ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Dynamic Policy Access for Secure Data Sharing

V.Punitha[1], G.Umamaheswari[2], R.Sangeetha[3], N.Tivya[4] , V.Sivashankari[5]

Associate Professor, Dept. of Computer Science, Saranathan College of Engineering, Panjappur, Tiruchiraapalli, India.[1]

B.E Students, Dept. of Computer Science, Saranathan College of Engineering, Panjappur, Tiruchiraapalli, India.[2,3,4,5]

ABSTRACT: Secure data may implicitly contain confidential information. This leads to privacy concerns if the provided information is misused. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This project addresses this issue by using access policies based on data attributes that allow the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted servers without disclosing the underlying data contents. The goal is achieved by exploiting and uniquely combining techniques of attribute-based encryption (ABE) and proxy re-encryption. The proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. The proposed scheme enables the data owner to delegate most of the computation overhead to powerful servers. Confidentiality of user access privilege and user secret key accountability is achieved.

KEYWORDS: Attribute-based encryption, Proxy re-encryption, Fine-grained, Access control, secret key.

I. INTRODUCTION

A security policy specifies session participant requirements. However, existing frame works provide limited facilities for the automated reconciliation of participant policies. This paper considers the limits and methods of reconciliation in a general purpose policy model. The authors identify an algorithm for efficient two-policy reconciliation, and show that, in the worst case, reconciliation of three or more policies is intractable. Further, they suggest efficient heuristics for the detection and resolution of intractable reconciliation. Based upon the policy model, they describe the design and implementation of the policy language. The expressiveness both directly and indirectly of our model, is demonstrated through the representation and exposition of policies supported by existing policy languages. They conclude with brief notes on the integration and enforcement of privacy security policy.

II. RELATED WORK

During business collaborations, multiple participating organizations often need to share data for common interests. In such cases, it is necessary to combine local policies from different organizations into a global one in order to manage access to the shared data. However, local policies of organizations may be different or even conflicting, due to diverse rules and rule combining algorithms chosen. Few existing methods for policy combination are able to automatically combine multiple local policies into a global one. Authors proposed a bottom-up approach to address the issues of multiple policy combinations. The key idea is to first classify the rules based on attribute constraints in each policy, and then reduce the rules of the corresponding classes to one with the same attribute constraints. The reduced rules are then combined into a new global policy by choosing the appropriate rule combining algorithm in XACML. The latter ensures compliance with each of the local policies at syntax and semantic levels. To validate the approach, authors developed a proof-of-concept implementation of the automated policy combination. Experimental results demonstrate that our approach is highly scalable and supports a number of attribute constraints in each local policy.

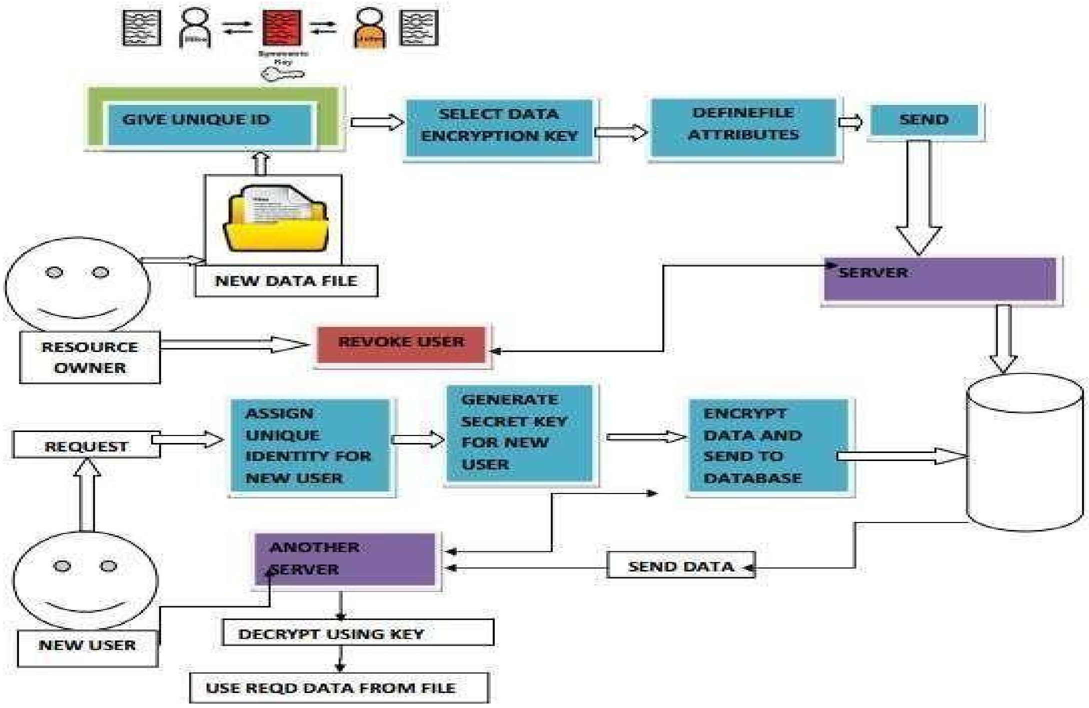
III. EXISTING SYSTEM

The file group-based scheme, on the other hand, is just able to provide coarse-grained data access control. It actually still remains open to simultaneously achieve the goals of fine-grainedness, scalability, and data confidentiality for data access control. Traditional access control architectures usually provide same kind of access permissions to the data owner and other users where the consistency of the data is compromised. Unauthorized users are not able to decrypt since they do not have the data decryption keys. This general method actually has been widely adopted by existing works which aim at securing data storage on untrusted servers. One critical issue with this branch of approaches is how to achieve the desired security goals without introducing a high complexity on key management and data encryption. Any further extension or scaling causes huge costs and defeats the purpose of the dynamic policy access.

IV.PROPOSED SYSTEM

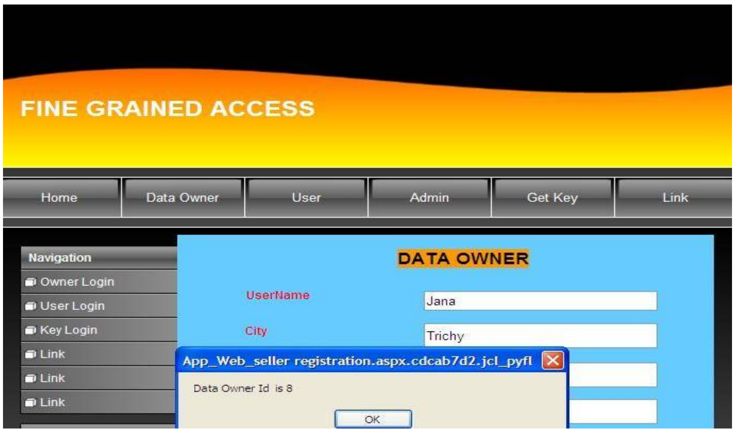
This paper proposes a secure and scalable fine-grained data access control scheme for data sharing. The scheme is partially based on our observation that, 4 in practical application scenarios each data file can be associated with a set of attributes which are meaningful in the context of interest. The access structure of each user can thus be defined over these attributes to reflect the scope of data files that the user is allowed to access. As the access structure is defined, fine-grainedness of data access control is achieved. Such a design also brings about the efficiency benefit, as compared to previous works, in that, 1) the complexity of encryption is just related the number of attributes associated to the data file, and is independent to the number of users in the system. 2) Data file creation/deletion and new user grant operations just affect current file/user without involving system-wide data file update or re-keying. One extremely challenging issue with this design is the implementation of user revocation, which would inevitably require re - encryption of data files accessible to the leaving user, and may need update of secret keys for all the remaining users.

V. SYSTEM ARCHITECTURE



Initially the data owner creates a unique ID for the data file. This file contains the attributes of the user like access rights and information to be shared between the servers. The new user who wants to access is given a unique identity. A unique secret key for this user is generated and sent to the server. Then the key is verified for the user to ensure the secure transmission of the data. If verification fails than the transmission is stopped and further processing is aborted.

VI.RESULTS



UserName: Jana

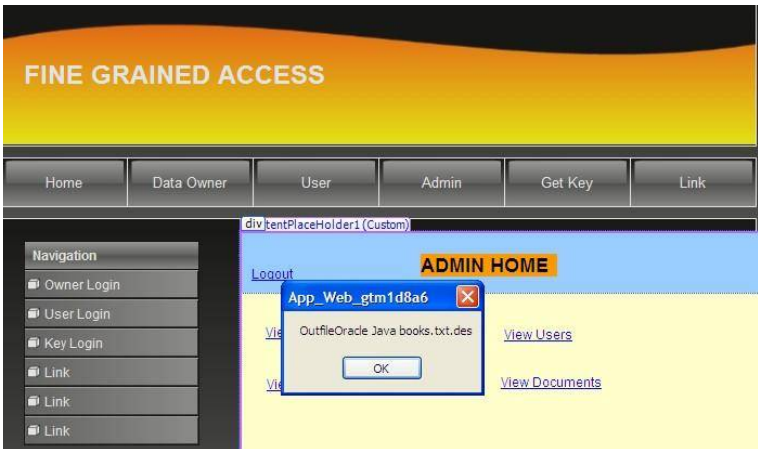
City: Trichy

App_Web_seller registration.aspx.cdcab7d2.jcl_pyfl

Data Owner Id is 8

DATA FILE UNIQUE ID CREATION:

In this module the resource owner creates a unique ID for the data file. This is the file containing the attributes of the user like access rights and information to be shared between the inter servers.



App_Web_gtm1d8a6

OutfileOracle Java books.txt.des

GENERATE DATA ENCRYPTION KEY

Generate a symmetric Data encryption key and encrypt the file. DES algorithm uses the symmetric key to encrypts the data file.

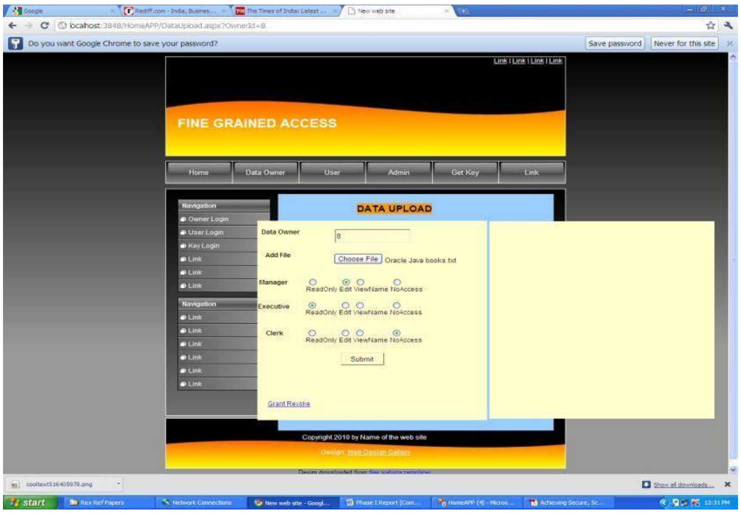
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017



DATA UPLOAD

Data Owner	8
Add File	Choose File Oracle Java books.txt
Manager	○ ReadOnly ● Edit ○ ViewName ○ NoAccess
Executive	● ReadOnly ○ Edit ○ ViewName ○ NoAccess
Clerk	○ ReadOnly ○ Edit ○ ViewName ● NoAccess

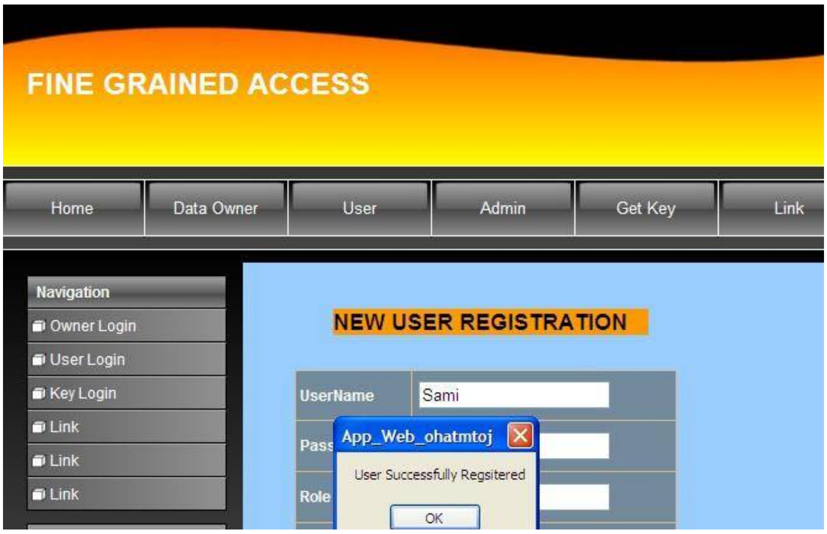
Submit

Grant Revoke

Copyright 2010 by Name of the web site

FILE ATTRIBUTE GENERATION

All the attributes for the data files are generated here by the resource owner. This is then sent to the server to be stored in a specified format with the attributes and data. For each data file the owner assigns a set of meaningful attributes which are necessary for access control. Different data files can have a subset of attributes in common.



