iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

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

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

Secure Key Management Scheme for Dynamic Hierarchical Access Control Based on ECC

Abinaya M [1], T Sivakumar[2]
[1,2,] Computer Science and Engineering, Anna University, Chennai

Abstract*: Access control is an indispensable security component of cloud computing, and hierarchical access control is of particular interest since in practice one is entitled to different access privileges. This paper presents a hierarchical key assignment scheme based on linear geometry as the solution of flexible and fine grained hierarchical access control in cloud computing. In our scheme, the encryption key of each class in the hierarchy is associated with a private vector and a public vector, and the inner product of the private vector of an class and the public vector of its descendant class can be used to derive the encryption key that descendant class. The proposed scheme belongs to direct access schemes on hierarchical access control, namely each class at a higher level in the hierarchy can directly derive the encryption key of its descendant class without the need of iterative computation. In addition to this basic hierarchical key derivation, we also give a dynamic key management mechanism to efficiently address potential changes in the hierarchy. Our scheme only needs light computations over finite field and provides strong key to distinguishability under the assumption of pseudorandom functions. Furthermore, the simulation shows that our scheme has an optimized trade-off between computations consumption storage space.
Keywords*: Hierarchical Access Control, Elliptic curve cryptography, ECC

I. INTRODUCTION

The scope of many existing system is ABE schemes have a high overhead because of the complexity of realizing the access structure and costly bilinear map operations in addition, attribute revocation is a subtle issue in ABE and requires extra computation and communication costs to deal with, With this in mind, we study the issue of flexible and fine-grained data access control in cloud computing with different primitive: Hierarchical Key Assignment.

A. System Details

1) *Exiting System:* Existing system is ABE scheme have a high overhead because of the complexity of realizing the access structure and costly bilinear map operations. In addition, attribute revocation is a subtle issue in ABE and requires extra computation and communication costs to deal with, With this in mind, we study the issue of flexible and fine-grained data access control in cloud computing with different primitive: Hierarchical Key Assignment. Existing security model of hierarchical key is used as a technique.
2) *Proposed system:* The proposed scheme belongs to direct access schemes on hierarchical access control, namely each class at higher level in the hierarchy can directly derive the encryption key of its descendant class without the need of iterative computation. In addition to this basic hierarchical key derivation, we also give a dynamic key management mechanism to efficiently address potential changes in the hierarchy.

II. SYSTEM ARCHITECTURE

Architecture diagram shows the relationship between different components of system. This diagram is very important to understand the overall concept of system. Architecture diagram is a diagram of a system, in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the block. They are heavily used in the engineering world in hardware design, electronic design, software design, and process flow diagrams.

