International Journal of Advanced Technology and Innovative Research

www.ijatir.org

ISSN 2348–2370
Vol.09,Issue.04,
March-2017,
Pages:0554-0557

A New Hybrid Encryption Algorithm with Diffie-Hellman Assumption in Cloud Computing

D. PAVAN KUMAR[1], DR. RAJEEV KUMAR[2]

[1]Ph.D Scholar, Dept of CSE, Shri Venkateswara University, Gajraula, UP, India.
[2]Assistant Professor, Dept of CSE, Shri Venkateswara University, Gajraula, UP, India.

Abstract: In the cloud, for achieving access management and keeping information confidential, the information the information house owners might adopt attribute -based encoding to encode the keep data. Users with restricted computing power are but a lot of possible to delegate the mask of the decoding task to the cloud servers to cut back the computing value. As a result, attribute -based encoding with delegation emerges. Still, there are caveats and queries remaining within the previous relevant works. as an example, throughout the delegation, the cloud servers might tamper or replace the delegated cipher text and respond a cast computing result with malicious intent. They will additionally cheat the eligible users by responding them that they're ineligible for the aim of value saving. What is more, throughout the encoding, the access policies might not be versatile enough likewise. Since policy for general circuits allows to realize the strongest variety of access management, a construction for realizing circuit ciphertext-policy attribute-based hybrid encoding with verifiable delegation has been thought of in our work. In such a system, combined with verifiable computation and encrypt then mac mechanism, the information confidentiality, the fine-grained access management and also the correctness of the delegated computing results are well bonded at identical time.

Keywords: Ciphertext-Policy Attribute-Based Encryption, Circuits, Verifiable Delegation, Multilinear Map, Hybrid Encryption.

I. INTRODUCTION

The emergence of cloud computing brings a revolutionary innovation to the management of the in fo resources. Inside this computing setting, the cloud servers can give numerous information services, like remote information storage and outsourced delegation computation, etc. For information storage, the servers store an oversized quantity of shared information, that may well be accessed by licensed users. For delegation computation, the servers may well be accustomed handle and calculate various information in step with the user's demands. As applications move to cloud computing platforms, cipher text -policy attribute-based encoding (CP -ABE)[1] and verifiable delegation (VD) area unit accustomed make sure the information confidentiality and also the verifiability of delegation on dishonest cloud servers. Information of knowledge of information} within the cloud for reducing data storage prices and supporting medical cooperation. Since the cloud server might not be credible, the file cryptological storage is an efficient methodology to forestall non-public information from being taken or tampered. within the in the meantime, they'll got to share information with the one who satisfies some necessities. the wants, i.e., access policy, may well be creating such information sharing be accomplishable, attribute-based encoding is applicable.

II. RELATED WORK

We concentrated on strategies diagonally manifold establishment and the problem of what terminologies could accomplish. In recent period, raised a structure for understanding KPABE for universal circuits. Previous to this technique, the well-built form of appearance is Boolean formulas in ABE systems, which is at rest a distant weep from being clever to articulate right of entry, manage in the form of any agenda or route. Essentially, in attendance at a standstill stay behind two harms. The primary one is their have no creation for realizing CPABE for universal circuits, which is theoretically closer to conventional entrée manage. The further is associated to the effectiveness, since the outlet circuit ABE scheme is immediately a small piece encryption one. Thus, it is actually still leftovers an essential unlock trouble to design a professional circuit CP-ABE scheme. Further proposed the basic KEM/DEM structure for hybrid encryption which preserve encrypt messages of random distance end to end. Based on their clever work, a one-time MAC was collective with symmetric encryption to expand the KEM/DEM representation for hybrid encryption[2].Such enhanced representation has the benefit of achieving superior refuge necessities ABE with Verifiable allocation.

Since the opening of ABE, there have been advances in manifold instructions. The submission of outsourcing calculation is one of a significant way. Then intended the first ABE through outsourced decryption scheme to decrease the calculation cost for the duration of decryption. After that, proposed the description of ABE with demonstrable outsourced decryption[3]. They request to assurance the precision of the unique cipher text by using a promise. However, while the data owner creates an assurance without any top secret value regarding his individuality, the hopeless server can then fake a assurance for a message he decides.

