IJMTST | Volume: 2 | Issue: 08 | August 2016 | ISSN: 2455-3778

Access Policy Management For OSN Using Network Relationships

Dr. D. Bujji Babu[1] | P. Farhana[2] | Sk. Anjaneyulu[3]

[1, 2, 3]Department of Master of Computer Applications, QIS College of Engineering and Technology, Ongole, Andhra Pradesh, India.

ABSTRACT

In the online social networks (OSN) users and resources are interconnected via various types of relationships. The relationships are one-to-one, one-to-many, many-to-one, and many-to-many like that. Now a day's online social networks plays crucial role to monitor and to control the access of the resources. In the OSN, online provider should be enabled to specify which access permission can be granted in terms of existing relationships. In this work we used user-to-user relationship based access control model. Access control policies decide which permissions can be granted to the requested users based on their requests and we are using two path checking algorithms namely DFS and BFS to determine the path existence between users as well as the requested user is authenticated user or not.

KEYWORDS: *Online Social Networks, Policy, Access Control, Relationship, Management.*

INTRODUCTION

Online social networks have different characteristics like hiding the sensitive data and reveal the private data. . Through OSN, people can connect and share the information to each other. Sharing and communication in online social networks establishes e-relationships. In online social networks people share their ideas and opinions and also their private information.

Online social networks have different characteristics than traditional access control. In this role-based access control and system wide access control is specified by the security administrator. In online social networks prevent users from accessing unwanted user. Access control policies are applied user-to-user-relationships. In online social networks enforce redendency and limited relationship-based access control mechanisms. In this online social networks users want to choose private, public,.

In this we propose user-to-user relationship based access control model to allowing the user and control the policies. In this we present structure of UURAC model.

Decentralizing Attribute-Based Encryption

In this we discuss Multi-Authority Attribute –Based Encryption system. In this any user can have authority in the global. In this ABE can have Authority .ABE can create public key and deliver to private key to two different users.In this user have set of Authorities to encrypt the data by using any other frmula.Finally in this system cannot get any central authority. In this prior Attribute-Based Encryption system achieved collusion resistance

In this different users have different Authority. Each system come with different Authority.ABE creates different techniques to prevent the attacks between the users and global identifiers. By the purpose of using the encryption methods is to prevent the attacks and secure the users data. Not only a single encryption methodology but also *in* this use multiple encryption methodology. first plain test can be converted into cipher test by using one key and then cipher test can be converted into plain test by using another key.

Cipher text-policy Attribute Based Encryption:

In the distributed system user can access the data if and only if user can posses the data. Server can store the data and control the accessing of data. the server is trusted server. If suppose server

store the data can be reveled then confidential data can be revealed. Because of these reason we can encripte the data that encrypted data is nothing but ciphertext.That we call the Cipher text-policy Attribute-Based Encryption

By using these techniques the encrypted can be put confidentiality. If the server is un trusted the confidential data cannot be revealed. In this model the methods we are using are against the attacks. In the previous Attribute-Based Encryption Systems only using attributes to describe the encrypted data. In Attribute-Based Encryption Systems attributes are nothing but users resourses.Attribute-Based Encryption Systems is traditional access control method.

Attribute Based Data Sharing With Attribute Revocation:

In this model data are also encrypted. In Cipher text-policy Attribute Based Encryption(CP-ABE) controlling the data of shared data. In Cipher text policy Attribute Based Encryption users have set of attribute and user contain encrypted data. A user decrypt the plaintext if only the resources of user satisfy and user is authorized.

This paper model overcome the defects of (CP-ABE).In this model the semi-trustable on-line proxy server are available. In this schemes we propose a solution to revoke user attribute with minimal effort. In this we integrate the technique of proxy re-encryption with CP-ABE. In this the techniques are also applicable to Key –Policy Attribute Based Encryption counterpart.

Identity-based Encryption with Efficient Revocation

Identity-based encryption(IBE) is an alternative to publickeyencryption.In this IBE eliminates the public key Infrastructure. In this studding of revocation mechanisms. In this sender use time period when encrypting. Private keys are mainted by trusted authorities.

