International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 2 – APRIL 2016.

A SECURE DELEGATION OF DATA ENCRYPTION USING K-MULTILINEAR DECISIONAL DIFFIE-HELLMAN ASSUMPTION IN CLOUD COMPUTING

B.Ambika[#1] G.Sangeetha[*2]

M.E. Scholar, Cse Dept.,Arm College Of Engineering And Technology, Marai Malai Nagar, Chennai.
Asst. Professor, Cse Dept., Arm College Of Engineering And Technology, Marai Malai Nagar,Chennai

ambika.senthil2008@gmail.com
sangeearya10@gmail.com

***Abstract*- In the cloud, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data. Users delegate the mask of the decryption task to the cloud servers to reduce the computing cost. As a result, attribute-based encryption with delegation emerges. Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could tamper or replace the delegated ciphertext and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work. In such a system, 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 at the same time. Besides, our scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.**

Index Term: **Cloud Computing, ABE, CP-ABE, KP-ABE, CIA, IBE, Cloud storage.**

I. INTRODUCTION

Cloud computing is the computing technique which describes the combination of logical entities like data, software which are accessible via internet. Cloud computing provides help to the business applications and functionality along with the usage of computer software by providing remote server which access through the internet. Client data is generally stored in servers spread across the globe. Cloud computing allows user to use different services which saves money that users spend on applications. Data owners and organizations are motivated to outsourced more and more sensitive information into the cloud servers, such as emails, personal documents, videos and photos, company finance data, government documents, etc.

To provide end - to - end data security and privacy in the cloud, sensitive data has to be encrypted before outsourcing to protect data privacy. In cloud computing, effective data utilization is a very difficult task because of data encryption, also it may contain large amount of outsourced data files.

As applications move to cloud computing platforms, ciphertext-policy attribute-based encryption (CP-ABE) and verifiable delegation (VD) are used to ensure the data confidentiality and the verifiability of delegation on dishonest cloud servers. There are two complementary forms of attribute-based 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 system, the decision of access policy is made by the key distributor instead of the enciphered, which limits the practicability and usability for the system in practical applications. On the contrary, in a CP-ABE system, each ciphertext is associated with an access structure, and each private key is labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if the key's at-tribute set satisfies the access structure associated with a ciphertext. Apparently, this system is conceptually closer to traditional access control methods. On the other hand, in a ABE system, the access policy for general circuits could be regarded as the strongest form of the policy expression that circuits can express any program of fixed running time.

Related Work. Using ABE, The cloud server might tamper or replace the data owner's original ciphertext for malicious attacks, and then respond a false transformed ciphertext. Improving the efficiency and providing intuitive description of the security proof, the conception of hybrid encryption is also introduced in this Attribute based encryption in the system.

Drawbacks

- There is no construction for realizing CP-ABE for general circuits, which is conceptually closer to traditional access control

- The other is related to the efficiency, since the exiting circuit ABE scheme is just a bit encryption one.

II. LITERATURE SURVEY

A: FUZZY IDENTITY BASED ENCRYPTION:

We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω ′, if and only if the identities ω and ω ′ are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term "attribute-based encryption". In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

B: ATTRIBUTE BASED ENCRYPTION FOR FINE-GRAINED ACCESS CONTROL OF ENCRYPTED DATA:

As more sensitive data is shared and stored on the Internet, there will be a need to encrypt data stored at these sites. One drawback is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE). It is the first decentralized ABE scheme with privacy-preserving based on standard complexity assumptions.

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

A new public key cryptosystem is proposed and analyzed. The scheme is quite practical, and is provably secure against adaptive chosen ciphertext attack under standard intractability assumptions. There appears to be no previous cryptosystem in the literature that enjoys both of these properties simultaneously.

This paper presents a novel framework for generic construction of hybrid encryption schemes secure against chosen ciphertext attack. Our new framework yields new and more efficient CCA-secure schemes, and provides insightful explanations about existing schemes that do not fit into the previous frameworks. This could result in finding future improvements. Moreover, it allows immediate conversion from a class of threshold public-key encryption to a hybrid one without considerable overhead, which is not possible in the previous approaches.

Finally we present an improved security proof of the Kurosawa-Desmedt scheme, which removes the original need for information-theoretic key derivation and message authentication functions. We show that the scheme can be instantiated with any computationally secure such functions, thus extending the applicability of their paradigm, and improving its efficiency.

D: A NEW PARADIGM OF HYBIRD ENCRYPTION SCHEME:

In this paper, we show that a key encapsulation mechanism (KEM) does not have to be IND-CCA secure in the construction of hybrid encryption schemes, as was previously believed. That is, we present a more efficient hybrid encryption scheme by using a KEM which is not necessarily IND-CCA secure. Nevertheless, our scheme is secure in the sense of IND-CCA under the DDH assumption in the standard model. This result is further generalized to universal2 projective hash families.

Attribute-Based Encryption (ABE) is a promising cryptographic primitive which significantly enhances the versatility of access control mechanisms. Due to the high expressiveness of ABE policies, the computational complexities of ABE key-issuing and decryption are getting prohibitively high. Despite that the existing Outsourced ABE solutions are able to offload some intensive computing tasks to a third party, the verifiability of results returned from the third party has yet to be addressed. Aiming at tackling the challenge above, we propose a new Secure Outsourced ABE system, which supports both secure outsourced key-issuing and decryption. Our new method offloads all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally. In addition, for the first time, we propose an outsourced

ABE construction which provides check ability of the outsourced computation results in an efficient way.

E: OUTSOURCING THE DECRYPTING OF ABE CIPHERTEXTS:

Attribute-based encryption (ABE) is a new vision for public key encryption that allows users to encrypt and decrypt

messages based on user attributes. For example, a user can create a ciphertext that can be decrypted only by other users with attributes satisfying ("Faculty" OR ("PhD Student" AND "Quals Completed")). Given its expressiveness, ABE is currently being considered for many cloud storage and computing applications. However, one of the main efficiency drawbacks of ABE is that the size of the ciphertext and the time required to decrypt it grows with the complexity of the access formula. In this work, we propose a new paradigm for ABE that largely eliminates this overhead for users. Suppose that ABE ciphertexts are stored in the cloud. We show how a user can provide the cloud with a single transformation key that allows the cloud to translate any ABE ciphertext satisfied by that user's attributes into a (constant-size) El Gamal-style ciphertext, without the cloud being able to read any part of the user's messages. To precisely define and demonstrate the advantages of this approach, we provide new security definitions for both CPA and replayable CCA security with outsourcing, several new constructions, an implementation of our algorithms and detailed performance measurements. In a typical configuration, the user saves significantly on both bandwidth and decryption time, without increasing the number of transmissions.

III. PROPOSED WORK

3.1 Problem Definitions

Prompted by the requirements in the cloud, we modify the model 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 private and achieve fine grain access control, our starting point is a circuit key-policy attribute-based encryption proposed by Sahai and Waters. We give the anti-collusion circuit CP-ABE construction in this paper for the reason that CP-ABE is conceptually closer to the traditional access control methods.

To validate the correctness, we extend the CP-ABE ciphertext into the attribute-based for two complementary policies and add a MAC for each ciphertext, so that whether the user has permissions he/she could obtain a privately verified key to verify the correctness of the delegation and prevent from counterfeiting of the ciphertext.

Improving the efficiency and providing intuitive description of the security proof, the conception of hybrid encryption is also introduced in this work. Besides, security of the VD-CPABE system ensures that the untrusted cloud will not be able to learn anything about the encrypted message and forge the original ciphertext. As a result, attribute-based encryption with delegation emerges.

Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could tamper or replace the delegated ciphertext and respond a forged computing result with malicious intent. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving.

Furthermore, during the encryption, the access policies may not be flexible. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work. In such a system, 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.

Advantages:

- Our proposed scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Diffie-Hellman assumption.
- An extensive simulation campaign confirms the feasibility and efficiency of the proposed solution. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation has been considered in our work.

A: ARCHITECTURAL DETAILS:

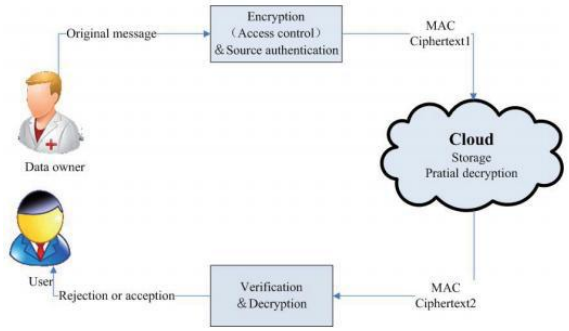

Fig 1: Architecture Diagram

An architecture diagram is the one which describes the overall view of this work. It is the pictorial representation of the entire work which is to be carried out. This architecture consists of four modules. It is the first part of system design. The main aim of the input design is covering user oriented descriptions of the input to the computer oriented form. All the inputs are converted into a computer based format. The goal of designing input data is to make data entry easier and free errors as possible.

IV. SYSTEM ANALYSIS

System analysis is defined as the process of gathering and interpreting facts, diagnosing problem and using the facts to improve the system. The objectives of the system analysis phase are the establishment of the requirements for the

system to be acquired, developed and installed. Fact finding or gathering is essential to any analysis of requirement. Information systems and information technology infrastructure has been integrated into business processes for more than two decades. A detailed study of the system is done by making use of various techniques. The conclusion is an understanding of how the system functions. This system is called existing system. Now, the existing system is subjected to close study and the problem areas are identified. The solutions are given as a proposal. The proposed system is presented to the user.

A. NOTATIONS:

- Zp - finite field with prime order p.
- ⊥ - formal symbol denotes termination.
- x ← X- x is randomly selected from X.
- A is an algorithm then A(x) → y denotes that y is
- the output by running the algorithm A on input x.

