International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 8 – MAY 2017.

An Enhanced Circuit Ciphertext in Cloud based Efficient User Revocation Mechanism on Top of Anonymous ABE

ANIL KUMAR MAGAPU [#1] and K RAJESH [*2]

[#] *PG Scholar, Kakinada Institute Of Engineering & Technology Department of Computer Science & Engineering , JNTUK,A.P, India.*

[*] *Assistant Prof, Dept of CSE, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA.*

***Abstract*— In this paper, we show how Circuit Cipher text policy extends the User Revocation algorithm with a hierarchical structure to improve scalability and flexibility while inherits the feature of fine-grained access control. The scheme provides full support for hierarchical user grant, file creation, file deletion, and user revocation in cloud computing. We formally prove the security of the proposed scheme based on the security Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against un-trusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-graininess, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to un-trusted cloud servers without disclosing the underlying data contents.**

Index Terms*— Hybrid encryption, Verifiable delegation, Multi-linear map.

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 [1]. Cloud computing allows user to use different services which saves money that users spend on applications. Data owners and organizations are motivated to outsource 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. For data storage, the servers store a large amount of shared data, which could be accessed by authorized users. For delegation computation, the servers could be used to handle and calculate numerous data according to the user's demands. To overcome the above problem in this paper new technique is introduced technique which used Cipher text policy attribute-based encryption [2]. In this scheme is a promising cryptographic solution to these issues for enforcing access control policies defined by a data owner on outsourced data. Some problem of applying the only attribute-based encryption in an outsourced architecture introduces several challenges with regard to the attribute and user revocation. So we used the cipher text –policy attribute encryption.

As applications move to cloud computing platforms, cipher text-policy attribute-based encryption (CPABE) and verifiable delegation (VD) are used to ensure the data confidentiality and the verifiability of delegation on dishonest cloud servers [3]. Data owners may wants to share their outsourced data with other large amount of users. Users may want to only retrieve certain specific data files they are interested in during a given session. Some of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates. They focused on policies across multiple authorities and the issue of what expressions they could achieve. Uses another form of encryption is hybrid encryption for encrypt messages of arbitrary length. Onetime MAC was combined with symmetric encryption to develop the KEM/DEM model for hybrid encryption [4]. Attribute-based encryption with verifiable delegation is decryption scheme to reduce the computation cost during decryption.

II. LITERATURE SURVEY

A. Securely Outsourcing Attribute-Based Encryption with Check ability:

In this paper [5], 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 an decryption are getting prohibitively high. We propose a new Secure Outsourced ABE system, which supports both secure outsourced key-issuing and decryption

B. Outsourcing the Decryption of ABE Cipher texts

Attribute-based encryption (ABE) [6] 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 repayable 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.

C. Attribute-Based Encryption with Verifiable Outsourced Decryption

J. Lai, R. H. Deng, C. Guan and J. Weng [7] proposed an attribute-based encryption (ABE) which 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.

D. Decentralizing Attribute-Based Encryption

Lewko and Waters [8] proposed 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.

E. Cipher text-Policy Attribute-Based Encryption: an Expressive, Efficient, and Provably Secure Realization

Waters presented a new methodology for realizing Cipher text-Policy Attribute Encryption (CP-ABE) under concrete and noninteractive cryptographic assumptions in the standard model [9]. Our solutions allow any encryptor to specify access control in terms of any access formula over the

attributes in the system. In our most efficient system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model.

We present three constructions within our framework. Our first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. Our next two constructions provide performance tradeoffs to achieve provable security respectively under the (weaker) decisional Bilinear-Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions.

III. EXISTING SYSTEM

The servers could be used to handle and calculate numerous data according to the user's demands [10]. As applications move to cloud computing platforms, cipher text-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[11]. The increasing volumes of medical images and medical records, the healthcare organizations put a large amount of data in the cloud for reducing data storage costs and supporting medical cooperation. There are two complementary forms of attribute based encryption [12]. One is key-policy attribute-based encryption (KP-ABE) and the other is ciphertext-policy attribute-based encryption (CPABE) [13].

- The cloud server might tamper or replace the data owner's original ciphertext for malicious attacks, and then respond a false transformed ciphertext [14].
- The cloud server might cheat the authorized user for cost saving. Though the servers could not respond a correct transformed ciphertext to an unauthorized user, he could cheat an authorized one that he/she is not eligible [15].