In this the number of users increases the key updated.IBE schemes increases the efficiency of the trusted party. The basis' of in this model is Fuzzy IBE primitive and binary tree structure.

Provably Secure Cipher text Policy ABE

In cipher text policy attribute-based encryption(CP-ABE) every component associated with set of attributes. Means secret key associated with set of attributes and cipher text associated with set of attribute.Decription method is used to getting the plain text from cipher text.Inthis the fine granted access control is used on sharing data. In CP-ABE scheme study the access structures ,AND gates on positive and negative attributes. This scheme Plain text will be safe undefrDiffie-Hellman(DBDH) assumption.

This paper we getting the cipher text and also for cipher text secure apply the canetti-Halevi technique. In this we also introduce the hierarical attributes to our basic schemes for reducing both cipher text size and encriptpion, derition time.

This system break the traditional model and contain the AND gates on positive and negative gates. The result of this by separating the threshold secret sharing from CP-ABE primitive and we obtain the simple and efficient schems and also secure from complexity assumption.

A cipher test policy attribute-based encryption(CP-ABE)consistsoffourfundamentalalg orithems:Setup,Encript,KeyGen and Decript. Encriptor use AND gate on positive and negative attributes. In this the presenting of smaller cipher texts and faster encryption and decryption operations.

Improving Privacy and Security in Multi-Authority Attribute-Based Encryption

Attribute based encryption (ABE)determines the ability.thatability based on users Attributes. In muti-authority ABE scheme, multiple attribute-authorities monitors are present. that monitor have different set of attributes. In this paper there are different decryption keys issued to the user.

This paper proposed a solution which removes the trusted central Authority. and also protect the user by preventing the pooling and Secure the user data

Fuzzy Identity-Based Encryption

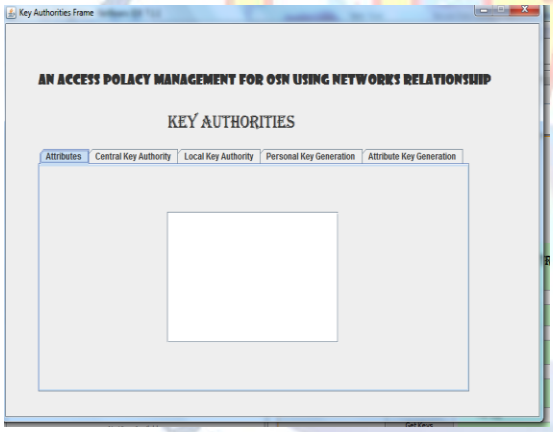
This paper introduce a new type of Identity-Based Encryption Scheme. Name of this Identity-Based Encryption is called Fuzzy. Identity-Based Encription.In this Identity is nothing but set of attributes. This paper taken private key is anthem type identity. Plain text can be encrypted with this identity and cipher text can be decrypt with this identity. It can allow the use of biometric identities. Fuzzy-IBE can be use the one type of application is attribute based encryption. This paper present two constructions. These construction can be viewed as a Identity-Based Encription.This IBE schemes is for both error tolerant. against collisions and errors.

In this Fuzzy Identity-Based Encryption Scheme user have a secret key. In this user can be decrypt the data eith the help of public key. Fuzzy-ABE gives two interesting new applications. First is Identity-Based Encryption system that uses biometric identities. Biometric measurements are nothing but a noisy

Second Fuzzy IBE can be used another application. In this the party that have all Attributes and wish to encrypt a document. the advantages of Fuzzy IBE is document is stored simple and untrusted server instead of trusted server to perform authentication checks before delivering a document. The technique in this construction is users private key as a set of private key component. By the method of shamirs method secret sharing of users private key.Shamirs secret sharing with in the exponent gives our scheme error tolerant. In this private key components are needed to decripthecomponents.

This scheme resistance to collision attacks. In this different users have their private key components.

