ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Circuit CP-ABE with Fine Grained Access Control and Verifiable Delegation in Cloud Computing

J. Venkata Ramana[1], M Venkatesh Naik[2]

M.Tech, Dept of CSE, CRIT College, Affiliated to JNTUA, AP, India[1]

Assistant Professor & HOD, Dept of CSE, CRIT College, Affiliated to JNTUA, AP, India[2]

ABSTRACT: With the growing status of cloud computing, firms and data owners begins to outsource their primary data to the general public cloud for decreased management price and ease of access. Encryption helps to shield user data confidentiality, it makes tricky to perform comfy undeniable textual content search over the encrypted data Attribute-Based Encryption (ABE) is a promising cryptographic primitive which significantly enhances the flexibility of entry manage mechanisms. There are two complementary types of attribute headquartered encryption. One is key-policy attribute-based encryption (KP-ABE) and the opposite is cipher text-policy attribute-based encryption (CPABE). In a KP-ABE process, the decision of access coverage is made by the important thing distributor instead of the encipherer, which limits the practicability and value for the system in useful functions. On the contrary, in a CP-ABE system, every cipher textual content is associated with an entry constitution, and each confidential secret is labeled with a collection of descriptive attributes.

A circuit ciphertext-policy attribute-founded hybrid encryption with verifiable delegation scheme is offered to precise the strongest type of access control coverage. Ciphertext policy attribute-founded hybrid encryption is built-in with verifiable computation and encrypt-then-mac mechanism to delegate the verifiable partial decryption paradigm to the cloud server.

KEYWORDS: Anomaly detection systems, Keyed Intrusion Detection System, Adversarial Learning, Feature Selection, Classifier Security, Evasion Attacks, machine learning.

I. INTRODUCTION

Cloud computing is the computing system which describes the mixture of logical entities like data, program that are available through web. Cloud computing supplies aid to the business purposes and functionality together with the utilization of pc program by way of supplying remote server which entry via the web. Consumer data is frequently saved in servers spread across the globe. Cloud computing makes it possible for person to use unique services which saves cash that users spend on applications. Knowledge homeowners and firms are inspired to outsourced more and more touchy knowledge into the cloud servers, similar to emails, private documents, movies and photos, enterprise finance data, govt records, and many others.

To furnish end - to - end data protection and privacy in the cloud, touchy knowledge needs to be encrypted earlier than outsourcing to protect information privateness. In cloud computing, strong information utilization is an extraordinarily elaborate project because of information encryption, also it should contain gigantic quantity of outsourced data files.

As functions move to cloud computing systems, ciphertext-policy attribute-based encryption (CP-ABE) and verifiable delegation (VD) are used to make certain the data confidentiality and the verifiability of delegation on dishonest cloud servers. There are two complementary forms of attribute-situated encryption. One is key-policy attribute-based encryption (KP-ABE) and the other is ciphertext-policy attribute-based encryption (CP-ABE). In a KP-ABE approach, the choice of entry coverage is made by means of the key distributor as an alternative of the enciphered, which limits

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

the practicability and usefulness for the process in realistic applications. On the opposite, in a CP-ABE method, each and every ciphertext is related to an entry constitution, and each and every private key's labeled with a set of descriptive attributes. A person is equipped to decrypt a ciphertext if the important thing's at-

tribute set satisfies the entry constitution related to a ciphertext. It appears, this approach is conceptually towards normal entry manage approaches. However, in a ABE approach, the access coverage for common circuits could be viewed because the strongest form of the coverage expression that circuits can specific any software of constant running time.

II. EXISTING SYSTEM

The servers might be used to manage and calculate countless information consistent with the user's needs. As applications move to cloud computing systems, ciphertext-policy attribute-based encryption (CP-ABE) and verifiable delegation (VD) are used to ensure the information confidentiality and the verifiability of delegation of dishonest cloud servers. The growing volumes of medical portraits and clinical records, the healthcare companies put a colossal amount of information in the cloud for lowering knowledge storage charges and assisting clinical cooperation. There are two complementary varieties of attribute established encryption. One is key-policy attribute- based encryption (KP-ABE) and the other is ciphertext-policy attribute-based encryption (CPABE).

The cloud server would tamper or replace the data owner's customary ciphertext for malicious attacks, and then reply a false converted ciphertext. The cloud server could cheat the approved consumer for rate saving. Although the servers might now not reply a correct converted ciphertext to an unauthorized user, he would cheat a licensed person who he/she is just not eligible.

