International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Circuit Cipher Text-Policy Attribute-Based Hybrid Cryptography With Demonstrable Delegation In Cloud Computing

Yadavalli. Gopi*[1], Bapanapalli Alekhya[2]

*[1]Assistant Professor, Department of MCA , St. Mary's Group Of Institutions, Guntur, Andhra Pradesh, India
[2]PG Student , Department of MCA , St. Mary's Group Of Institutions, Guntur, Andhra Pradesh, India.

ABSTRACT

In the cloud, for achieving access control and data security, the data owners could uses attribute-based encryption to encrypt the stored data. To reduce the cost, the users, which have a limited computing power, are nevertheless more likely to delegate the mask of the decryption task to the cloud servers. The result shows, attribute-based encryption with delegation come out. Still, there are some problems and questions regarding to previous related works. For example, during the delegation or release, the cloud servers could misrepresent or replace the delegated cipher text and respond a fake result with malevolent intent. As well as for the purpose of cost saving the cloud server may also fraud the eligible users by responding them that they are unworthy. Even, the access policies may not be flexible during the encryption. Since policy for general circuits are used to achieve the strongest form of access control, a construction to design circuit cipher text-policy attribute-based hybrid encryption with verifiable delegation has been developed. This system is mixed with verifiable computation and encrypt-then-Mac mechanism, the data confidentiality, the fine-grained access control as well as the correctness of the delegated computing results are well guaranteed at the same time. As well as this scheme achieves security against chosen-plaintext attacks under the k-multilinear Decisional Daffier-Hellman assumption. Moreover, this scheme achieves feasibility as well as efficiency.

Keywords: Cipher text-policy attribute-based encryption, circuits, verifiable delegation, multi linear map, hybrid Encryption

I. INTRODUCTION

Cloud computing is innovation, which uses advanced computational power as well as improved storage capabilities. Cloud computing is a long dreamed vision of computing utility, which enable the sharing of services over the internet. Cloud is a large group of interconnected computers, which is a major change in how we store information and run application. Cloud computing is a shared pool of configurable computing resources, on-demand network access and provisioned by the service provider. The advantage of cloud is cost savings. The prime disadvantage is security. The appearance of cloud computing transports a radical novelty to the organization of the data possessions within this calculating surroundings, the cloud servers can present different data services, such as isolated data storage and outsourced allocation calculation etc. For information cargo space, the servers amass a huge quantity of communal information, which might be accessed by certified users. For allocation calculation, the servers could be accustomed to hold and determine frequent data dealing to the user's burden. As applications shift to cloud computing proposals, verifying delegation process using cipher text-policy attribute-based encryption (CP-ABE) is used to guarantee the data privacy and the verifiability of allocation on untruthful cloud servers. Captivating health check data distribution as an example among the rising volumes of health check images and health check records, the medical care associations set a big amount of data in the cloud for dropping. To make such data sharing be achievable, attribute based encryption is used. There are two forms of attribute-based encryption. One is key-policy attribute-based encryption (KP-ABE) and the second is ciphertext-policy attribute-based encryption. In CP-ABE system, each cipher text is contains an access

Structure and each private key are labeled with a set of descriptive attributes. A user is able to decrypt a ciphertext if and only if the key's attribute set satisfies the access structure associated with a cipher text. The cloud server provides another service which is delegation computing. The VD-CPABE scheme shows that the entrusted cloud will not be able to learn anything about the encrypted message and build the original cipher text.

II. PROBLEM STATEMENT

The cloud server is able to replace delegated cipher text and respond a fake result with malevolent intent. As well as for the purpose of cost saving the cloud server may also fraud the eligible users by responding them that they are unworthy. In suchscheme, the access policies may not be flexible during the encryption.

Outsourcing Decryption of Multi-Authority ABE Cipher texts Keying Li and Hue Ma 2013

The believed of multi-authority attribute established encryption was gave by Pursue in TCC 2007. In this paper, we enhance Chase's scheme to permit encryptions to ascertain how countless qualities are needed for every single cipher text from connected attribute authorities. The counseled scheme can be perceived as a multi trapdoor construction. Further-more, we apply the LMSSS to outsource the decryption of multi-authority attribute established encryption scheme for colossal universe. In addition, the outsourcing scheme can be comprehended in the setting of multi-authority key-policy attribute established encryption. Both our schemes can be spread to RCCA safeguard ones.

