Volume No:2, Issue No:9 (February-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Performance of Cloud-Based Data Protection Using Principle of a Hybrid Circuit

S.Kavya
M.Tech Software Engineering,
Information Technology,
Christu Jyoti Institute of Technology and Science.

G.Rama Rao
Associate Professor,
Information Technology,
Christu Jyoti Institute of Technology and Science.

ABSTRACT:
Keeping confidential data to the cloud and access control, data owners accept their standards-based encryption to encrypt stored data can. Users with limited computing power, however, mask the decryption server cloud computing to reduce the cost of operations is likely to be more representative. Consequently, the representatives of encryption laws based properties. However, last question, and the remaining tasks related to security. For example, a representative, and for damages for the cloud server computing results with malicious intent or a cipher instead of hands to answer a fake. They deserve to be able to trick the user cost savings, they answer unworthy purposes. Furthermore, when encoding, it is not enough and flexible access policies can be. Access control circuit common policy, representatives circuit ciphertext- hybrid encryption policy based on the properties of our work was to test a form that can be obtained is considered. In such a system, verifiable measurement systems collect and encrypt-then-MAC, data privacy, access control, computing results and at the same time guarantee the precision of a fine and representative. Secondly, our program is under the impression that a multilinear Hellman decision as protection against attacks from the selected text. Moreover, the proposed solution is a comprehensive campaign to demonstrate the ability to copy and processing was done.

INTRODUCTION:
The number of servers needed to handle user data and can be used to calculate. Medical images and medical records, health care institutions to reduce the amount of data and data storage costs increasingly large amounts of cloud-based medical association. There are two types of encryption are based on complementary characteristics. Can be expensive. General admission control policy circuits are used to express the strong form. K multilinear- Hellman proposed the notion that has been shown to be safe on the resolution.

On the other hand, we have the whole program. Abe will be guaranteed basic civil construction and maintenance of traditional access control system because I would imagine.

SYSTEM PRELIMINARIES:
ATTRIBUTE AUTHORITY:
Well, that user will be prompted to provide. Each user is allowed to remain in the mail is important to have the right to request to. There are two types of encryption are based on complementary characteristics. A major policy-based encryption features (KP Abbey), and policy-based encryption ciphertext- (CPABE) the other characteristics. Abe has limited use of the system and the practical application of the system of decision-making and greater reliability is one encipherer distributor.

CLOUD SERVER:
Furthermore cloud server data files for user data, and provide access to the text related files are uploaded to the server are required to decrypt the data is required to decrypt . Provide the customer has been successfully decrypted file

DATA OWNER:
Book early to get access to the data owner's profile. The owner of the encrypted file to the server to upload data to the cloud. Random encryption key generation went a file is uploaded to the cloud. The encrypted file is stored in the cloud.

DATA CONSUMER:
Data consumer will initially ask for the key to the Authority to verify and decrypt the file in the cloud. Data consumer can access the file based on the key received from mail id. As per the key received the consumer can verify and decrypt the data from the cloud.

Volume No:2, Issue No:9 (February-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

RELATED WORK:

Attribute-based encryption. Sahai and water quality-based encryption (ABE) proposed the notion. Many of the manifestations of this problem they can complete the following activities and policies focused. Up until recently, a typical round of aid and water KPABE being felt. In fact, there are still two problems. First, a normal circuit, which is not the idea that the traditional access control CPABE. Other activity, with respect to the circuit Abbey is a bit encryption. So, this is clearly an important issue for the design of the project still remains an effective open circuit C. Abbey. Hybrid encryption. Kramer and Shoup encryption hybrid public KEM arbitrary length / can encrypt a message of democratic construction is proposed. Based on the original work, a long-time Democratic symmetric encryption, MAC, KEM / hybrid model to make. The use of such a model has been modified to achieve high security. Representatives verify the authenticity of the Abbey. Since the introduction of the Abbey, there are several development directions.

Application outsourcing is an important way of counting. And Al Green. When outsourcing decryption decryption program is designed to reduce the cost of the counting Abbey. Later, Li and Al. The proposed definition is canceled check outsource Abbey encryption. They try to use the original password to guarantee the right to make a commitment. However, without any assurance from the owner of the data to create value for their secret identity, and then choose a dedicated server, the message might be unreliable. Then there is the risk of changes in the ciphertext message. Additionally, ciphertext message is just enough to change the relevant responsibilities. He / she will cheat users to answer terminator is not allowed to access data in the cloud server to permit would not be fair.

