Leveraging the Privacy Applications by Improving the Confidentiality in Facebook

S. S. Soorya[1], D. Saravanan[2]
[1]Student/CSE, PavendarBharathidasan College of Engineering & Technology, Trichy ,TAMILNADU, INDIA
[2]HOD/CSE, PavendarBharathidasan College of Engineering & Technology, Trichy, TAMILNADU, INDIA

Abstract- **This project enhances existing system and introduces new social network privacy management models. A mechanism of cryptography technique is used to obtain this objective. By applying the key concept the privacy and security is achieved. RSA algorithm of cryptography technique applies the encryption and decryption methods on the user publishing files which provide the way to securely transact the desired data to the recipient. Key concept enables the user to create group, create cloud, upload files, and assign private keys to the group members. This helps the member in a particular group can view the encrypted transmitted file using the private key.**

Keywords: RSA, RBAC, SNS, API, Online social network, Facebook

I.INTRODUCTION

Moreover, when there is adequate information, short-term benefits are often opted over long-term privacy. However, contrary to common belief, people are concerned about privacy. But managing ones privacy can be challenging. This can be attributed to many things, for example, the lack of privacy controls available to the user, the complexity of using the controls, and the burden associated with managing these

Social networking sites are experiencing tremendous adoption and growth. This trend is increasing for all age groups. These technologies have become and will continue to be a vital component of our social fabric. There are tremendous amount of users online, there is also a tremendous amount of user profile data and content online, new content is being added every day. This large amount of content coupled with the significant number of users online makes maintaining appropriate levels of privacy very challenging. There are varying levels of privacy controls, depending on the online site. For example, some sites make available user profile data to the Internet with no ability to restrict access. While other sites limit user profile viewing to just trust friends. Individuals voice concerns over the lack of adequate controls around their privacy information while freely providing their personal data. Other research concludes that individuals lack appropriate
information to make informed privacy decisions.

controls for large sets of users. Security unaware users typically follow an open and permissive default policy. As a result, the potential for unwanted information leakage is great.

One approach that has been taken to alleviate the burden of managing access permissions for large sets of friends is the implementation of a role-based access control model (RBAC). Role-based access control provides

a level of abstraction with the introduction of a role between the subject and the object permission. A role is a container with a functional meaning, for example, a specific job within an enterprise. Permissions to objects are assigned to roles and subjects are assigned to roles. Role members are granted object permissions associated with the role(s) in which they belong. This level of abstraction alleviates the burden of managing large numbers of subjects to object permissions assignments.

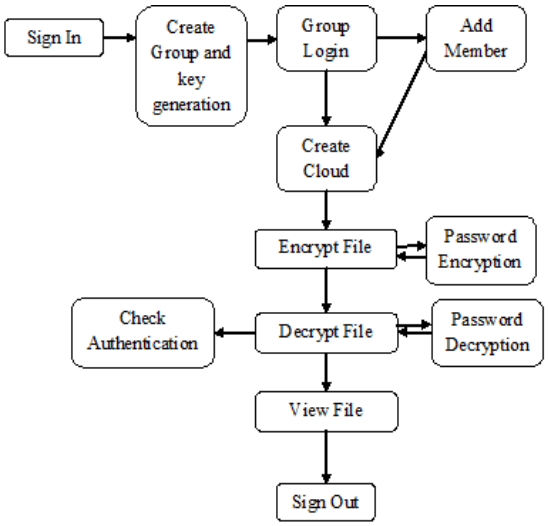

Fig 1 System Architecture

II RBAC MODEL:

Role-based access control provides a level of abstraction with the introduction of a role between the subject and the object permission. A role is a container with a functional meaning, for example, a specific job within an enterprise. Permissions to objects are assigned to roles and subjects are assigned to roles. Role members are granted object permissions associated with the roles in which they belong. This level of abstraction alleviates the burden of managing large numbers of subjects to object permissions assignments.

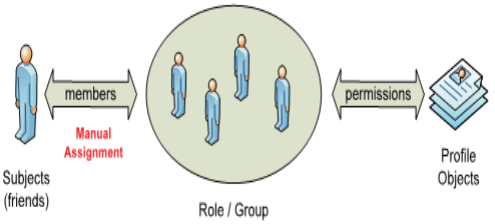

Fig 2 RBAC model

III EXISTING SYSTEM

Collective Privacy Management in Social Networks discussed a novel model for privacy management across social networks, where data may belong to many users. Social network sites make available user profile data to the Internet with no ability to restrict access. While other sites limit user profile viewing to just trust friends. Other studies introduce the notion of the privacy paradox, the relationship between individual privacy to disclose their personal information and their actual behavior. Other research concludes that individuals lack appropriate information to make informed privacy decisions.

- It Concentrate only on behavioral things.
- Some privacy policies are difficult to manage.
- Some privacy policy tools are complex to handle.
- No effort was made to determine whether information revealed by users in social networking sites was accurate.

IV PROPOSED SYSTEM

Friend grouping mechanism enhances traditional group-based policy management approaches in two areas. Provides the user with assistance in grouping their friends and provides the user the ability to set friend-level exceptions within the group policy. Proposed system introduces the cryptography algorithm for secure

data transmission. Enables the permitted persons can see the uploaded information using randomly generated keys.

- Helps users to group their friends more effectively.
- Share keys among the group efficiently.
- Allow only the specified persons to view posted data.

V SIMULATION SETUP AND RESULT

The simulation is done in ASP.Net with C# and the datas are maintained under using database SQL Server 2005. The scope of this project is to develop a demonstration of facebook application where the user is authenticated using login module, then invite their friends and accept friend requests for grouping friend module. By using randomly generated key value data is uploaded in the encrypted format then the uploaded data is allowed to view only those have the key value.

In user registration and login, only the registered user can able to login the social network for example here demonstration of facebook is used. This registration is for user authentication. Enables the user to register their details before login into the application. Takes inputs as Username, UserId, Password, and IPaddress. Logged user redirected into the Create Group module.

Fig No 3 Registration Form

Fig No 4 Login Form

It redirected to create group and key generation, in which here enables the user to create group for sharing files among the group. A user can create many number of groups, the one who creates the group is the owner of that group. For each group there will be a public key is generated. Once the group is created the group owner is redirected to login into the group for further processing.

Fig No 5 Creation of Group

The group login enables the owner to login into the group. The logged owner adds registered users into the group. For each newly added member there will be a private key is generated. By using that private key, member of that group can get access to the shared file by the owner.

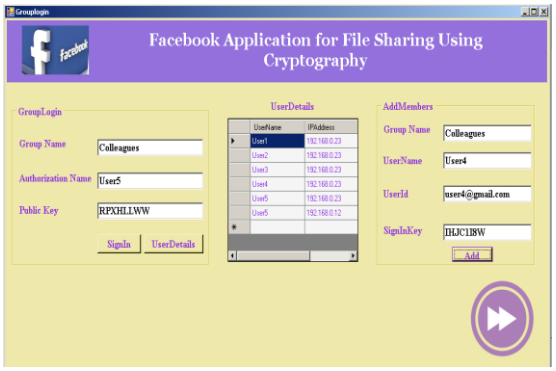

Fig No 6 Creation of Group Login

Then it redirected to create cloud which creates a specific location to store the file which is to be encrypted. Here the user who has public key allowed to upload files into the storage area. Then the stored files are used for the encryption process.

Fig No 7 Creation of Cloud

Then the file encryption and file decryption, In this the files are loaded for encryption process. Cryptography technique of RSA algorithm does the process of encryption on the loaded file. The encryption process takes password as a user input to encrypt the file along with that password. Then it utilizes the decryption process of RSA algorithm. Encrypted file is decrypted here. Before the user get into the decryption process the user is validated for authentication. Only the authenticated user allows to decrypts the file. Password applied for encryption is needed here to decrypt.

Fig No 8 Decrypted Form

Fig No 9 Encrypted Form

VI SUMMARIES

This project utilizes the concept of Cryptography technique for privacy management. Cryptography technique of RSA algorithm is used in this project. Symmetric key applies same key for both encryption and decryption process. Use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. It is less costly than the asymmetric one. Encryption method of RSA algorithm does the process of encrypting user uploaded file into non-human readable format. Password is assigned for security concern so that while transmitting data via network it is hard to the hijackers to hack the data. Decryption method of RSA algorithm does the process of decrypting the encrypted file.

VI CONCLUSION AND FUTURE ENHANCEMENT

This project, enhance existing and introduce new privacy management models. Login module ensures the authentication of a user. Create group and key generation module enables the user to create group and add members to the group. Create cloud module creates a specific location to store the file which is to be encrypted. RSA algorithm efficiently handled to encrypt and decrypt the file for secure transmission. Further study might involve enhancing the privacy in different way and sharing data securely by using different cryptography algorithm.

The privacy for existing is upon in viewing the image efficiently. Here using the symmetric key that is same key for both encryption and decryption techniques. Further the asymmetric key will be used, by implementing different techniques and algorithm for viewing video and audio file format.

REFERENCES:

[1] Clauset A, Newman M, and Moore C (2004), 'Finding Community Structure in Very Large Networks,' Physical Rev. E, vol. 70, p. 066111.

[2] Acquisti A and Gross R (2006), 'Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook,' Proc. Sixth Int'l Conf. Privacy Enhancing Technologies (PET '06).

[3] Jones S and Neill E O (2010), 'Feasibility of Structural Network Clustering for Group-Based Privacy Control in Social Networks,' Proc. Symp. Usable Privacy and Security.

[4] Yuksel A S, Yuksel M E, and Zaim A H(2010), 'An Approach for Protecting Privacy on Social Networks,' Proc. Conf. Systems and Networks Comm.

[5] Fong P W (2011), 'Relationship-Based Access Control: Protection Model and Policy Language,' Proc. Conf. Data and Application Security and Privacy.

[6] Alessandro Acquisti, Jens Grossklags (2005),' Privacy and Rationality in Individual Decision Making', IEEE Security and Privacy, vol.3, no. 1, pp. 26-33.

[7] Besmer A, Watson J, and Lipford H R (2010), 'The Impact of Social Navigation on Privacy Policy Configuration', Proc.Symp.Usable Privacy and Security

[8] Carminati B, Ferrari E, Heatherly R, Kantarcioglu M, and Thuraisingham B M (2011), 'Semantic Web-Based Social Network Access Control', Computers and Security, vol.30, pp.108-115.

[9] Cheng Y, Park J, and Sandhu R S (2012), 'A User-to-User Relationship Based Access Control Model for Online Social Networks,' Proc. 26th Ann. IFIP WG 11.3 Conf. Data and Applications Security and Privacy.

[10] Newman M E J (2004), 'Fast Algorithm for Detecting Community Structure in Networks,' Physical Rev. E, vol. 69, article 066133.

[11] Dunphy P, Heiner A P, and Asokan N, (2010),'A Closer Look at Recognition-Based Graphical Passwords on Mobile Devices,' Proc. Symp. Usable Privacy and Security.

[12] Fang L and K. LeFevre (2010), 'Privacy Wizards for Social Networking Sites,' Proc. Conf. World Wide Web.

[13] Krasnova H, Gunther O, Spiekermann S, and Koroleva K (2009), 'Privacy Concerns and Identity in Online Social Networks,' Identity in the Information Soc., vol. 2, no. 1, pp. 39-63.

[14] Lipford H R, Watson J, Whitney M, Froiland, K and Reeder R W(2010), 'Visual versus Compact: A Comparison of Privacy Policy Interfaces,' Proc. SIGCHI Conf. Human Factors in Computing Systems.