Attribute based hybrid encryption policy for encrypting the cloud data

[1]Shweta S G, [2]Dr Jayashree A

[1]Student, [2]Lecturer in CSE Department
[1]Computer science department,
PDA college of engineering, Gulbarga,India

***Abstract*— In the cloud, for keeping data confidential and achieving access control, the data owners could adopt attribute-based encryption to encrypt the stored data. Users with limited computing power are more likely to delegate the original of the decryption task to the cloud servers to reduce the cost computing. As a result, attribute-based encryption with delegation emerges. Still, there are warning and questions remaining in the previous relevant works. For instance, during the delegation, the cloud servers could damage or replace the delegated ciphertext and respond a forged computing result with malicious intent. They may also cheat the authorized 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. Since policy for general circuits enables to achieve the strongest form of access control, a construction for realizing ciphertext-policy attribute-based hybrid encryption with verifiable delegation in the cloud has been considered in this work. In such a system, combined with verifiable computation and encrypt-then-mac mechanism, the data confidentiality, the fine-grained access control and the defects of the delegated computing results are well guaranteed at the same time. Besides, our scheme achieves security against chosen-plaintext attacks under k-multilinear Decisional & Diffie-Hellman assumption. Moreover, an extensive simulation campaign confirms the feasibility and efficiency of the proposed solution.**

Index Terms*—Random key generation, Dual encryption, time seal, Malware injection attack.(keywords)*

I. INTRODUCTION (HEADING 1)

The requirement of cloud computing carry a revolutionary innovation to the management of the data resources.The cloud servers can offer various data services, such as outsourced delegation computation [1] and remote data storage [2], [3], etc Within this computing situation. For data storage, the servers store a huge amount of shared data, which could be accessed by delegated users. For delegation computation, the servers could be used to knob and determine numerous data according to the user's claim. As applications shift to cloud computing platforms, ciphertext-policy attribute-based encryption (CP-ABE) [4], [5] and verifiable delegation (VD) [6], [7] are used to ensure the data confidentiality and the verifiability of delegation on corrupt cloud servers. Taking medical data distribution as an example (see Fig. 1), with the increasing volumes of medical files and medical documents, the health protection management put a huge amount of data in the cloud for decreasing data storage costs and supporting medical service. Since the cloud server may not be creditable, the file cryptographic storage is an valid method to block secret data from being snatched or destroy. In the meantime, the authority may wish to share data with the person who comfort some requirements. The requirements, i.e., access policy, could be {Medical cooperation Participation ^ (Chief Doctor _Attendant Doctor) ^ Pediatric}. To make such data allocation be attainable, attribute based encryption is applicable. There are two equivalent forms of attribute-based encryption. One is ciphertext-policy attribute-based encryption and other is key-policy attribute-based encryption (KP-ABE) [8], [9], [10], In a CP-ABE system, each ciphertext is combine with an access structure, and each secret key is classify with a set of detailed attributes. if the key's attribute set entertain the access structure correlate with a ciphertext then user is capable to decode a ciphertext. Apparently, this system is conceptually nearest to common access control methods. On the opposed in a KP-ABE system, the selection of access policy is built by the key distributor rather of the enciphered, which maximum the practicability and usability for the system in practical functions On the other hand, in a ABE system, the access policy for normal circuits could be notice as the strongest form of the policy expression that circuits can explicit any program of settled running time..

II. RELATED WORK

Attribute-based encryption (ABE) is a public-keybased one-to-many encryption that allows users to encrypt and decrypt data based on user attributes Different from identity-based encryption scheme, an attribute-based encryption scheme is a scheme in which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each ciphertext [4].ABE comes in two sapidity called key-policy ABE (KP-ABE) and ciphertext-policy ABE. In KP-ABE, attributes are used to describe the encrypted data and policies are built into user's keys; while in CP-ABE, the attributes are used to describe a user's probate, and an encryptor determines a policy on who can decrypt the data[1]. Attribute-based encryption (ABE) is a public-keybased one-to-many encryption that allows users to encrypt and decrypt data based on user attributes [5]. In a decentralized attribute-based encryption (ABE) system, any party can act as an authority by creating a public key and issuing private keys to different users that reflect their attributes without any collaboration. Such an ABE scheme can eliminate the burden of heavy communication and collaborative computation in the setup phase of multiauthority ABE schemes, thus is considered more preferable [7]. With the growing popularity of cloud computing, organizations and data owners starts to outsource their important data to the public cloud for reduced management cost and ease of access. Encryption helps to protect

user data confidentiality, it makes difficult to perform secure plain text search over the encrypted data [8]. In [10] the wide variety of small, computationally weak devices and the growing number of computationally intensive tasks makes it appealing to delegate computation to data centers. However, outsourcing computation is useful only when the returned result can be trusted, which makes verifiable computation (VC) a must for such scenarios. In this work we extend the definition of verifiable computation in two important directions: public delegation and public verifiability, which have important applications in many practical delegation scenarios..

III. Proposed Work

Proposed scheme is proven to be secured based on k-multilinear Decisional Diffie-Hellman assumption. By the side, we implement our scheme over the integers. The costs of the computation and communication ingestion show that the scheme is practical in the cloud computing. Therefore, we could apply it to make sure the fine-grained access control, verifiable delegation and the data confidentiality in cloud. Since policy for general circuits enables to achieve the endurance form of access control, a construction for accost circuit ciphertext-policy attribute-based hybrid encryption with verifiable deputation has been advised in our work. The data confidentiality, the fine-grained access control and the correctness of the delegated computing results are well guaranteed at the same time in a system, that is in combination with verifiable encrypt then Mac computation and mechanism. By the side, under the k-multilinear Decisional Diffie-Hellman assumption our scheme achieves security against chosen-plaintext attacks.

IV. System Model

The system design defined as a graphical representation of how the data flow through an information system and also models its process aspects. A DFD represents what type of information is given to the system in the form of out and what kind of output will be received from the output.

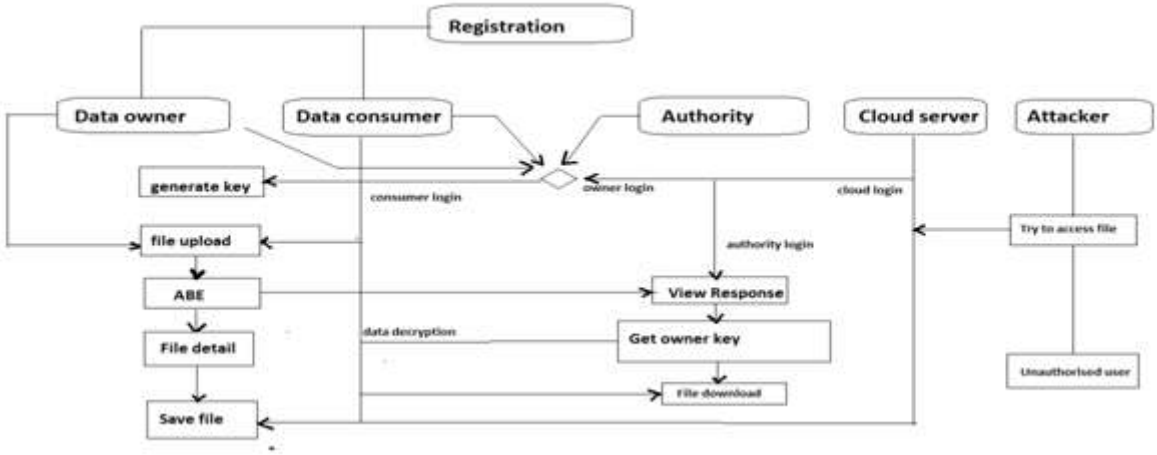

Fig 1 : **System design of attribute based hybrid encryption policy for encrypting the cloud data**

Data owner

Data owner carries the data and transmit the encrypted data to cloud service provider to store the data in cloud servers. Dual encryption of the file is to be done with the random key encryption and by the symmetric key to access the file by users, apply this theory to encrypt the data and then sync them to cloud servers to use in common with the other users.

Data Consumer

This is an entity who wants to access the outsourced data. If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the data owner, and is not revoked in any of the attribute groups, then he will be able to decrypt the ciphertext and obtain the data. Data consumers are the bodies who access the encrypted data stored in cloud servers. Only the authorized users who comply with the access theory of data owner can decrypt the encrypted data to retrieve the plaintext data.

Authority

In this module, the authority login and request the key to access the file. the authority can see all the details of data owner and data consumer and ends the session by logging out.

Cloud Service

It is an entity that provides a data service. It consists of data servers and a data service manager. data from data owners are stored in the data servers. The data service manager is in charge of controlling the accesses from outside users to the outsourced data in servers and providing corresponding contents services.

Attacker

Cloud malware injection is the attack that attempts to inject a malicious service, application or even virtual machine into the cloud system depending on the cloud service models. If any of the attackers try to inject the file the data owner receive an alert message so it is not possible to access the data by unauthorized user.

Proposed Algorithm:

We have proposed a combination of two different security algorithms to eliminate the security challenges of Personal Cloud Storage. We have taken a combination of algorithms like: AES and symmetric key encryption. A symmetric key algorithm, in which a single key is used for both encryption/decryption of data. Whereas AES is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. A user can upload Text file in Personal Cloud Storage. When uploading file AES and symmetric key encryption encoding schemes are used to encrypt data. The Block Diagram of proposed work at multilevel encryption is shown in following figure

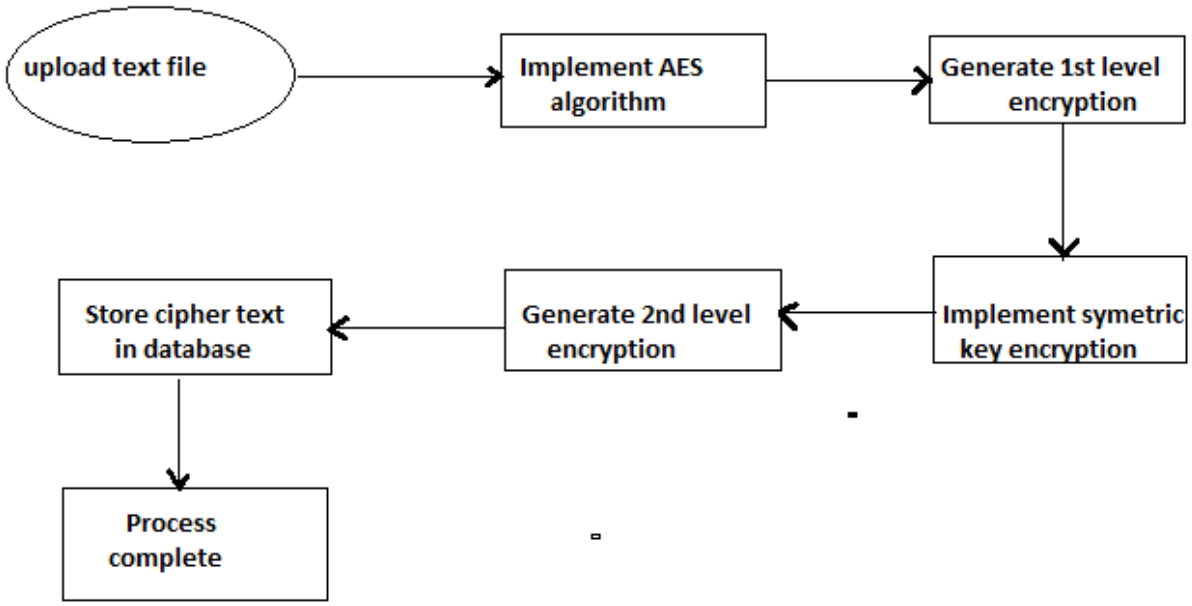

Fig 2: Block Diagram of Multilevel Encryption

V. Implementation And Results

The implementation of this work is executed in the utmost renowned tool of java that is Eclipse Luna by connecting it to MySQL Workbench 5.2 CE. Eclipse Luna is an incorporated advancement environment (IDE) for creating applications using standardized java programming language. Bootstrap and JSP technologies are used for developing WebPages and provide contribution in the UI design. Hibernate is an ORM structure used for database access where as the spring framework provides security in the design. The CSP used in this work is DriveHQ which is an IT cloud service provider and have some unique features like DriveHQ file manager, DriveHQ online backup and cloud file sharing. Generator API's are used for the generation of a random encryption secret key for both the user and the consumer and will be mailed to the registered emailID. The experimental results compute that this work achieves security by providing the automatic CANCELLATION OF THE accessing the file right after a time period allotted by the data owner. Malwar injection attacks can be resisted too. Besides its higher security, this work can accomplish high processing and storage ability.

.

VI. Conclusion and Future Work

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. 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. Now we are going to encrypt the particular file and uploading it onto the cloud. For further enhancements we can upload huge data containing files (it may be video, audio or many more). Even we can go for further live video streaming files by using some good technologies like hadoop and spark. Even we can add the concept of re-encryption of encrypted file. Further we can add the concept of auto triggering SMS with OPT.

REFERENCES

[1]M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing,"Univ.California,Berkeley,CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009.

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

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

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

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

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

[7]S. Yamada, N. Attrapadung, and B. Santoso, "Verifiable predicate Encryption and applications to CCA security and anonymous Predicate authentication," in Proc. Int. Conf. Practice Theory Public Key Cryptography. Conf. Public Key Cryptography. 2012, pp. 243–261.

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

[9]S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters, "Attribute based Encryption for circuits from multilinear maps," in Proc. 33rd Int. Cryptol. Conf., 2013, pp. 479–499.

[10]S. Gorbunov, V. Vaikuntanathan, and H. Wee, "Attribute-based encryption for circuits," in Proc. 45th Annu. ACM Symp. Theory Comput., 2013, pp. 545–554.

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

[12]V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based Encryption for Fine-grained access control of encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

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

[14]R. Cramer and V. Shoup, "Design and analysis of practical public key Encryption schemes secure against adaptive chosen ciphertext Attack," SIAM J. Comput., vol. 33, no. 1, pp. 167–226, 2004.

[15]D. Hofheinz and E. Kiltz R, "Secure hybrid encryption from weakened Key encapsulation," in Proc. 27th Int. Cr