Thus the cipher text connecting to the message is at danger of being interfered[4]. In addition, just transform the assurances for the cipher text connecting to the message is not sufficient. The cloud server can mislead the user with appropriate agreements by react the terminator to trick that he/she is not permitted to right of entry to the data.

III. PRELIMINARY

A. Our Contribution

Existing system in every ciphertext is related to associate degree access structure, and every non -public secret is labeled with a group of descriptive attributes. A user is in a position to rewrite a ciphertext if the key's attribute set satisfies the access structure related to a ciphertext. CP - ABE below sure access policies. The users, UN agency wish to access the information files, select to not handle the complicated method of decoding domestically as a result of restricted resources. Instead, they're presumably to source a part of the decoding method to the cloud server. Whereas the untrusted cloud servers UN agency will translate the first ciphertext into a straightforward one may learn nothing concerning the plaintext from the delegation. Whereas the untrusted cloud servers UN agency will translate the first ciphertext into a straightforward one may learn nothing concerning the plaintext from the delegation.

B. Our Techniques

The increasing volumes of records place an outsized quantity information of knowledge of information within the cloud for reducing information storage prices and supporting data cooperation. Every cipher text is related to associate degree access structure and user is ready to decipher a cipher text, the storage service provided by the cloud server and therefore the outsourced information[5] mustn't be leaked even though malware or hackers infiltrate the server. User may validate whether or not the cloud server responds correct remodeled cipher text to assist him/her decipher cipher text straight off and properly

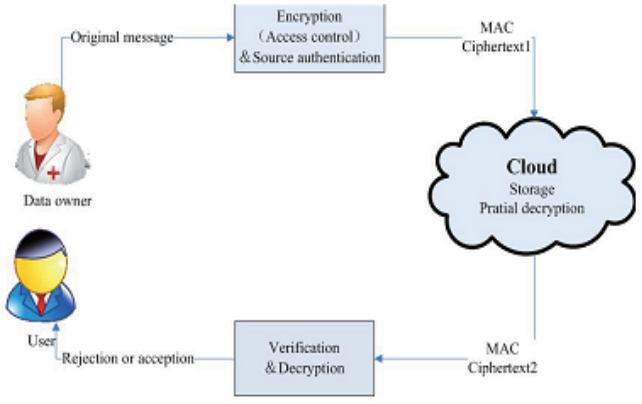

Fig1. System Architecture.

IV. LITERATURE SURVEY

A. Above the Clouds: A Berkeley View of Cloud Computing

Provided certain obstacles are overcome, we believe Cloud Computing has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new interactive Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get their results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT. The economies of scale of very large-scale datacenters combined with ``pay-as-you-go" resource usage has heralded the rise of Cloud Computing. or example, a user can create a cipher-text 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 cipher-text 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 cipher-texts 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 cipher-text satisfied by that user's attributes into a (constant-size) El Gamal-style cipher-text, 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.

B. Attribute-Based Encryption with Verifiable Outsourced Decryption.

Attribute-based encryption (ABE) is a public-key-based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and cipher-texts. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. Recently, Green et al. proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that allows the

cloud to translate any ABE cipher-text satisfied by that user's attributes or access policy into a simple cipher-text, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed cipher-text. Security of an ABE system with outsourced decryption ensures that an adversary (including a malicious cloud) will not be able to learn anything about the encrypted message; however, it does not guarantee the correctness of the transformation done by the cloud. In this paper, we consider a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can efficiently check if the transformation is done correctly. We give the formal model of ABE with verifiable outsourced decryption and propose a concrete scheme. We prove that our new scheme is both secure and verifiable, without relying on random oracles. Finally, we show an implementation of our scheme and result of performance measurements, which indicates a significant reduction on computing resources imposed on users.