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

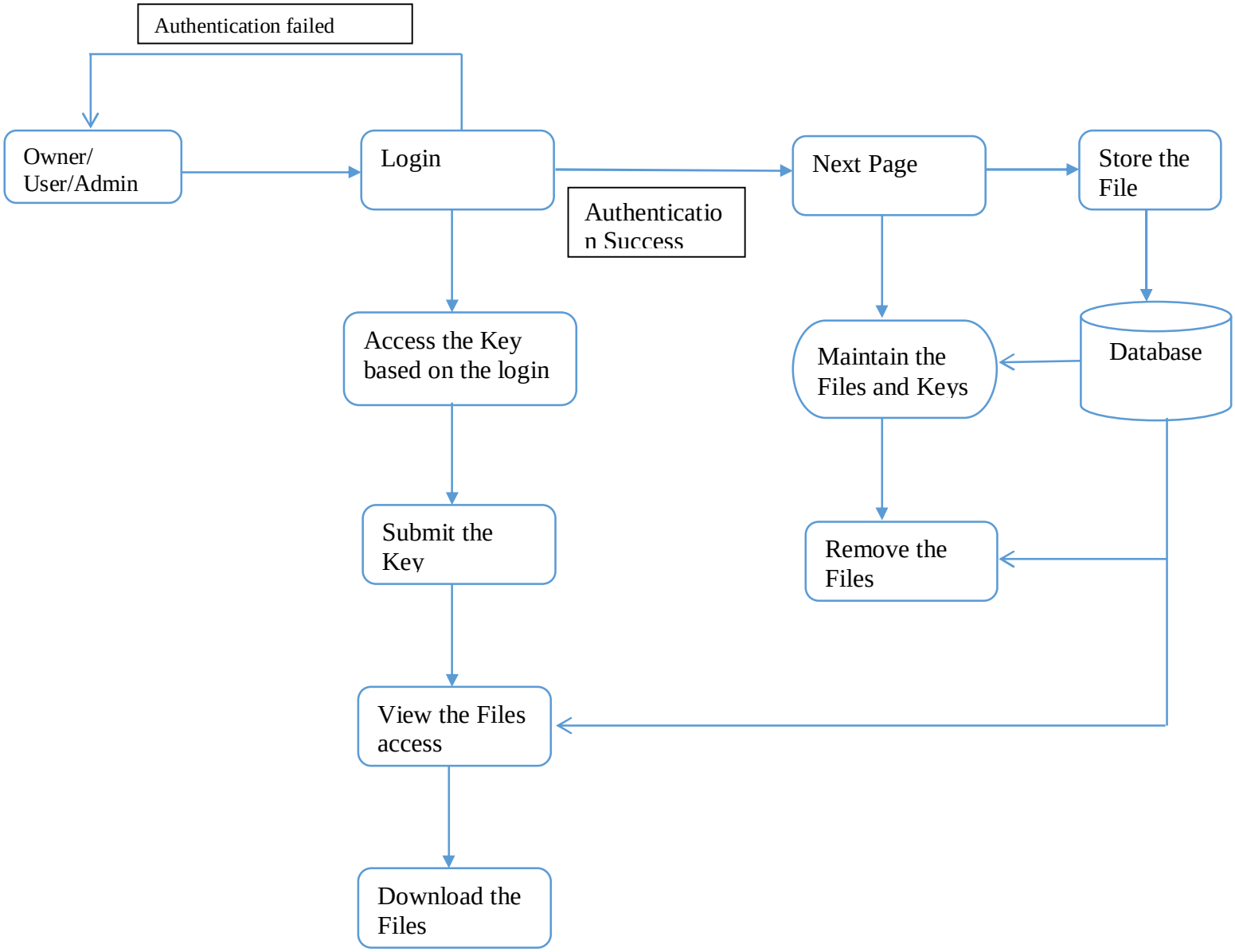


FIGURE 1: SYSTEM ARCHITECTURE

There are three modules present in this architecture . Owner, Users, Admin

A. Owner module

1) Authentication
2) Generate the Public Key
3) Multi Key Generating
4) Upload the Files

