iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4250

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Hybrid VD-CPABE with Secure Outsourcing

K. Maha Lakshmi[1], D. Manasa[2], P. Bhargav Kumar[3]
Department of IT, L.B.R.C.E, Krishna, A.P

Abstract: ***In this, for achieving access control to keep the data confidential, the data owner could adopt the Attribute Based Encryption(ABE) to encrypt stored data. In this during delegation the server could tamper or replace the delegated cipher-text and respond a false transformed cipher-text. This cause the server might cheat the authorized user. So, In this we propose a hybrid VD-CPABE (Verifiable Delegation Cipher-text Policy Attribute Based Encryption) Scheme with secure Outsourcing. In this we are using Verifiable delegation model. This model does not support to cheat any authorized user for every data manager maintains a secret key who is having that key that person can gain the data. Otherwise he cannot access the data. Finally it provides security to our data.***
Keywords : Attribute Based Encryption, Hybrid encryption, Verifiable Delegation Cipher-text policy attribute based encryption.

I. INTRODUCTION

Security consists of the policies and practices adopted to prevent and study unauthorized access, depart, mid-course correction, or contend of an individual digital assistant became omitted in and network-accessible resources. It involves the authorization of recover to specific in constrict, which is civilized by the administrator.. Users submit or are isolated an ID and code bought on credit or contradictory authenticating recommendation that allows them gain to intuition and programs within their authority. Security lottery covers a divergence of personal digital assistant networks, both public and unreasonable, that are circumlocutory in everyday jobs; conducting transactions and communications bounded by businesses, government agencies and individuals. Network bribe in the thrift is attentive in intelligence in organizations, enterprises, and special types of institutions. It does as its perform explains: It secures the constrict, as with a inaction as protecting and overseeing operations for done. The most common and absolutely done process of protecting a unite resource is by assigning it a unique favour and an indistinguishable password.

Security management is different for all kinds of situations. A home or small office may only require basic security meanwhile large businesses may require high-maintenance and current software and hardware to prevent malicious attacks from hacking and spamming.

For data storage, it stores a large amount of shared data, which could be accessed by authorized persons. For delegation computation, the servers could calculate the numerous data. As an application move to the server the cipher-text policy attribute based encryption (CP-ABE)[5],[6] and verifiable delegation[1] used to ensure the data confidentiality. Data confidentiality means if the information is stored on a system that information is protected against unauthorised users and it is often a measure of the ability of system to protect its data. There are two forms in attribute based encryption. First one is key policy attribute based encryption(KP-ABE)[6].In this, the access policy decision is made by key distributor and it limits some applications for users and second one cipher-text policy attribute based encryption(CP-ABE)[5],[6].In this, the CP-ABE maintains access structure and after encrypt the data by data owner the authorised user decrypt data and he/she satisfying the access structure of CP-ABE ,the person who satisfies the access structure that person access the original text that means decrypted data otherwise the data cannot be accessed by any person. The verifiable delegation model keeps the data as private and also achieves the fine grained access control mechanism. This access control mechanism achieved by dual encryption .This fine grained access control is flexible, efficient and provides security to the outsourcing systems. These outsourcing systems obtain the services from the outside suppliers. ABE with outsourced decryption scheme to reduce the computation cost during decryption. Here forged/cheating of the authorised user is not allowed.

A. Verifiability

During delegation the user could validate if the server responds to the Correct cipher-text it helps him/her to decrypt the cipher-text correctly. The server could not respond to the false cipher-text and it does not cheat the authorized user .By using verification key him/her could decrypt the data correctly, without that key they cannot access the data. So, here forgery is not allowed.

II. BACKGROUND WORK

In this, Encrypted data put into the server by using ABE with efficient verifiable outsourced decryption[2] to reduce the

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

computation cost. During decryption while reducing computation cost the decryption cost is also reduces and by using KP-ABE scheme overcome the restriction of circuits[3] and by using securely outsourcing [4] we introduce key generation service provider(KGSP) and Decryption service provider(DSP) and by using this verifiable delegation model removes multi authority ABE scheme[7] it maintains single authority. i.e., in this data owner obtain privately verified key to verify correctness of data and the VD-CPABE [1] System does not allow to cheat authorised user.