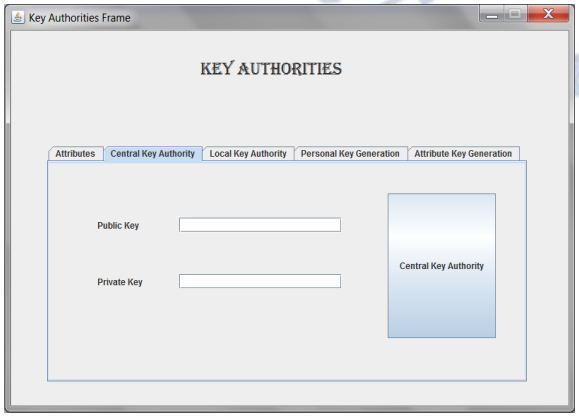
For the implementation of this project we used java Technology and the screens are as follows.



screen 1: home page

Description:

The above screen displays the home page of the key Authorities.



Screen 2: Central key Authority

Description:

The above key Authority is Central key Authority.

Screen 3: Local key Authority

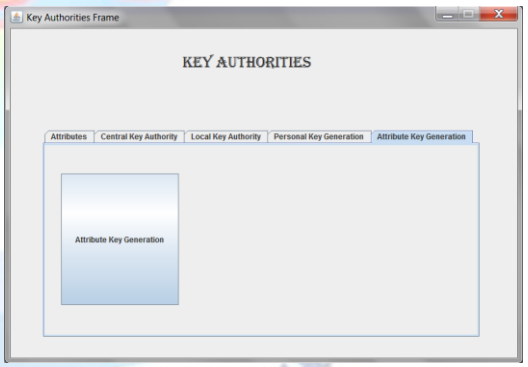
Description:

The above key Authority is local key Authority.

Screen 4: personel key Generation

Description:

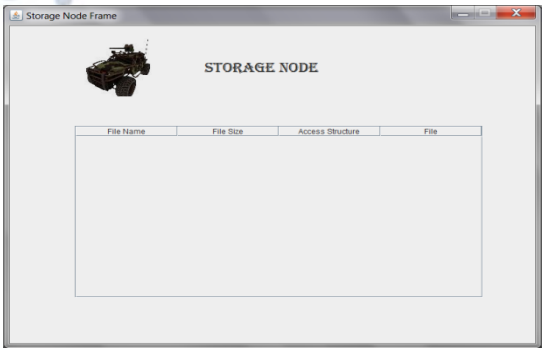
The above key Authority is personal key Generation.



Screen 5: Attribute key

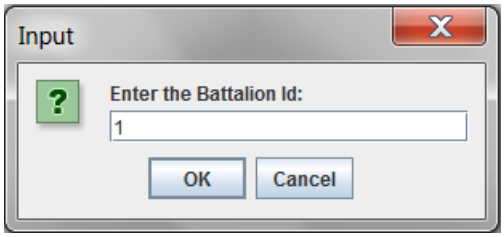
Generation Description:

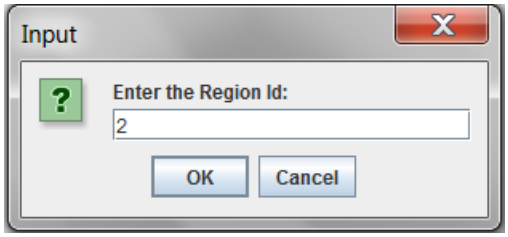
The above key Authority is Attribute key Generation.



Screen 5: Storage Node

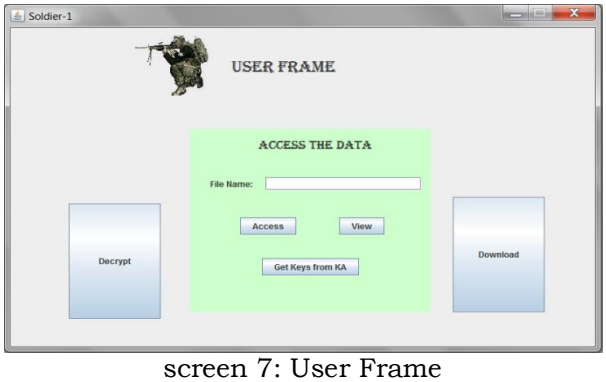
Description:
The above Screen is storage node. It displays the how data is stored.