Attribute Instituted Encryption alongside Privacy Maintaining employing Asymmetric Key in Cloud Computing

S.Sankareswar and S.Hemanth 2014 Symmetric key algorithm uses alike key for both encryption and decryption. The authors seize a centralized way whereas a solitary key allocation center (KDC) distributes hidden keys and qualities to all users. A new decentralized admission manipulate ion scheme for safeguard data storage in clouds that supports nameless authentication. The validity of the user who stores the data is additionally verified. The counseled scheme is to obscure the users qualities employing SHA algorithm .The Parlier cryptosystem, is a probabilistic asymmetric algorithm for area key cryptography. Parlier algorithm use for Conception of admission strategy, file accessing and file refurbishing procedure and additionally obscuring the admission strategy to the user employing query established algorithm.

Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Safeguard Realization Brent Waters 2006 we present a new methodology for comprehending Cipher text -Policy Attribute Encryption (CP-ABE) below concrete and non-interactive cryptographic assumptions in the average model. Our resolutions permit each encrypt or to enumerate admission manipulation in words of each admission formula above the qualities in the system. In our most effectual arrangement, cipher text size, Encryption and decryption period scales linearly alongside the intricacy of the admission formula. The merely preceding work to accomplish these parameters was manipulated to facts in the generic cluster model. We present three constructions inside our framework. Our arrangement is proven selectively safeguard below an assumption that we call the decisional Parallel Bilinear Die- Hellman Exponent (PBDHE) assumption that can be believed as a generalization of the BDHE assumption. Our subsequent two constructions furnish presentation transactions to accomplish provable protection suitably below the (weaker) decisional Bilinear-Di e-Hellman Exponent and decisional Bilinear Die-Hellman assumptions.

How to Representative and Confirm in Public: Verifiable Computation from Attribute-based Encryption Bryan Par no Mariana Beam ova and Vend Vaikuntanathan 2011 The expansive collection of tiny, computationally frail mechanisms and the producing number of computationally intensive tasks makes it appealing to representative computation to data centers. Though, outsourcing computation is functional merely after the returned consequence can be trusted, which

Makes verifiable computation (VC) a have to for such scenarios. In this work, we spread the meaning of verifiable computation in two vital directions: area delegation and area verifiability that have vital requests in countless useful delegation scenarios. Yet, continuing VC constructions established on average cryptographic assumptions flounder to accomplish

these properties Cryptanalysis of the Multilinker Chart above the Integers Jung He Chon, Kyoohyung Han and Altering Lee 2014. *Vol-2 Issue-2 2016 IJARIIE-ISSN (O)-2395-4396* 1816 www.ijariie.com 784

We delineate a polynomial-time cryptanalysis of the (approximate) multilinker chart of Croon, Leporine and Debouche (CLT). The attack relies on an adaptation of the so -called zero sizing attack opposing the Garb, Gentry and Halve (GGH) candidate multi-linear map. Zero sizing is extra desecrating for CLT than for GGH. In the case of GGH, it permits to break generalized ions of the Decision Linear and Subgroup Membership setbacks from pairing-based cryptography. For CLT, this leads to a finished break: all numbers meant to be retained hidden can be efficiently and openly recovered.

III. PRELIMINARY

A. Our Contribution

Existing system in every cipher text is related to associate degree access structure, and every non -public secret is labelled 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 cipher text. 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 because of restricted resources. Instead, they are presumably to source a part of the decoding method to the cloud server. Whereas the entrusted cloud servers UN agency will translate the first cipher text into a straightforward one may learn nothing concerning the plaintext from the delegation. Whereas the entrusted cloud servers UN agency will translate the first cipher text into a straightforward one may learn nothing concerning the plaintext from the delegation.

B. Our Techniques The increasing volumes of records place 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, user is ready to decipher a cipher text, the storage service provided by the cloud server, and therefore the outsourced information [4] must not 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.

IV. EXISTING SYSTEM

In existing system, the attribute-based encryption technique was used. However, this scheme contains some problems and questions regarding to related works. Like during the delegation or release the cloud servers could misrepresent or replace the delegated cipher text and respond a fake result with malevolent intent. For the purpose of cost saving the cloud server may also fraud the eligible users by responding them that they are unworthy. Even, the access policies may not be flexible enough as well during the encryption.

Disadvantage of Existing System:-

No guarantee that the calculated result returned by the cloud is always correct.

The cloud server may build ciphertext or fraud the eligible user that he even does not have permissions to decryption.

Loss the data security, confidentiality as well as access control.

V. SYSTEM ARCHITECTURE

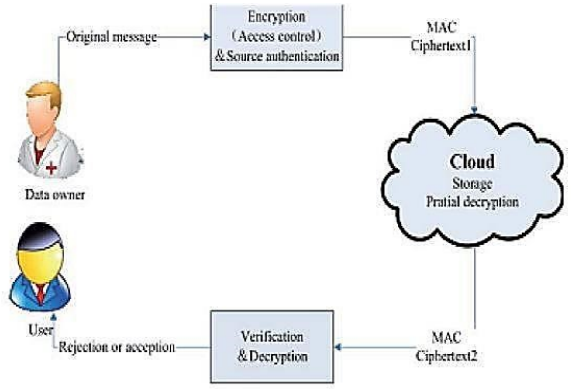

Figure 1. System Architecture

The system contains four modules,

1. Cloud Storage Module
2. Data Owner Module
3. Data User Module
4. Authority Module

Cloud Storage:

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage

providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store end user, organization, or application data.