B. USER MODULE

1) Authentication
2) Register to Central Authority
3) View the Allocated Files

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

4) Download the Files

C. Admin Module

1) Authentication
2) View the Files
3) Maintaining the Files

III.RESULTS

A. The results are as follows

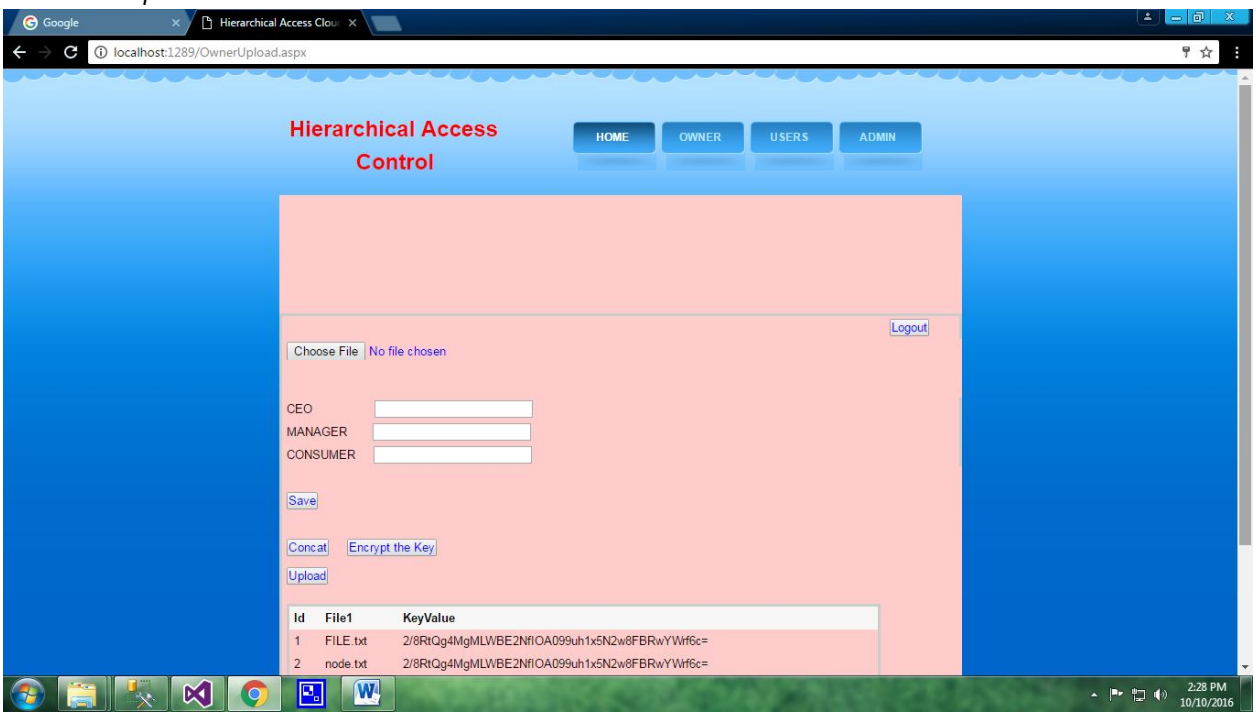


FIGURE 1: FILE UPLOAD

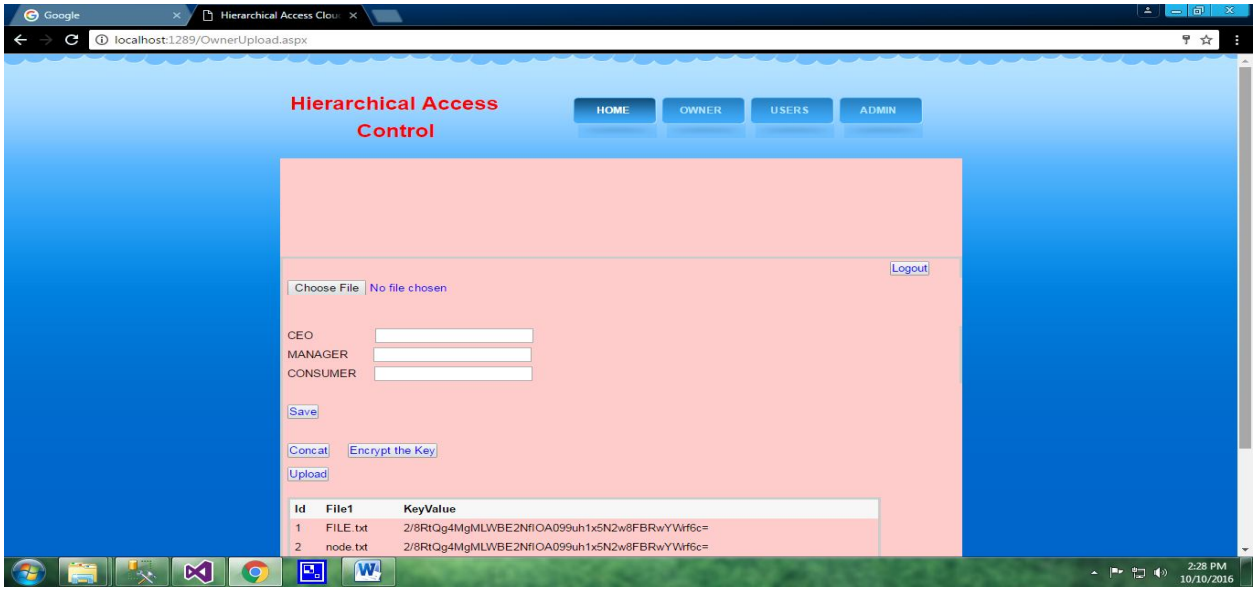


FIGURE 2: KEY GENERATE

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

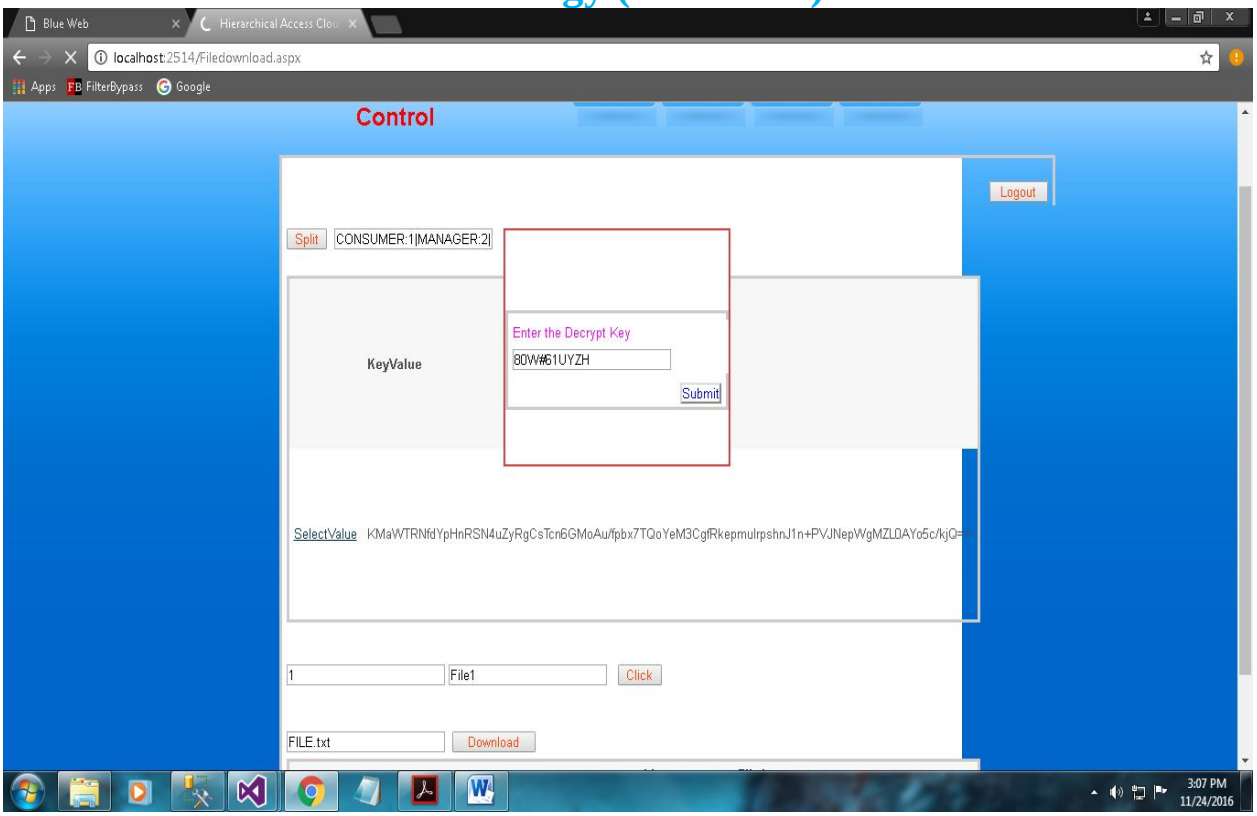


FIGURE 3: FILE DOWNLOAD

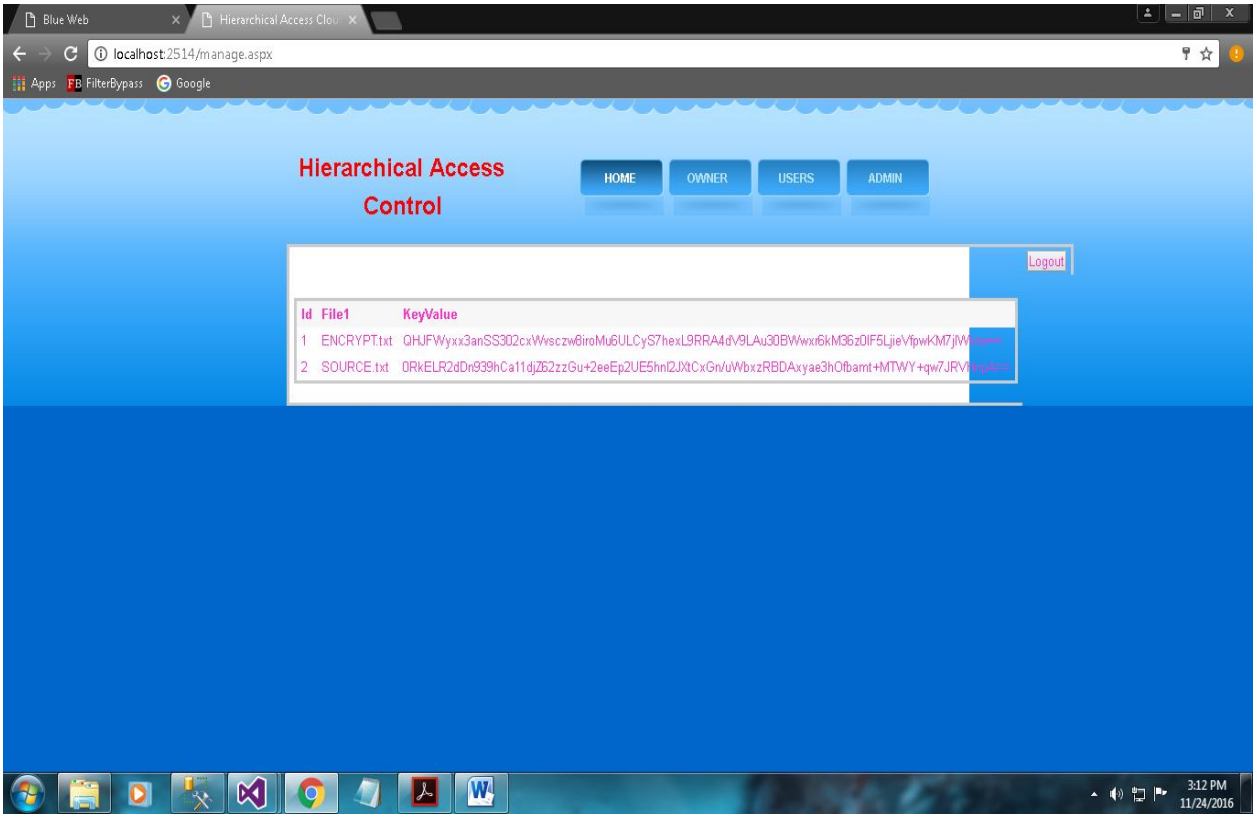


Figure 4: Admin Maintains the Data

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

IV. FUTURE WORK

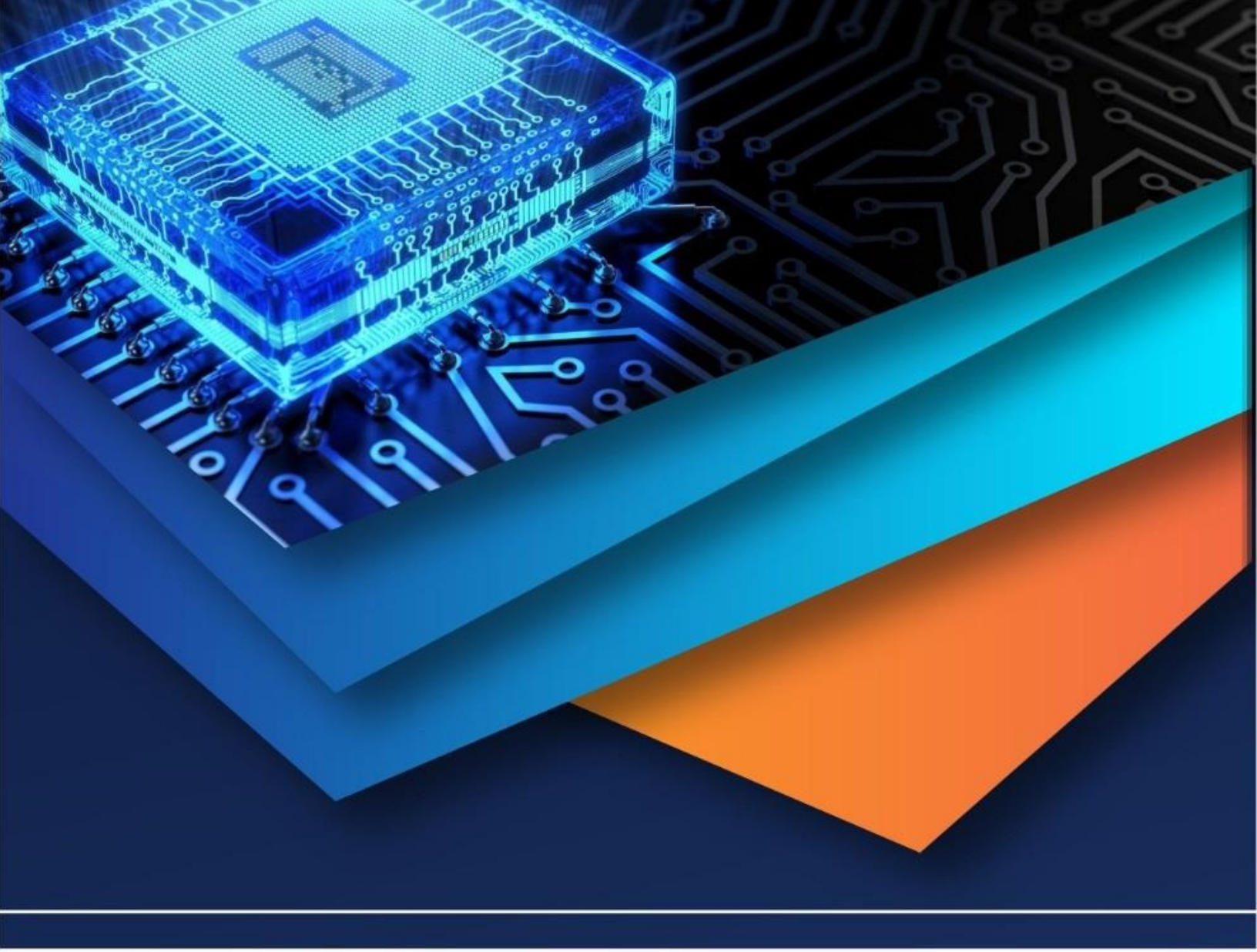