In a KP-ABE approach, the selection of access coverage is made with the aid of the key distributor instead of the encipherer, which limits the practicability and usefulness for the system in useful purposes. On the opposite, in a CP-ABE system, each cipher textual content is related to an access structure, and each and every personal key is labeled with a set of descriptive attributes.
A circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme is presented to precise the strongest type of access control policy. Ciphertext policy attribute-based hybrid encryption is built-in with verifiable computation and encrypt-then-mac mechanism to delegate the verifiable partial decryption paradigm to the cloud server.

III. LITERATURE SURVEY

ATTRIBUTE BASED ENCRYPTION FOR FINE-GRAINED ACCESS CONTROL OF ENCRYPTED DATA:
As extra sensitive data is shared and stored on the web, there will be a need to encrypt data stored at these websites. One drawback is that it can be selectively shared only at a rough-grained level (i.e., giving a different party your exclusive key). We develop a new cryptosystem for fine-grained sharing of encrypted information that we call Key-policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with units of attributes and confidential keys are associated with entry constructions that control which ciphertexts a consumer is capable to decrypt. We display the applicability of our building to sharing of audit-log know-how and broadcast encryption. Our building helps delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE). It's the first decentralized ABE scheme with privacy-keeping founded on regular complexity assumptions.

A PRACTICAL PUBLIC KEY CRYPTOSYSTEM PROVABLY SECURE AGAINST CHOSEN CIPHERTEXT ATTACK:

his paper presents a novel framework for development of hybrid encryption schemes secure against chosen ciphertext assault. Our new framework yields new and extra effective CCA-secure schemes, and supplies insightful explanations about present schemes that don't match into the earlier frameworks. This could influence in finding future upgrades.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Furthermore, it enables immediate conversion from a category of threshold public-key encryption to a hybrid one without considerable overhead, which is not achievable within the previous strategies.

A NEW PARADIGM OF HYBIRD ENCRYPTION SCHEME:

In this paper, we show that a key encapsulation mechanism (KEM) does no longer need to be IND-CCA secure within the development of hybrid encryption schemes, as used to be earlier believed. That is, we present a extra efficient hybrid encryption scheme by way of making use of a KEM which is not always IND-CCA secure. However, our scheme is secure within the experience of IND-CCA below the DDH assumption in the common mannequin. This outcomes is additional generalized to universal two projective hash families.
Attribute-Bsed Encryption (ABE) is a promising cryptographic primitive which drastically enhances the flexibility of access control mechanisms. Due to the excessive expressiveness of ABE insurance policies, the computational complexities of ABE key-issuing and decryption have become prohibitively excessive. Despite that the prevailing Outsourced ABE solutions are able to dump some intensive computing duties to a 3rd get together, the verifiability of outcome again from the 1/3 occasion has yet to be addressed. Aiming at tackling the challenge above, we advise a brand new cozy Outsourced ABE procedure, which supports each secure outsourced key-issuing and decryption. Our new method offloads all entry coverage and attribute related operations in the key-issuing system or decryption to a Key Generation Service Provider and a Decryption Service Provider (DSP), respectively, leaving only a constant number of straightforward operations for the attribute authority and eligible customers to participate in the neighborhood. In addition, for the first time, we endorse an outsourced

ABE construction which presents examine capability of the outsourced computation results in an effective approach..

OUTSOURCING THE DECRYPTING OF ABE CIPHERTEXTS:

Attribute-Based Encryption (ABE) is a brand new imaginative and prescient for public key encryption that makes it possible for users to encrypt and decrypt messages headquartered on person attributes. For instance, a consumer can create a ciphertext that can be decrypted best with the aid of different users with attributes satisfying ("Faculty" OR ("PhD Student" AND "Quals Completed")). Given its expressiveness, ABE is currently being considered for a lot of cloud storage and computing functions. However, one of the predominant efficiency drawbacks of ABE is that the dimensions of the ciphertext and the time required to decrypt it grows with the complexity of the entry system. On this work, we recommend a brand new paradigm for ABE that mostly eliminates this overhead for users. Think that ABE ciphertexts are saved in the cloud. We show how a user can provide the cloud with a single transformation key that makes it possible for the cloud to translate any ABE ciphertext satisfied through that consumer's attributes right into a (steady-measurement) El Gamal-form ciphertext, without the cloud being ready to read any part of the consumer's messages. To exactly define and reveal the benefits of this procedure, we furnish new protection definitions for each CPA and replayable CCA safety with outsourcing, several new constructions, an implementation of our algorithms and designated performance measurements. In a traditional configuration, the consumer saves significantly on both bandwidth and decryption time, without growing the quantity of transmissions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

