org/, accessed 2014.

[13] W. Ren, K. Ren, W. Lou, and Y. Zhang, “Efficient user revocation for Privacy-aware PKI,” in *Proc. ICST*, 2008, Art. ID 11.

[14] M. Chase and S. S. M. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in Proc. 16th CCS, 2009, pp. 121–130.

[15] H. Lin, Z. Cao, X. Liang, and J. Shao, “Secure threshold multi authority attribute based encryption without a central authority,” Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.

[16] V. Božovi´c, D. Socek, R. Steinwandt, and V. I. Villányi, “Multi-authority attribute-based encryption with honest-but-curious central authority,” Int. J. Comput. Math., vol. 89, no. 3, pp. 268–283, 2012.

[17] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2011, pp. 568–588.

[18] S. Müller, S. Katzenbeisser, and C. Eckert, “On multi-authority cipher text-policy attribute-based encryption,” Bull. Korean Math. Soc., vol. 46, no. 4, pp. 803–819, 2009.

[19] J. Li, Q. Huang, X. Chen, S. S. Chow, D. S. Wong, and D. Xie, “Multiauthority cipher text-policy attribute-based encryption with accountability,” In Proc. 6th ASIACCS, 2011, pp. 386–390.

[20] S. Yu, K. Ren, and W. Lou, “Attribute-based content distribution with hidden policy,” in Proc. 4th Workshop Secure Netw. Protocols, Oct. 2008, pp. 39–44.