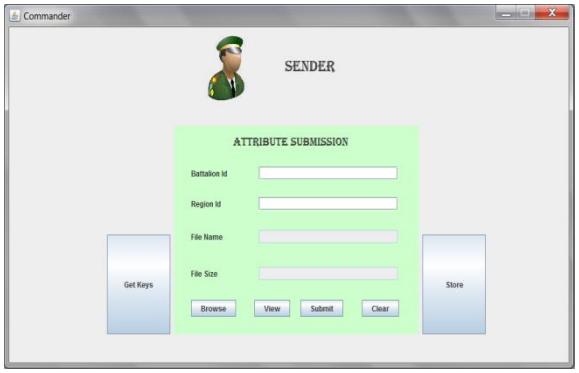
Screen 6: Input Node

Description:
The above Screen shows input we are give to the storage node.



screen 7: User Frame

Description:
The above Screen is User Frame. It displays how user access the data..



Screen 8: Attribute Submission Frame

Description:
The above Screen is Attribute Submission Frame. In this screen sender to check the Authorized person gives the Attribute Submission for the requested file.

Screen 9: Data In Attribute Submision Frame.

Description:
The above Screen is Data In Attribute Submission Frame..It shows the login form.

Screen 10: View Frame

Description:
The above Screen is view frame. It can be click to view the data in the storage node.

Screen 11: Attribute Submitted To KA Frame.

Description:
The above Screen is Attribute Submited to KA Frame..It shows attribute is submitted to Key Authentication

Screen 12:Attributes in KA Frame

Description:
The above Screen is Key Authority frame. It shows the attributes entered by the user.

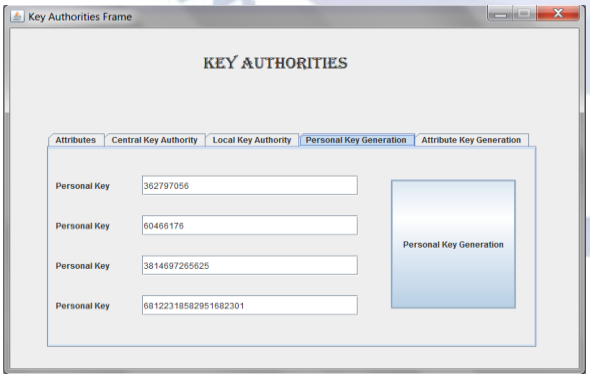
Screen 13: Keys in Central Key Authority Frame

Description:
The above Screen is Keys in Central Key Authority frame. It shows the keys generated by Central key Authority.

Screen 14: Keys in Local Key Authority Frame

Description:

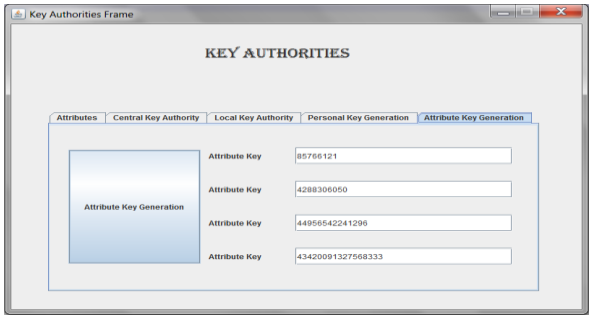
The above Screen is Keys in Local Key Authority frame. It shows the keys generaed by local key Authority



Screen15: Keys In Personal Key Generation Frame

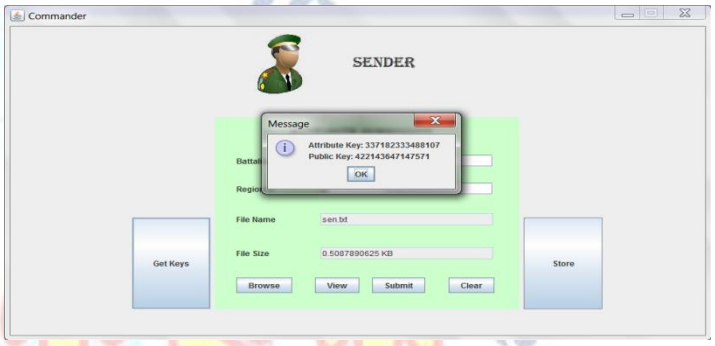
Description:

The above Screen is Keys in personal Authority frame. It shows the keys generated by personnel key generation.