IV. PROPOSED SYSTEM

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. The proposed scheme is proven to be secured based on k-multilinear Decisional Diffie-Hellman assumption. On the other hand, we implement our scheme over the integers. During the delegation computing, a user could validate whether the cloud server responds a correct transformed cipher text to help him/her decrypt the cipher text immediately and correctly.

A. ARCHITECTURE:

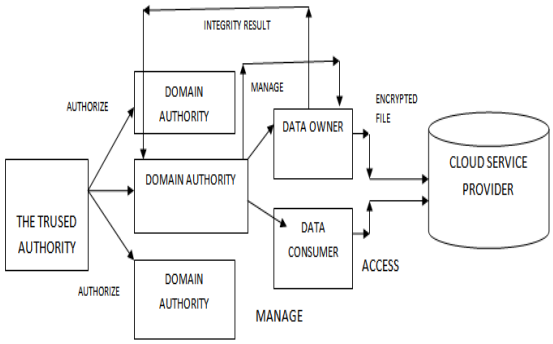

Fig. 1 Architecture diagram

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.

Advantages of proposed system:

- The generic KEM/DEM construction for hybrid encryption which can encrypt messages of arbitrary length.
- They seek to guarantee the correctness of the original cipher text by using a commitment.
- We give the anti-collusion circuit CP-ABE construction in this paper for the reason that CPABE is conceptually closer to the traditional access control methods.

B. MODULES

1. Cloud Storage
2. Security Model
3. Ciphertext-policy attribute-based encryption
4. Hybrid encryption
5. Email Authentication

C. 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.

1) Security Model

Since we use key encapsulation mechanism (KEM) and authenticated encryption (AE) to build our hybrid VD-CPABE scheme, we describe the security definition separately at first. The confidentiality property (indistinguishability of encryptions under selective chosen plaintext attacks (IND-CPA)) required for KEM is captured by the following games against adversary A.

a) Game.KEM

• Init. The adversary gives a challenge access structure f∗, where it wishes to be challenged.

• Setup. The simulator runs the Setup algorithm and gives the public parameters PK to the adversary.

• KeyGen Queries I. The adversary makes repeated private key queries corresponding to the sets of attributes x1, ..., xq1 . We require that ∀i ∈ q1 we have f∗(xi) = 0.

• Encrypt. The simulator encrypts K0 under the structure f∗, random chooses K1 from key space and flips a random coin b. Then the simulator sends Kb and the ciphertext CK∗ to the adversary.

• KeyGen Queries II. The adversary makes repeated private key queries corresponding to the sets of attributes xq1 , ..., xq where f∗(x) = 0.

• Guess. The adversary outputs a guess b′ of b. We define the advantage of an adversary A in this game is Pr[b′ = b] − 1 2 . Then a KEM scheme is secure against selective chosen plaintext attacks if the advantage is negligible. The confidentiality property (indistinguishability of encryptions under selective chosen ciphertext attacks (IND-CCA)) required for AE is captured by the following games against adversary A.

b) Game.AE

- Init. The adversary submits two equal length messages M0 and M1.
- Setup. The simulator runs the Setup algorithm and generators the symmetric key KAE.
- Encrypt. The simulator flips a random coin b, encrypts Mb under the symmetric key KAE, generates the ciphertext C∗ and gives it to the adversary.
- Decrypt Queries. The adversary makes repeated decryption queries. When the given ciphertext C≠ C∗, the simulator will return DKAE(C) and σKAE(C) to the adversary.

D. Cipher text - policy attribute–based encryption

In this section, we present the definition and security model of our hybrid VD-CPABE. In such a system, a circuit ciphertext-policy attribute-based encryption scheme, a symmetric encryption scheme and an encrypt-then-mac mechanism are applied to ensure the confidentiality, the fine-grained access control and the verifiable delegation

A hybrid VD-CPABE scheme is defined by a tuple of algorithms (Setup, Hybrid-Encrypt, Key- Gen, Transform, Verify-Decrypt). The description of each algorithm is as follows. Setup(λ, n, l). Executed by the authority, this algorithm takes as input a security parameter λ, the number of attributes n and the maximum depth l of a circuit. It outputs the public parameters PK and a master key MK which is kept secret. more information. This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing Hybrid-Encrypt(PK,M, f). This algorithm is executed by the data owner. It could be conveniently divided into two parts: key encapsulation mechanism (KEM) and authenticated symmetric encryption (AE). The KEM algorithm takes as input the public parameters PK and an access structure f for circuit. It computes the complement circuit f and chooses a random string R. Then it generates KM = {dkm, vkm}, KR = {dkr, vkr} and the CP-ABE ciphertext (CKM,CKR). The AE algorithm takes as input a message M, the random string R, the symmetric key.

E. Hybrid encryption

Cramer and Shoup proposed 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. Since the introduction of ABE, there have been advances in multiple directions. The application of outsourcing computation is one of an important direction. Green et al designed [15] the first ABE with outsourced decryption scheme to reduce the computation cost during decryption. After that, Lai et al. proposed the definition of ABE with verifiable outsourced decryption. They seek to guarantee the correctness of the original ciphertext 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 ⊥ to cheat that he/she is not allowed to access to the data.

F. Email Authentication:

Email authentication is a collection of techniques aimed at equipping messages of the email transport system with verifiable information. It is a coarse-grained

authentication, usually at Administrative Management Domain (ADMD) level, and implies no sort of authorization. That is, the purpose of email authentication is to validate the identities of the parties who participated in transferring a message, as they can modify the message. The results of such validation can then be used in delivery decisions, which are beyond the scope of email authentication proper, and are quite different in nature.

Recipients can use authentication to verify the source of an incoming message and avoid phishing scams. For example, if you see messages claiming to be from google.com, but are not properly authenticated as coming from google.com, these are phishing messages. You should not enter or send any personal information. Remember, Google will never ask you to send personal information

G. *IMPLEMENTATION*

The results of the proposed system are shown below.

Fig.2 Decryption of partial File

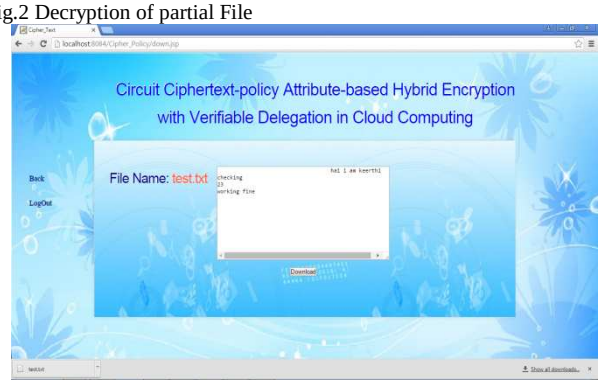

Fig.3 File Download

V. CONCLUSION

We created a system for Ciphertext-Policy Attribute Based Encryption. Our system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. Our system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys. Finally, we provided an implementation of our system, which included several optimization techniques.

In the future, it would be interesting to consider attribute-based encryption systems with different types of expressibility. While, Key-Policy ABE and Ciphertext-Policy ABE capture two interesting and complimentary types of systems there certainly exist other types of systems. The primary challenge in this line of work is to find new systems with elegant forms of expression that produce more than an arbitrary combination of techniques. One limitation of our system is that it is proved secure under the generic group heuristic. We believe an important endeavour would be to prove a system secure under a more standard and non-interactive assumption. This type of work would be interesting even if it resulted in a moderate loss of efficiency from our existing system.

REFERENCES

[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] 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.

[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/.
[21] 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.
[22] M. Bellare and C. Namprempre, "Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm," in Proc. ASIACRYPT, pp.531-545, Springer- Verlag Berlin, Heidelberg, 2000.
[23] J. Coron, T. Lepoint and M. Tibouchi, "Practical Multilinear Maps over the Integer," in Proc. CRYPTO, pp.476-493, Springer-Verlag Berlin, Heidelberg, 2013.
[24] S. Garg, C. Gentry and Shai Halevi, "Candidate Mulitilinear Maps from Ideal Lattices and Applications," in Proc. EUROCRYPT, pp.1-17, Springer-Verlag Berlin, Heidelberg, 2013.

AUTHOR PROFILE

ANIL KUMAR MAGAPU is a student of Kakinada Institute Of Engineering & Technology affiliated to JNTUK, Kakinada pursuing M.Tech (Software Engineer). His Area of interest includes Cloud Computing and its objectives in all current trends and techniques in Computer Science.

K.RAJESH M.TECH is working as Assistant Professor, Department of Computer Science & Engineering, Kakinada Institute of Engineering & Technology, JNTUK, A.P, INDIA.