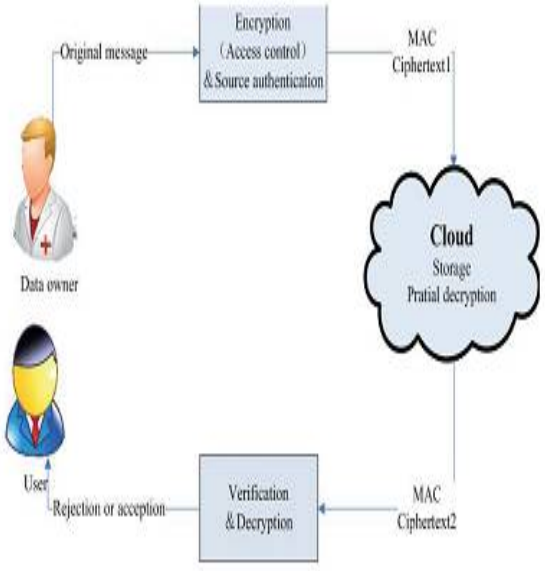
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

SYSTEM ARCHITECTURE



IV.PROPOSED WORK

Prompted by the requirements within the cloud, we change the mannequin of CP-ABE with verifiable delegation and present a concrete construction to realize circuit ciphertext-policy based hybrid encryption with verifiable delegation (VD-CPABE).

To keep data confidential and achieve first-class grain access control, our commencing factor is a circuit key-policy attribute-based encryption proposed with the aid of A. Sahai and Brent Waters. We supply the anti-collusion circuit CP-ABE construction on this paper considering CP-ABE is conceptually toward the average access control methods.

To validate the correctness, we lengthen the CP-ABE ciphertext into the attribute-based for two complementary policies and add a MAC for every ciphertext, so that whether or not the consumer has permissions he/she could receive a privately demonstrated key to verify the correctness of the delegation and preclude from counterfeiting of the ciphertext.
Bettering the efficiency and offering intuitive description of the protection proof, the thought of hybrid encryption is also presented on this work. Apart from, safety of the VD-CPABE method ensures that the untrusted cloud will not be ready to gain knowledge of anything in regards to the encrypted message and forge the common ciphertext. As a result, attribute-based encryption with delegation emerges.

Still, there are caveats and questions remaining within the prior important works. For example, in the course of the delegation, the cloud servers could tamper or substitute the delegated ciphertext and respond a cast computing result with malicious intent. They may additionally cheat the eligible customers by means of responding them that they're ineligible for the purpose of fee saving. Moreover, during the encryption, the entry insurance policies might not be flexible. For the reason that policy for common circuits allows to obtain the strongest type of access manage, a development for realizing circuit ciphertext-coverage attribute-founded hybrid encryption with verifiable delegation has been regarded in our work. In this type of procedure, combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control and the correctness of the delegated computing results are well guaranteed. The generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

V. IMPLEMENTATION

1. Attribute Authority:

Authority will have to offer the key, as per the consumer's key request. Every customers request can must be raised to authority to set off access key on mail. There are 2 complementary forms of attribute-headquartered secret writing. One is key-policy attribute-based Encryption (KP-ABE) and the alternative is ciphertext-policy attribute-based encryption (CPABE). In a KP-ABE approach, the selection of entry coverage is created by means of the key distributor instead than the encipherer, which limits the usefulness and usefulness for the system in sensible functions.

2. Cloud Server:

Cloud server may have the entry to documents that rectangular measure uploaded through the understanding proprietor Cloud server wishes to decipher the records offered underneath their permission.
In addition expertise user can must decipher the data to entry the preliminary text through offering the character key. File has been decrypted efficaciously and supplied for shopper.

3.Data owner:

Data owner can have to register initio to result in access to the profile. Data owner can transfer the file to the cloud server in the encrypted format. Random encryption key new release is going down whereas uploading the file to the cloud. Encrypted file will be hold on the cloud.

4. Data Consumer:

Data consumer may also be initio lift for the key to the Authority to verify and decipher the enter the cloud. Data consumer will access the file mainly established on the important thing received from mail identification. As per the key bought the customer will affirm and decipher the info from the cloud.

VI. CONCLUSION

A circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme is presented, circuits are used to state the secure type of access control policy. Certifiable computation and encrypt-then-mac mechanism are combined with ciphertext-policy attribute-based hybrid encryption and assign the verifiable partial decryption paradigm to the cloud server. The expenses of the computation and communique consumption show that the scheme is useful in the cloud computing. For that reason, it might be significant to make sure the data confidentiality.

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Parallel and Distributed Systems, 2012.
[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.