- G(λ, k)- group generation algorithm where λ is the
- security Parameter.
- k -the number of allowed pairing operation.
- ε: Zp → R- negligible if for every c > 0 there is a K such that ε(k) < k−c for all k > K.

B. ALGORITHMS

Following are few other algorithms which are used:

1) Setup(λ, n, l):
This algorithm is executed by the authority. It takes as input a security parameter λ, the number n of input size and the maximum depth l of a circuit. PK = (g_ k ,H1,H2,H3, y, h1,..., hn, hn+1, ..., h2n), MK = g_.

2) Hybrid-encrypt
(PK, f = (n, q, A,B, GateT ype), M ∈ {0, 1}m)): This algorithm is executed by the data owner. Taking the public parameters PK, a description f of a circuit and a message M ∈ {0, 1}m as input.

3) KeyGen(MK, x ∈ {0, 1}n):
The authority generates the private key for the user. Then the user sends his transformation key to the cloud server. This algorithm takes as input the master secret key and a description of the attribute x ∈ {0, 1}n. It firstly chooses a random t ∈ Zp. Then it creates the private key as KH = g_yt,

L = gt, if xi = 1 Ki = (yhi)t , if xi = 0 Ki = (yhn+i)t , i ∈ [1,n]. The transformation key is TK = {L,Ki, i ∈ [1, n]}.Note that, for the data owner IDo, the authority generates his private key with the identity attribute ID0 as KH = g_yt, L =gt, KIDo = Ht3 (IDo).

4) Transform(TK,CT):
The transformation algorithm is executed by the cloud server. It takes as input the transformation key TK and the original ciphertext CT.

The algorithm partially decrypts the ciphertext.

C: DESIGN GOALS

For effective utilization of outsourced data, our system should achieve security and performance guarantee as follows:
1) Secure keyword search:
To explore different mechanisms for designing effective keyword search schemes based on the existing searchable encryption framework.
2) Secure data sharing:
To allow user to share data over the cloud without losing privacy.
3) Security guarantee:
To prevent cloud server from learning the plaintext of either the data files or the searched keywords, and achieve the as strong- as- possible security strength compared to existing searchable encryption schemes.
4) Efficiency:
Above goals should be achieved with minimum communication and computation overhead.

V. EXPECTED RESULT

Our design should allow the user to verify the Correctness, Completeness, and Freshness of returned search results. The main idea behind our scheme is to let cloud server return the accurate search results according to requested search query.
Few other expected results are as follows.

- Encryption and decryption results: Data encryption and decryption is done by using verifiable delegation. Encrypted data is saved to the cloud. To access that data user will download it and decrypt it. Because of encryption high level of security is applied to the data.
- Search Results: This proposed system will give more accurate search results than available system. The accuracy of search results is improve because ranking of those results.
- Communication results: Secure and fast communication option is provided in the system. The communication cost is also reduced.

VI. CONCLUSION

To the best of our knowledge, we firstly present a circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation scheme. General circuits are used to express the strongest form of access control policy. Combined verifiable computation and encrypt-then-mac mechanism with our ciphertext-policy attribute-based hybrid encryption, we could delegate the verifiable partial decryption paradigm to

the cloud server. In addition, the proposed scheme is proven to be secure based on k -multilinear Decisional Diffie-Hellman assumption. On the other hand, we implement our scheme over the integers. The costs of the computation and communication consumption show that the scheme is practical in the cloud computing. Thus, we could apply it to ensure the data confidentiality, the fine-grained access control and the verifiable delegation in cloud.

REFERENCES

[1] [1] 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.

[2] [2] S. Garg, C. Gentry and S. Halevi, "Candidate mulitilinear maps from ideal lattices and applications", Proc. 32nd Annu. Int. Conf. Theory Appl. Cryptograph. Techn., pp. 1-17, 2013.

[3] [3] 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.

[4] [4] B. Parno, M. Raykova and V. Vaikuntanathan, "How to delegate and verify in public: Verifiable computation from attribute-based encryption", Proc. 9th Int. Conf. Theory Cryptograph., pp. 422-439, 2012.

[5] [5] 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.

[6] [6] 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.

[7] [7] A. Lewko and B. Waters, "Decentralizing Attribute- Based Encryption," in Proc. EUROCRYPT, pp.568- 588, Springer-Verlag Berlin, Heidelberg, 2011.

[8] [8] W. Nagao, Y. Manabe and Tatsuaki Okamoto, "A Universally Composable Secure Channel Based on the KEM-DEM Framework," in Proc. CRYPTO, pp.426-444, Springer-Verlag Berlin, Heidelberg, 2005.

[9] [9] A. Sahai and B. Waters, "Fuzzy identity based encryption", Proc. 30th Annu. Int. Conf. Theory Appl. Cryptograph. Techn., pp. 457-473, 2005