CONCLUSION:

The best of our knowledge, we conducted the first round of the delegation presented a hybrid encryption scheme based on the principle characteristics is ciphertext-. General admission control policy circuits are used to express the strong form. Based on the number and characteristics of our ciphertextpolicy see encrypt and Mac hybrid encryption mechanism to verify the authenticity, we checked decryption server part of the system is the transition to the cloud. Furthermore, the assumption that the resolution has been shown to be safe on the proposed K multilinear- Hellman.

On the other hand, we have the whole program. Counting the cost of using cloud computing and communication plan is the practical one. So, we have representative data privacy in the cloud and checked thoroughly, to ensure you can apply access control.

REFERENCES:

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, ”Above the Clouds: A Berkeley View of Cloud Computing,” University of California, Berkeley, Technical Report, no. UCB/EECS-2009-28, 2009.

[2] M. Green, S. Hohenberger and B. Waters, ”Outsourcing the Decryption of ABE Ciphertexts,” in Proc. USENIX Security Symp., San Francisco, CA, USA, 2011.

[3] J. Lai, R. H. Deng, C. Guan and J. Weng, ”Attribute-Based Encryption with Verifiable Outsourced Decryption,” in Proc. IEEE Transactions on information forensics and security, vol. 8, NO. 8, pp.1343-1354, 2013.

[4] A. Lewko and B. Waters, ”Decentralizing Attribute-Based Encryption,” in Proc. EUROCRYPT, pp.568-588, Springer-Verlag Berlin, Heidelberg, 2011.

[5] B. Waters, ”Ciphertext-Policy Attribute-Based Encryption: an Expressive, Enficient, and Provably Secure Realization,” in Proc. PKC, pp.53-70, Springer-Verlag Berlin, Heidelberg, 2011.

[6] B. Parno, M. Raykova and V. Vaikuntanathan, ”How to Delegate and Verify in Public: verifiable computation from attribute-based encryption,” in Proc. TCC, pp.422-439, Springer-Verlag Berlin, Heidelberg, 2012.

[7] S. Yamada, N. Attrapadung and B. Santoso, ”Verifiable Predicate Encryption and Applications to CCA Security and Anonymous Predicate Authentication,” in Proc. PKC, pp.243-261, Springer-Verlag Berlin, Heidelberg, 2012.

[8] J. Han, W. Susilo, Y. Mu and J. Yan, ”Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption,” in Proc. IEEE Transactions on Parallel and Distributed Systems, 2012.

Volume No:2, Issue No:9 (February-2017)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

[9] S. Garg, C. Gentry, S. Halevi, A. Sahai and B. Waters, "Attribute-Based Encryption for Circuits from Multilinear Maps," in Proc. CRYPTO, pp.479-499, Springer-Verlag Berlin, Heidelberg, 2013.

[10] S. Gorbunov, V. Vaikuntanathan and H. Wee, "Attribute-Based Encryption for Circuits," in Proc. STOC, pp.545-554, ACM New York, NY, USA, 2013.

[11] A. Sahai and B. Waters, "Fuzzy Identity Based Encryption," in Proc. EUROCRYPT, pp.457-473, Springer-Verlag Berlin, Heidelberg, 2005.

[12] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based Encryption for Fine-grained access control of encrypted data," in Proc. CCS, pp.89-98, ACM New York, NY, USA, 2006.

[13] R. Cramer and V. Shoup, "A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack," in Proc. CRYPTO, pp.13-25, Springer-Verlag Berlin, Heidelberg, 1998.

[14] R. Cramer and V. Shoup, "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack," in Proc. SIAM Journal on Computing, vol. 33, NO. 1, pp.167-226, 2004.

[15] D. Hofheinz and E. Kiltz R, "Secure hybrid encryption from weakened key encapsulation," in Proc. CRYPTO, pp.553-571, Springer-Verlag Berlin, Heidelberg, 2007.

[16] M. Abe, R. Gennaro and K. Kurosawa, "Tag-KEM/DEM:A New Framework for Hybrid Encryption," in Proc. CRYPTO, pp.97-130, Springer-Verlag New York, NJ, USA, 2008.

[17] K. Kurosawa and Y. Desmedt, "A New Paradigm of Hybrid Encryption Scheme," in Proc. CRYPTO, pp.426-442, Springer-Verlag Berlin, Heidelberg, 2004.

[18] J. Li, X. Huang, J. Li, X. Chen and Y. Xiang, "Securely Outsourcing Attribute-based Encryption with Checkability," in Proc. IEEE Transactions on Parallel and Distributed Systems, 2013.

[19] J. Hur and D. K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," in Proc. IEEE Transactions on Parallel and Distributed Systems, 2011.

[20] T. Granlund and the GMP development team, "GNU MP: The GNU Multiple Precision Arithmetic Library, 5.1.1," 2013, http://gmplib.org/.