Screen 16:Keys In Attribute Key Generation Frame

Description:
The above Screen is Keys in Attribute Key Generation frame. It shows the keys generated by Attribute key generation.

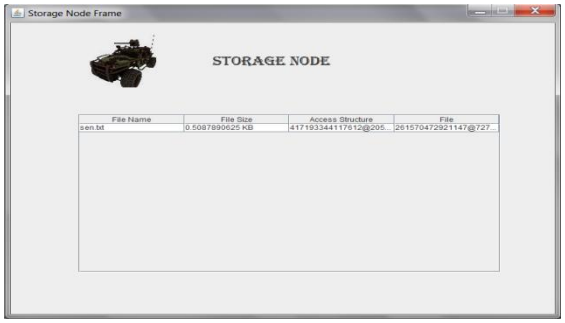


Screen 17: Keys generated to the User

Description:
The above Screen is Keys Generated to the User.It shows the Keys Generaed to the User.

Screen 18:Status Frame

Description:
The above Screen is Status frame. It shows the status of the file.

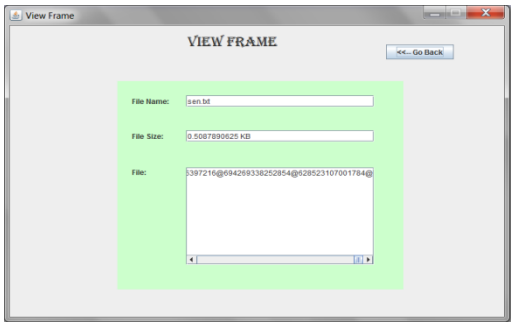


Screen 19: Data Frame

Description:
The above Screen is Data frame. It shows the data in the Storage No**de**

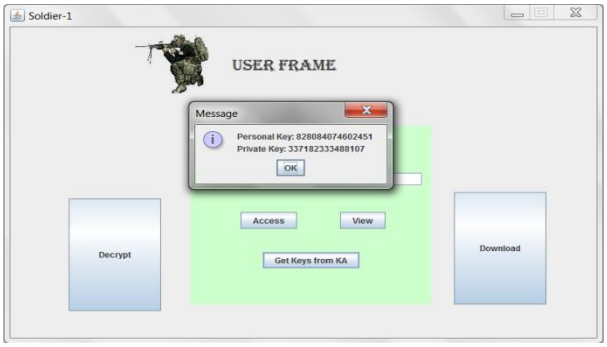
Screen 20: File Accessing

Description:
The above Screen is File Accessing.It shows the accessation of the file



screen 21: Encrypted Data Frame

Description:
The above Screen is Encrypted Data FrameIt shows the Encrypted Data**.**



Screen 22:Getting keys from KA

Description:
The above Screen is Getting Data from KA .Ishows the keys generated by key Authentication to Decript and get the original data.

References

A.Personel Information Privacy Settings Of Online Social Networks and Their Suitability For Mobile Internet Devices

Protecting personal information means privacy is an important issue in online social network providers and users. Social network providers have developed several techniques to decrease threats and risks to the users' privacy. Because of these risks there may be chance ofthefting.the study aims measure to give the awareness to the users to protecting the personnel information to modify privacy settings.servey results show privacy for online social networks need to be improved to support different type of mobile phones screens. Because most users use their mobile phones for Internet services, privacy settings that are compatible with mobile phones be developed. And also the Results of this study can be used to develop a new privacy system which will help users control their personal information easily from different devices, including mobile Internet devices and computers.[5].