III. EXISTING SYSTEM

In this, for achieving access control and keeping message Confidential, the data owners could assume ABE to encrypt stored data. Users with limited computing power are more likely to delegate the mask of the decryption task to the servers to reduce the computing cost. During delegation the server might tamper or replace the delegated cipher-text and respond a false transformed cipher-text with malicious intent. They may also cheat the authorized/ eligible user by responding them that they are ineligible for the purpose of cost saving. So, it does not provide security to our data.

IV. PROPOSED SYSTEM

In this we propose, verifiable delegation model for to solve the problem in existing system. It does not allow to cheat authorized user because data owner maintains a secret key without having key you cannot access the data.

A. System Model

In this model the Data Owner Encrypt and upload a file into the server then the resultant file contains Cipher-text. If user wants original file he/she requests Authority to generate private key for decrypt file then authority generates private key to user. By using private key User Decrypt and download the file from server.

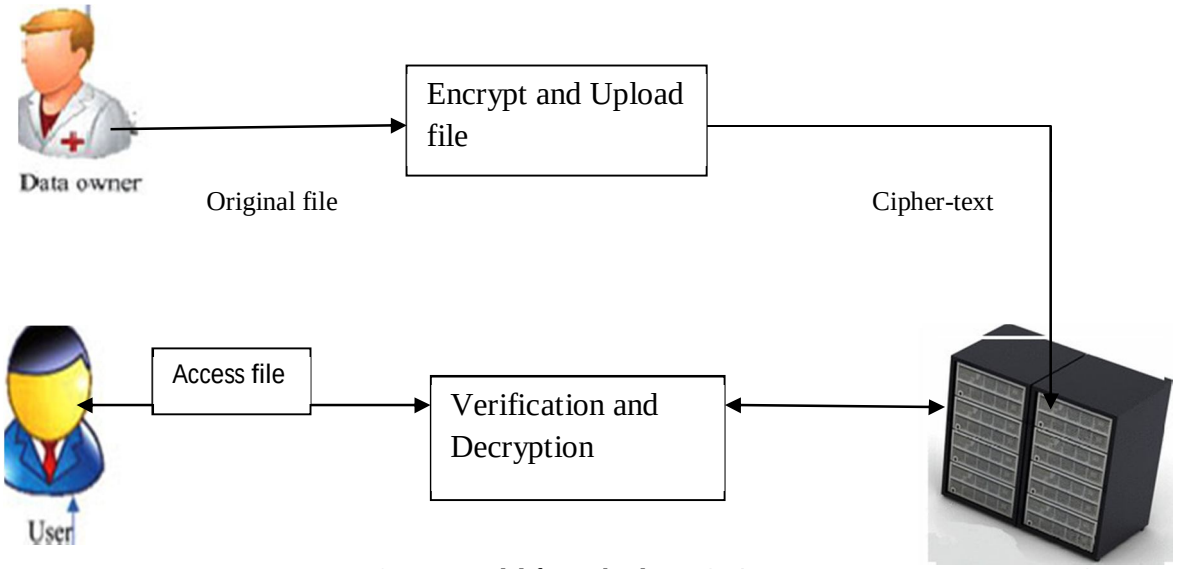


Fig1 : System model for Hybrid VD-CPABE

B. Hybrid VD-CPABE Scheme

Our Hybrid VD-CPABE scheme is having tuple of algorithms. They are

1) *Setup Algorithm:* This algorithm is Executed by the authority, this algorithm takes as input a security parameter λ the number of attributes n. It outputs the public key PK and a master key MK which is kept secret.
2) *Hybrid-Encrypt Algorithm:* Hybrid Encryption is the combination of symmetric and asymmetric encryption. Symmetric encryption means same key i.e., either public or private key can be used for encrypt or decrypt the message. In this project we use asymmetric encryption because it uses one key to encrypt a message and another key to decrypt the message. This Hybrid-Encrypt algorithm is executed by the data owner. Here Data owner encrypt and upload the file into server. The encryption can be done by using public key PK which is the output of setup algorithm. It outputs cipher-text CT.
3) *KeyGen Algorithm:* The authority generates private keys for the users. This algorithm takes as input the master key MK and a bit string x. It outputs a private key SK.

4) Decrypt Algorithm: It is Executed by the user, this algorithm takes as inputs the private key SK and the cipher-text CT. By using private key SK user decrypt the file and it outputs original plaintext.

V. EXPERIMENTAL RESULTS

In this performance analysis graph we show the relationship between the files and their time to upload in server. In this above graph, we consider the file name on x-axis and time count on y-axis from 0 to infinity these values will change dynamically based on the time. If the file size is small the uploading time is less. If the file size is huge then it takes more amount of time to upload file into server. Based on the size of the files only the uploading time will be depended.

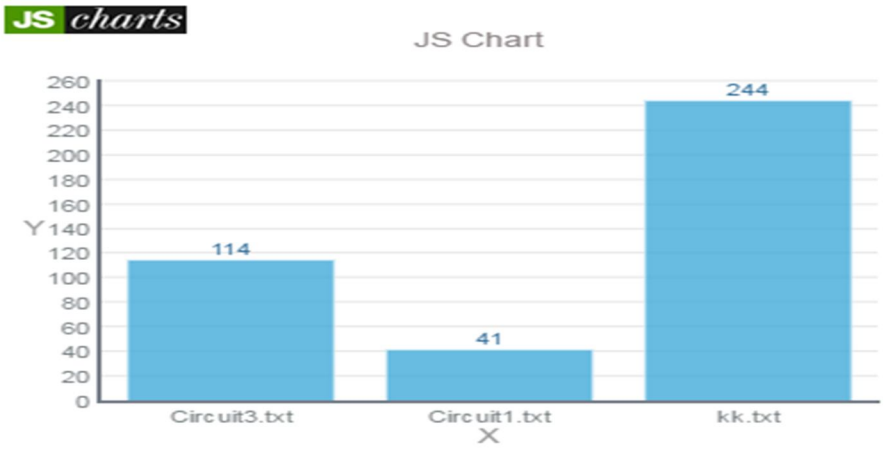


Fig2: Performance Analysis

VI. CONCLUSION

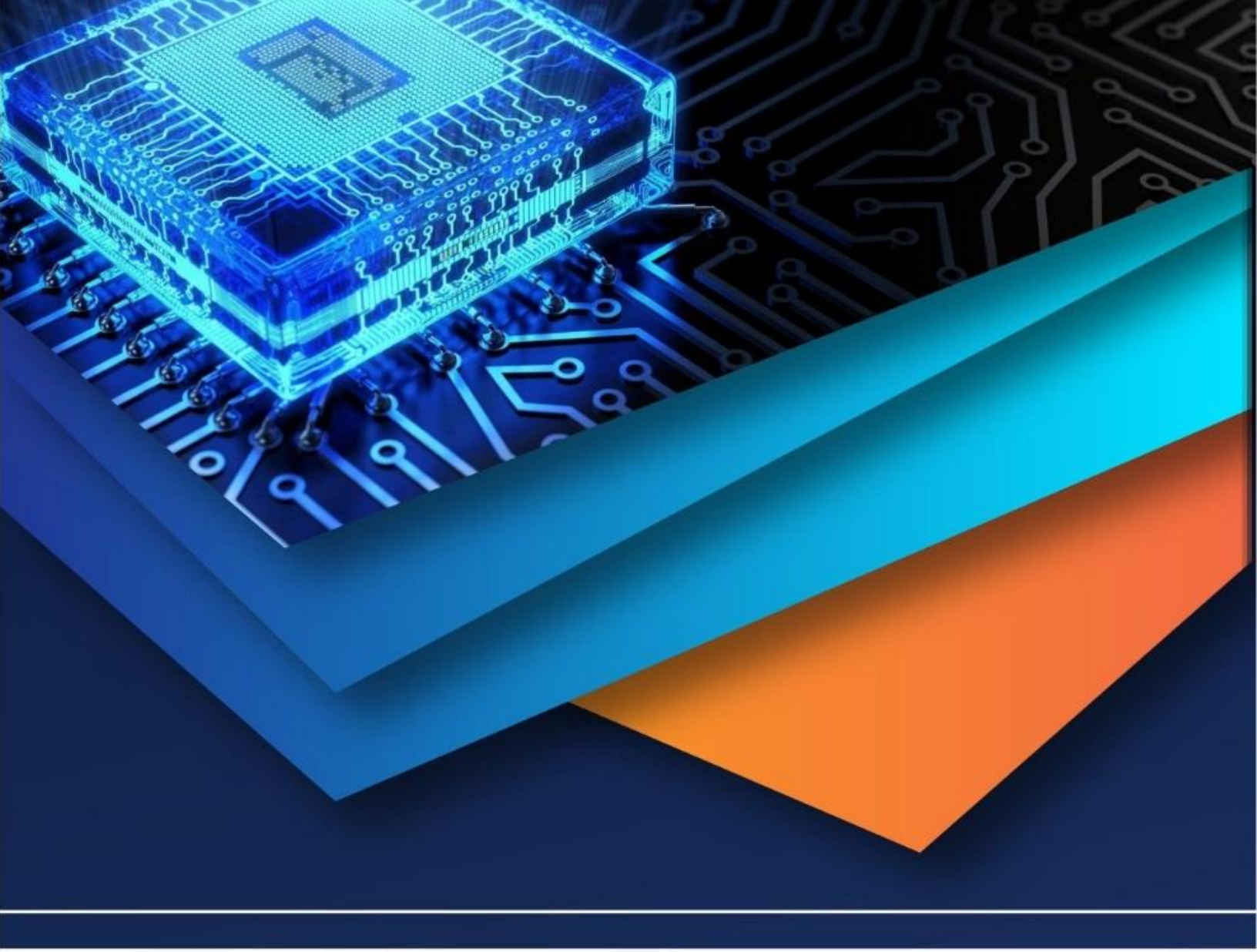
In this paper, we have studied problem is during delegation the server might tamper or replace the delegated cipher-text and respond a forged computing results with malicious intent. They may also cheat the eligible users by responding them. This problem is overcome by using verifiable delegation model. It does not allow to cheat authorized user because data owner maintains a secret key without having the key user cannot access the data. This verifiable delegation model provides security and does not allow unauthorized user. Here also we present verifiable delegation and encryption mechanism with our hybrid encryption, we could delegate the verifiable decryption paradigm to the server.

VII. FUTURE WORK

The future scope of this prt is for security, KEM combines with the IND-CCA (Indistinguishability under selective chosen cipher-text attack)secure authenticated encryption scheme which yields our IND-CPA(Indistinguishability under selective chosen plaintext attack) secure hybrid VD-CPABE scheme. In future we also implement multi-linear decisional Diffie-Hellman assumptions.

REFERENCES

[1] Jie Xu, Qioyan Wen, Wenmin Li and Zhengping Jin " Circuit Ciphertext-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing" JANUARY 2016
[2] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 8, pp. 1343–1354, Aug. 2013.
[3] S. Garg, C. Gentry, S. Halevi, A. Sahai, and B. Waters, "Attribute based encryption for circuits on Lattices," in Proc. 33rd Int. Cryptol. Conf., 2013, pp. 479–499.
[4] J. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 8, pp. 2201–2210, Aug. 2013.
[5] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, Jul. 2011
[6] 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.
[7] 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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY