A Novel Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing for Data Security

DR. B. VAMSEE MOHAN¹, J. DEVika²

¹Associate Professor, Dept of CSE, PBRVITS, Kavali, Andhra Pradesh, India.
²PG Scholar, Dept of CSE, PBRVITS, Kavali, Andhra Pradesh, India.

Abstract: In this Project, we show how Circuit Cipher text policy schema based extends the User Revocation schema with a hierarchical structure to improve scalability and flexibility while at the same time inherits the feature of fine-grained access control. Second, we demonstrate how to implement a full-fledged access control scheme for cloud computing. The scheme provides full support for hierarchical user grant, file creation, file deletion, and user revocation in cloud computing. Third, 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 untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, 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-grainedness, 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 untrusted cloud servers without disclosing the underlying data contents.

Keywords: 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 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. 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 application 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. Data owners may want 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 a onetime MAC were combined with symmetric encryption to develop the KEM/DEM model for hybrid encryption. Attribute-based encryption with verifiable delegation is decryption scheme to reduce the computation cost during decryption.
II. 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. It is now attractive to deploy an innovative new Internet service on a third party's Internet Datacenter rather than your own infrastructure, and to gracefully scale its resources as it grows or declines in popularity and revenue. Expanding and shrinking daily in response to normal diurnal patterns could lower costs even further. Cloud Computing transfers the risks of over-provisioning or under-provisioning to the Cloud Computing provider, who mitigates that risk by statistical multiplexing over a much larger set of users and who offers relatively low prices due better utilization and from the economy of purchasing at a larger scale. We define terms, present an economic model that quantifies the key buy vs. pay-as-you-go decision, offer a spectrum to classify Cloud Computing providers, and give our view of the top 10 obstacles and opportunities to the growth of Cloud Computing.

B. Outsourcing the Decryption of ABE Cipher-texts

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 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.

C. 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.

D. 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.
A Novel Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing for Data Security

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.

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 of information [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 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

IV. SYSTEM ARCHITECTURE
The system contains four modules,
1. Cloud Storage Module
2. Data Owner Module
3. Data User Module
4. Authority Module

1. 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.

Fig1. System Architecture

2. 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.

3. 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.

4. Authority: Authority generates private keys for the data owner and user.

V. 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.

VI. REFERENCES


Author's Profile:

**B. Vamsee Mohan** received the B.Tech degree from St. Peter's Engineering College, Avadi, Chennai, India. He completed M.Tech in Computer Science Engineering from JNTU University, Kakinada, India. He is having nearly 17 years of teaching experience. He is currently working as Assoc. Professor, Dept of C.S.E, PBRVITS College, Nellore, A.P, and India.

**Devika Jinkala** received B.Tech in Computer Science and Engineering from Ramireddy Subbaramy Reddy Engineering College affiliated to the Jawaharlal Nehru technological university Anathapur in 2015, and pursuing M. Tech in Computer Science and Engineering from PBR Visvodaya Institute of Technology And Science affiliated to the Jawaharlal Nehru technological university Anantapur in 2017, respectively.