B.Intelligent Access Control Polices For Social Network Site

Online Social Networks have been adopted the Relationship-based access control (ReBAC).Authorized policies are specified in these relationships. Sometimes these Relationships are not sufficient. Various Security and Privacy Requirements satisfies to days OSN users. In this we are consider the attribute-based policies and Relationship-based access control.ReBAC enhances the access control capabilities. Finger-grained control are not available in ReBAC.In this User-to-User Relationship-based access control model proposed .In this also present path checking algorithms to determined the relationships and granted the data[3].

C.Attribute-aware Relationship-based Access Control for Online Social Networks?

Online social networks adopted Relation-ship access control authorized policies are specified in these relationships. These relationships increasing security and privacy .In this we integrate attribute-based policies into relationship-based access control. User-to-user relationship-based access control. In this path checking algorithm determine required attributes and relationships in order to grant access.[1].

D. Consumer-Centric Protection for Online Social Networks

Online social networks are constructing and shaped by internet technologies. Internet users use of OSN services to share and celebrate their personal lives with friends and family. OSN services handling privacy-sensitive information. In this paper, we define the notion of Consumer-Centric Protection (CCP) for OSNs.By

using state-of-the-art security and privacy-preserving mechanisms OSN services handling privacy-sensitive information.[7].

E.*Relationship-based Access Control For Online Social Networks; Beyond User-to-User Relationships*

User-to-user relationships based access control .An access control modeling approach in online social networks .online social networks applications allow --various user in this we develop a relationship-based access control model for OSNs.In this (U2U)user-to-user relation ships and resource-to-resource relation ships. most access control proposals for OSNs only focus on controlling users' normal usage activities. Authorization policies are defined in terms of patterns of relationship. We also provide simple specifications of conflict resolution policies to resolve possible conflicts among authorization policies[4].

F.Towards Implicit Contextual Integrity

Online social networks need mechanisms need mechanisms .those mechanisms manage interactions and increasing the awareness of different contexts and also preventing users from exchanging inappropriate information. Privacy theory that expresses the appropriateness of information sharing[6].

G. Towards Provenance and Risk-Awareness in Social Computing

Social computing has been growing phenomenally. Social computing is appropriate way of protecting the security and privacy of data shared in the system. Social computing mainly on predefined access control policies to achieve authorization statically. Social computing unsuitable for capturing the dynamic changes in social environment[2].

Conclusion

DTN technologies are used in military application. In miltrey application it allows wireless devices by the purpose of to share the confidential information and communicate one to another. In this CP-ABE provide cryptographical solution these solution is for to access the data and control the data, secure the confidential data like those types of issues. In this we propose a secure data retrieval method using CP-ABE. For decryption in this we use multiple key authorities to manage the data and attributes independently. Inherent key escrow problem is resolved such that to provide confidentiality to data. Even if there is hostile environment the granted data securely stored. In this fine granted key revocation can be done for each attribute.

We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Acknowledgment

The satisfaction that accompanies the successful completion of the project would be incomplete without the mention of the people who made it possible. I consider it my privilege to express my gratitude and respect to all those who guided and nspired in the successful completion of my project. I am grateful to our college secretary and correspondent Sri. N.S. Kalyan Chakravathi and the president of this SNES Sri. N. Nageswara Rao, for providing me an opportunity to utilize the infrastructural facilities and computational facilities at QIS College of Engineering and Technology, Ongole and allowing availing the entire faculty in the college.

References

[1] A.LewkoandB.Water"Decentralizingattributebasedencryption,"ptology ePrint Archive: Rep. 2010/351, 2010.2007, pp. 321–334

[2] J. Bethencourt, A. Sahai, and B. Waters," Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. ASIACCS, 2010, pp. 261–270.

[4] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-basedencryptionwith efficient revocation," in Proc. ACM Conf. Computer. Community. Security, 2008, pp. 417–426

[5] .L. Cheung and C. Newport, "Provably secure cipher text policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.

[6] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005, pp. 457–473