Data Owner:

The data owner encrypts his message under access policy, then computes the complement circuit, which outputs the opposite bit of the output of f, and encrypts a random element R of the same length to under the policy

Data User:

The users can outsource their complex access control policy decision and part process of decryption to the cloud. Which extended encryption ensures that the users can obtain either the message M or the random element R, which avoids the scenario when the cloud server deceives the users that they are not satisfied to the access policy, however, they meet the access policy actually.

Authority:

Authority generates private keys for the data owner and user.

VI. 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 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 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 was 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 UN trusted server could 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.

A. 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. $G(\lambda, k)$- group generation algorithm where λ is the security Parameter. k -the number of allowed pairing operation. ε: $Zp \rightarrow R$- *negligible* if for every $c > 0$ there is a K such that $\varepsilon(k) < k-c$ for all $k > K$. **B. Algorithms Used** 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* $(PK, f = (n, q, A, B, GateType), M \in \{0, 1\}m)$): This algorithm is executed by the data owner. Taking the public parameters PK, a description f of a circuit and a message $M \in \{0, 1\}m$ as input.

2. 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 $x \in \{0, 1\}\ n$. It

firstly chooses a random $t \in Zp$. Then it creates the private key as $KH = g\_yt$, $L = gt$, if $xi = 1$ $Ki = (yhi)t$, if $xi = 0$ $Ki = (yhn+i)t$, $i \in [1, n]$. The transformation key is $TK = \{L,Ki, i \in [1, n]\}$.Note that, for the data owner *IDo*, the authority generates his private key with the identity attribute *ID*0 as $KH = g\_yt$, $L = gt$, $KIDo = Ht3$ (*IDo*).

3. Transform(TK,CT)

The cloud server executes the transformation algorithm. It takes as input the transformation key *TK* and the

Original cipher text *CT*. The algorithm partially decrypts the cipher text. **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.[6] **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.

VII.CONCLUSION

Design a circuit cipher text-policy attribute-based hybrid encryption with provable allocation method. The universal circuits are helpful to achieve or clear the strongest form of entrée manage strategy. Collective provable calculation and encrypt-then-Mac system with our cipher text policy attribute-based hybrid encryption, we could assign the provable fractional decryption paradigm to the cloud server. The k-multi-linear Decisional Diffie-Hellman assumption proves the

Proposed scheme is secure. On the other side, this scheme can use over the integers. The conclusion show that the method is sensible in the cloud computing. Thus, can be able to achieve data privacy, the fine-grained entrée manages and the demonstrable allocation in cloud.

VII. REFERENCES

[1]. JunbeomHur and Dong Kun Noh," Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems", VOL. 22, NO.7, JULY 2011 IEEE.

[2]. J. Han, W. Susilo, Y. Mu, and J. Yan, "Privacy-preserving decentralized key-policy attribute-based Encryption," IEEE Trans. ParallelDistrib. Syst., vol. 23, no. 11, pp. 2150–2162, Nov. 2012.

[3]. J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. ParallelDistrib. Syst., vol. 25, no. 8, pp. 2201–2210, Aug. 2013.

[4]. K. Kurosawa and Y. Desmedt, "A new paradigm of hybridencryption scheme," in Proc. 24th Int. Cryptol. Conf., 2004, pp. 426–442.

[5]. R. Cramer and V. Shoup, "A practical public key cryptosystemprovably secure against adaptive chosen ciphertext attack," inProc. 18th Int. Cryptol. Conf., 1998, pp. 13–25.

[6]. J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryptionwith verifiable outsourced decryption," IEEE Trans. Inf. ForensicsSecur., vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[7]. B. Waters, "Ciphertext-policy attribute-based encryption: Anexpressive, efficient, and provably secure realization," in Proc.14th Int. Conf. Practice Theory Public Key Cryptography. Conf. PublicKeyCryptography., 2011, pp. 53–70.

[8]. A. Lewko and B. Waters, "Decentralizing attribute-basedencryption," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptograph.Techn., 2011, pp. 568–588.

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

[10].M. Green, S. Hohenberger, and B. Waters, "Outsourcing thedecryption of ABE Ciphertexts," in Proc. USENIX Security Symp.,San Francisco, CA, USA, 2011, p. 34.