NEW USER REGISTRATION

UserName	Sami
Pass	
Role	

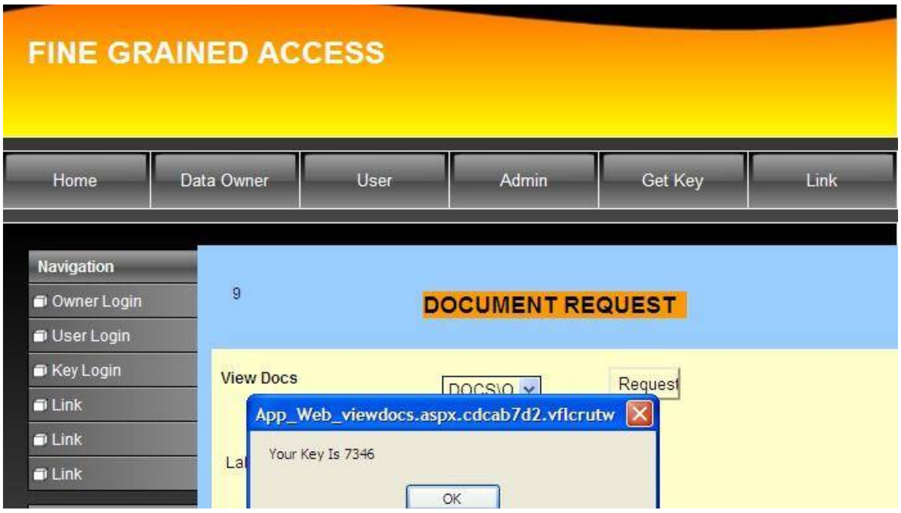
App_Web_ohatmtoj

User Successfully Regsitered

OK

UNIQUE IDENTITY

First the new user who wants to access is given a unique identity.



App_Web_viewdocs.aspx.cdcab7d2.vflcrutw

Your Key Is 7346

KEY GENERATION

A unique secret key for this user is generated and sent to the mail.

VII.CONCLUSION AND FUTURE WORK

In present instant scenario, data confidentiality and scalability have been achieved simultaneously, which is not provided by existing systems. A fined grained data access control on data sharing has been implemented. Proxy re - encryption technique has been used to attain this goal. Confidentiality of user access privilege and user secret key accountability is implemented. Formal security proofs show that our proposed scheme is secure under standard cryptographic models. For further enhancements the project can be enhanced for mobile users and the computing techniques used can be implemented in web services. This will enable the usage of the above implementation in all scenarios in day to day works in the World Wide Web as well.

REFERENCES

1. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,“Scalable secure file sharing on untrusted storage,” in Proc. of FAST’03, 2003.
2. E. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius: Securing remote untrusted storage,” in Proc. of NDSS’03, 2003.
3. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” in Proc. of NDSS’05, 2005.
4.S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, “Over- encryption: Management of access control evolution on outsourced data,” in Proc. of VLDB’07, 2007.
5. V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine- grained access control of encrypted data,” in Proc. Of CCS’06, 2006.
6. M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in Proc. of EUROCRYPT ’98, 1998.
7. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in Proc. of ESORICS ’09, 2009.
8. L. Youseff, M. Butrico, and D. D. Silva, “Toward a unified ontology of cloud computing,”in Proc. of GCE’08, 2008.
9. S. Yu, K. Ren, W. Lou, and J. Li, “Defending against key abuse attacks in kp-abe enabledbroadcast systems,” in Proc. of SECURECOMM’09, 2009.
10. D. Sheridan, “The optimality of a fast CNF conversion and its use with SAT,” in Proc. Of SAT’04, 2004.
11. D. Naor, M. Naor, and J. B. Lotspiech, “Revocation and tracing schemes for stateless receivers,” in Proc. of CRYPTO’01, 2001.
12. M. Atallah, K. Frikken, and M. Blanton, “Dynamic and efficient key management for access hierarchies,” in Proc. of CCS’05, 2005.