The future concept is the development of group-oriented applications, access control is confronted with the requirement of different and flexible access privileges. Take a multinational corporation as an example, in order to realize efficient data sharing and mobile office, the corporation can outsource all files and data to the cloud. Access control in such a situation has a hierarchical structure. the access to the cloud data requires that ordinary staff can only access the data of their own department, department managers need to access more data than the ordinary staff, and the chief executive officer (CEO) has the supreme seniority and can access all data.

V. CONCLUSION

We presented a new design of hierarchical key assignment based on linear geometry. Our scheme provides hierarchical access because class encryption key can be derived from the inner product of the public vector of that class and the private vector of its ancestor class. We also provided efficient key management solutions to address potential changes in the hierarchy. A formal proof shows that the proposed scheme has the property of strong key in distinguishability under the assumption of pseudorandom functions. Simulations show that our scheme provides an optimized trade-off between computation consumption and storage space, though the size of the public parameter in our scheme is slightly larger than others.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.
[2] K. Yang and X. Jia, “Data storage auditing service in cloud computing: Challenges, methods and opportunities,” World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.
[3] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1–11, 2011.
[4] K. Yang and X. Jia, “Expressive, efficient and revocable data access control for multi-authority cloud storage,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, Jul. 2014.
[5] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. 24th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 457–473.
[6] J.-Y. Huang, C.-K. Chiang, and I.-E. Liao, “An efficient attribute-based encryption and access control scheme for cloud storage environment,” in Proc. 8th Int. Conf. Grid Pervasive Comput., 2013, pp. 453–463.
[7] Z. Wan, J. Liu, and R. H. Deng, “HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing,” IEEE sTrans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY