International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Two Factor Access Control for Dynamic Group in the Cloud Environment

Deokate Rakhi N.[1], S. V. Todkari[2]

[1]Department of Computer Engineering, JSPM Hadapsar, Pune

[2]Professor, Department of Computer Engineering, JSPM Hadapser, Pune

Abstract: ***As cloud computing share resources over the network, security is the basic concern. Data owners store their data on external servers so data confidentiality, authentication, access control are some of the basic issue in cloud environment. To protect user's privacy traditional method use for authentication username and password. But this security mechanism is not secure at all the proposed method i.e. identification of user's are using an two factor authentication mechanism for cloud access gives better security than the traditional one. In this proposed methodology, an efficient access mechanism using capability list is introduced. . An important feature of cloud storage is data sharing. Sharing along with strong protection of data is the main aspect.***

Keywords: access control, authentication, confidentiality

1. Introduction

Cloud computing is an emerging technology with lower price, shared resources and rely based on the consumer demand. Due to numerous characteristics, it has effect on IT budget as well as impact on security, privacy, and security problems. All those CSPs who wish to enjoy this new tendency should take good care of the problems. Customer not understand where the information is stored, who handle other vulnerabilities that can occur and information. Following are a few problems which can be confronted by CSP while executing cloud services. Cloud computing is technology that allows user to access software application, store information, develop and test new software, create virtual server, draw on disparate IT resources, and more all over the internet.

Cloud computing is model driven methodology that provides configurable computing resources such as server, network, storage, and application as and when required with minimum efforts over the internet services. Cloud also indicates essential characteristics, delivery model, and deployment model. Cloud are need data center but the aim of cloud computing is to eliminate the need to think about data center. A data center is a facility used to house computer system and associated component such as telecommunication and storage system. It includes redundant backup power supplies, redundant data communication connections, environmental control (e.g. air conditioning, fire suppression), and security devices. Data center are tied to locality with specific component including redundant power supplies, redundant

communication, environment control, security devices, etc. Cloud are location-independent, providing abstracted version of data center component that are not tied to a specific data center: virtual server, virtual storage, virtual networking, etc. Reliability and redundancy comes from cloud provider using multiple data center, so cloud almost certainly span one or more data center, but themselves are not data center.
Cloud computing is a vast concept. Many of the algorithms for load balancing in cloud computing have been proposed. Some of those algorithms have been overviewed in this thesis. The whole Internet can be considered as a cloud of many connections less and connection oriented services. So the divisible load scheduling theory for wireless networks described in [9] can also be applied for clouds. The performance of various algorithms have been studied and compared. Cloud computing is emerging as a new paradigm of large-scale distributed computing. It has moved computing and data away from desktop and portable PCs, into large data centers. As a part of its services it provides flexible and easy way to keep and retrieve data and files especially for making large data sets and files available for the spreading no. of users around the world. Cloud computing provides the different types of services that are based in pay-as-go model. User can take services on cloud ranging from web application to scientific application. These services are delivered to the customer over the internet.

2. Review of Literature

D. Boneh [3] suggest in his system protocol that, first multi-server password system which splits your password on different machines. They are using public kay to perform this operation. Improvement in current franklins and boneh work published in D. Boneh, [3]. There is a problem whicle using Diffe-Hellman. After this P. Mackenzie, V. Boyko, and S. Patel protocol made some work in this area. They used identity based encryption also the Weil Pairing and latter presented two threshold protocol. These protocols are theoretically good. In this system, multi-server password systems, either the servers are equally exposed to the users or a user should communicate in parallel with several or all servers for authentication. You can introduce gateways also Recently, Brained projected a password system in which one server disclosures itself to users and the other is hidden from all. It is very interesting to setup these kinds of system. These both servers should have their own keys then it will be very easy to communicate between user and servers. Due to this reason, there is no fun in existing authentication mechanism.

[3]. R. D. Pietro G. Ateniese, [6] decorum only makes one-sided authentication and completely depend on Secure Socket Layer to create a session between server resides at front end and user on network. Yang suggest solution on this problem, He said that we can focus on backend server. Accomplishing safe role-based entree on scrambled data in cloud storage in that, A system for grasping multifaceted entre control on encrypted data that system call Cipher Text Policy Attribute-Based Encryption. Using this method, we can secure our data and make confidential to it. We are safe from collusion attack. Role based access control is not that much secure in current situations. [14].

Secure multi possessor data sending receiving for groups who are dynamic in nature. In this author propose a fully functional identity-based encryption scheme (IBE). They are taking security in random security model due to problem of diffie Hellman. Our scheme is built on bilinear maps between different cloud groups. Weil pairing is very important example of this. It bounces specific explanations for safe uniqueness based encryption schemes. There are lot applications of this system. This scheme should be secure counter to conspiracies of operators, explicitly, given secret keys for polynomials many founds. No one can learn about message. Our building is safe below the typical learning with errors (LWE) hypothesis. Previous buildings of attribute-based encryption were for Boolean formulas which captured by the difficulty class NC 1. During our building, present a new framework for making ABE schemes. [12].

Secure multi owner data sharing for dynamic groups in the cloud in that, propose a fully functional identity-based encryption scheme (IBE). The scheme has chosen cipher text security in the random oracle model supposing a variant of the computational Diffie Hellman problem. Our method is based on bilinear maps between groups. The Weil pairing on elliptic curves is an example of such a map. It gives precise meanings for secure identity based encryption patterns and give several applications for such systems. In an attribute-based encryption (ABE) scheme, a cipher text is associated with an ’-bit public index find and a message m, and a secret key is associated with a Boolean predicate P. The secret key allows to decrypt the cyphertext and learn m iP(ind)Moreover, the scheme should be secure against collusions of users, namely, given secret keys for polynomials many predicates, an adversary learns nothing about the message if none of the secret keys can individually decrypt the cipher text.[10] Fully collusion secure dynamic broadcast encryption with constant-size cipher texts or decryption keys in that, attribute-based encryption access control schemes for circuits of any arbitrary polynomial size, where the public parameters and the cyphertexts grow linearly with the depth of the circuit. Our construction is secure below the regular learning with errors (LWE) assumption. Previous constructions of attribute-based encryption were for Boolean formulas, captured by the complexity class NC1. During our construction, present a new framework for constructing ABE schemes. As a by-product of our framework, obtain ABE schemes for polynomial-size branching programs, corresponding to the complexity class LOGSPACE, under quantitatively better assumptions [12].

3. System Architecture / System Overview

Cloud computing, with the characteristics of intrinsic data sharing and low maintenance, provides a better utilization of resources. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers. However, security concerns become the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud [2]. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud.

In this system, data owner, authorised user, thrusted third party and cloud server. in cloud server lot data are saved. It is very flexible .in cloud, data sharing is importent term.when we upload file these file store on server. Modification of multiuser data, public auditing, probability for high error detection, effective user revocation and computational auditing performance can be characterized by a novel integrity auditing approach for data storage and sharing services. Attack of imitation can be avoid by given scheme. An important feature of cloud storage is data sharing. Sharing along with strong protection of data is the main aspect. Cryptography helps data owner to store data safely on cloud. While considering data privacy, we cannot rely upon traditional technique of authentication, because unexpected privilege escalation will expose all data. Solution is to encrypt data before uploading to the server with uploader’s own key. Data sharing is again important functionality of cloud storage, because user can share data from anywhere and anytime and to anyone. First the admin saves file in the cloud space so that it will be available to users at any time. So he will generate a public key, which is used to encrypt the file. Then he chooses the file to upload and it is encrypted using public key. After encryption the file is uploaded to the cloud space. IP generate hash code of each file which is get uploaded by the data owner. When the user needs to access the file, the admin will share the file details with the user. The generated key sent via secure Email to the user. When the user gets the Email from the admin, he will get the file details. He can now enter the file name and key to download it, in his system. After downloading the decryption is carried out with key. Then the file is saved in the predefined folder in the client system.

Unathorised access prevented by giving few preventive measures such as role based access, attack detection and preventions such as if unathorised user trying to access data files then those are identified and user gets blocked and he/she will not be log in to the system. The elimination of the costly certificate verification process makes it scalable and especially suitable for big data analytic environment.

Method

Two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device.

4. System Analysis

Cloud computing, with the features of inherent data allotment and low preservation cost, provides a better use of resources. In cloud computing, cloud service providers offer an abstraction of immeasurable storing space for customers to place data. It can support customers decrease their economic upstairs of data managements by drifting the local managements system into cloud servers. Though, safety worries develop the main constraint as we now subcontract the storing of data, which is probably complex, to cloud providers. To prevent data privacy, a communal method is to encrypt data files before the clients upload the encoded data into the cloud [2]. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. Thats why we have proposed this scheme.

Applications

Applications like File sharing, video uploading, Email and voice conferencing are using cloud to store their data economic beneficially. These are also called as collaborations applications. business applications who are based on cloud provide tremendous opportunities to business companies to only that much they are using. This is also called The Pay as You Go plan. Since businesses not worried to take the software, they have access to the latest solutions which ready in low cost. The handiness of solutions such as Customer relationship management, Human Resource, Enterprise Resource Planning Finance, and Accounting on cloud based data servers. So, that we can save upfront investment. The web servers, organization tools, diagnostic and commercial software are moving to cloud computing. Cloud based web structure and software will save your currency. Enterprises establishments are already benefiting by the low price. We can also improve office employee performance by taking very fast updates of work

4.1 Expected Result

After implementing some part of system we got system performance on satisfactory level. The below table shows the algorithm performance for user plain data conversion as well encryption decryption.

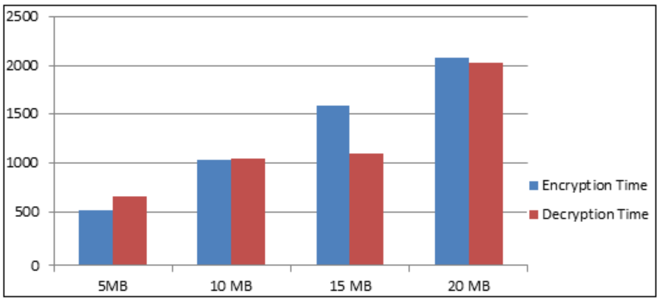

Figure 1: Performance measure

4.2 Table

Table 1: show that encryption time and decryption time in millisecond

Data Size in MB	Encryption Time (Milliseconds)	Decryption Time (Milliseconds)
5	515	612
10	1028	1033
15	1558	1066
20	2054	2023

5. Conclusion

In this given research work, weve projected a cloud-based storage scheme which provisions subcontracting of data that was dynamic, where the owner can elevate and scale and getting the information saved by the Cloud Service Provider, but also archiving this data on the isolated servers. Also, in the occurrence of dispute concerning information truthfulness, a TTP can decide on the party that is lying. The info proprietor smears entree control for the data that is subcontracted. Our two factor access control mechanism is efficient than others.

References

[1] Zhongma zhu and rui jiang, ”A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud” IEEE Trans. on parallel and distributed system, vol.27 no.1,jan 2016.

[2] 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, no. 4, pp. 50-58, Apr. 2010.

[3] S. Kamara and K. Lauter, ”Cryptographic cloud storage,” in Proc. Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136-149.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, ”Plutus: Scalable secure file sharing on untrusted storage,” in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29-42.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, ”Sirius: Securing remote untrusted storage,” in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131-145.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ”Improved proxy re-encryption schemes with applications to secure distributed storage,” in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 29-43.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, ”Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282-292.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ”Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89-98.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, ”Secure provenance: The essential of bread and butter of data forensics in cloud computing,” in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282-292.

[10] B. Waters, ”Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53-70.

[11] X. Liu, Y. Zhang, B. Wang, and J. Yang, ”Mona: Secure multiowner data sharing for dynamic groups in the cloud,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182-1191, Jun. 2013.

[12] v D. Boneh, X. Boyen, and E. Goh, ”Hierarchical identity based encryption with constant size ciphertext,” in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 440-456.

[13] C. Delerablee, P. Paillier, and D. Pointcheval, ”Fully collusion secure dynamic broadcast encryption with constant-size Ci-phertexts or decryption keys,” in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 39-59.

[14] Z. Zhu, Z. Jiang, and R. Jiang, ”The attack on mona: Secure multiowner data sharing for dynamic groups in the cloud,” in Proc. Int. Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185-189.

[15] L. Zhou, V. Varadharajan, and M. Hitchens, ”Achieving secure rolebased access control on encrypted data in cloud storage,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947-1960, Dec. 2013.

[16] X. Zou, Y.-S. Dai, and E. Bertino, ”A practical and flexible key management mechanism for trusted collaborative computing,” in Proc. IEEE Conf. Comput. Commun., 2008, pp. 1211-1219.

[17] M. Nabeel, N. Shang, and E. Bertino, ”Privacy preserving policy based content sharing in public clouds,” IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 2602-2614, Nov. 2013.

[18] D. Dolev and A. C. Yao, ”On the security of public key protocols,” IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 198-208, Mar. 1983.

[19] B. Dan and F. Matt, ”Identity-based encryption from the weil pairing,” in Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol., 2001, vol. 2139, pp. 213-229.

[20] B. Den Boer, ”Diffie-Hellman is as strong as discrete log for certain primes,” in Proc. Adv. Cryptol., 1988, p. 530.

[21] D. Boneh, X. Boyen, and H. Shacham, ”Short group signature,” in Proc. Int. Cryptology Conf. Adv. Cryptology, 2004, pp. 41-55.

[22] D. Boneh, X. Boyen, and E. Goh, ”Hierarchical identity based encryption with constant size ciphertext,” in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 440-456.