C. Decentralizing Attribute-Based Encryption

We propose a Multi-Authority Attribute-Based Encryption (ABE) system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority. In constructing our system, our largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority "tied" together different components (representing different attributes) of a user's private key by randomizing the key. However, in our system each component will come from a potentially different authority, where we assume no coordination between such authorities. We create new techniques to tie key components together and prevent collusion attacks between users with different global identifiers. We prove our system secure using the recent dual system encryption methodology where the security proof works by first converting the challenge cipher-text and private keys to a semi-functional form and then arguing security. We follow a recent variant of the dual system proof technique due to Lewko and Waters and build our system using bilinear groups of composite order. We prove security under similar static assumptions to the LW paper in the random oracle model.

V. PROPOSED SYSTEM

Attribute-based encryption the notion of attribute-based encryption (ABE). In subsequent works, they focused on policies across multiple authorities and the issue of what expressions they could achieve. Up until recently, raised a construction for realizing KPABE for general circuits. Prior to this method, the strongest form of expression is Boolean formulas in ABE systems, which is still a far cry from being able to express access control in the form of any program or circuit. Actually, there still remain two problems. The first one is their have no construction for realizing CPABE 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. Thus, it is apparently still remains a pivotal open problem to design an efficient circuit CP-ABE scheme. Hybrid encryption the generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length. Based on their ingenious work, a one-time MAC were combined with symmetric encryption to develop the KEM/DEM model for hybrid encryption. Such improved model has the advantage of achieving higher security requirements. ABE with Verifiable Delegation. Since the introduction of ABE, there have been advances in multiple directions. The application of outsourcing computation is one of an important direction. The first ABE with outsourced decryption scheme to reduce the computation cost during decryption. The definition of ABE with verifiable outsourced decryption. They seek to guarantee the correctness of the original cipher text by using a commitment. However, since the data owner generates a commitment without any secret value about his identity, the untrusted server can then forge a commitment for a message he chooses. Thus the cipher text relating to the message is at risk of being tampered. Furthermore, just modify the commitments for the cipher text relating to the message is not enough. The cloud server can deceive the user with proper permissions by responding the terminator $\perp$ to cheat that he/she is not allowed to access to the data.

1. Notations:

Zp - finite field with prime order p.

$\perp$ - formal symbol denotes termination.

$x \leftarrow X$- x is randomly selected from X.

A is an algorithm then $A(x) \rightarrow y$ 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.

$\varepsilon: Zp \rightarrow R$- negligible if for every $c > 0$ there is a K such that $\varepsilon(k) < k^{-c}$ for all $k > K$.

2. Algorithms used

Following are few other algorithms which are used:

- **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_.
- **Hybrid-encrypt:** (PK, f = (n, q, A, B, GateType), M$\in${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$\in$ {0, 1}mas input.
- **KeyGen(MK, x $\in$ {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]}.Notethat, 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).

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

A. Design goals

For effective utilization of outsourced data, our system should achieve security and performance guarantee as follows:

- **Secure keyword search:** To explore different mechanisms for designing effective keyword search schemes based on the existing searchable encryption framework.[6]
- **Secure data sharing:** To allow user to share data over the cloud without losing privacy.
- **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.
- **Efficiency:** Above goals should be achieved with minimum communication and computation overhead.

VI. 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.

VII. CONCLUSION

In the cloud, for accomplished admission association and keeping vision confidential, the knowledge the info the information homeowners could accept attribute-based cryptography to encipher the grasp on data. decoding task to the cloud servers to cut back the computing value. Our ciphertext strategy attribute -based hybrid cryptography, we incline to could representative the verifiable partial decoding to the cloud server

VIII. REFERENCES

[1] M. Armbrust, A. Fo x, R. Griffith, A. D. Joseph, R. H. Kat z, 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 SecuritySymp, 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, Efficient, 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.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.

[8] 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.

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

Author's Profile:

Dr. D. Pavan Kumar Has Received His M.Tech PG In Computer Science From ANU, Guntur in 2010. He is dedicated total teaching field from the last 23 years. He has guided 30 P.G Students And more than 50 U.G Students. He is a Member in MISTE. He is working as Professor in Prakasam Engineering College, Kandukur, Prakasam(Dt), AP, India.. He is highly passionate and enthusiastic about his teaching and believes that inspiring students to give of his best in order to discover what he already knows is better than simply teaching.

Dr.Rajeev Kumar Working As Asst Professor in Shri Venkateswara University, Gajraula, UP, India