Strengthen Privacy by Policy Generation & Secure Access on Content Sharing Sites

[1]Nada M. Sayed, [2]Prof. Deepali M. Khatwar
Computer Science and Engineering,
RTMNU University, Agnihotri College of Engineering,
Nagthana Road, Sindi(Meghe), Wardha, Maharashtra, India
[1]*nadathefriendly.sayed11@gmail.com*
[2]*deepalikhatwar@gmail.com*

Abstract:-Creating privacy controls for social networks that are both expressive and usable is a major challenge. Lack of user understanding of privacy settings can lead to unwanted disclosure of private information and, in some cases, to material harm. In light of these incidents, the need of tools to help users control access to their shared content is apparent. Toward addressing this need, we propose a Policy Hardening system to help users compose privacy settings for not only their images but securing each and every type of uploaded file. Dynamic groups are generated with particular policies of each group for secure access of files. We examine the role of social context, file content, and policies as possible indicators of users' privacy preferences. We propose a policy framework where user can upload all kind of files and provide different policies with different users.

Keywords: *Policy generation, dynamic group creation, encryption, access control*

*****

I. INTRODUCTION

Configuring privacy in a social network is a challenging usability problem for several reasons. Even with dramatic improvements in usability, privacy suffers from the secondary goal problem [7]; users will always prefer connecting with their friends on social networks to managing access control lists. Web-crawls and user surveys have estimated that over 80% of social network users do not change their privacy settings at all from the default [1, 5] and less than 1% of users opt-out of several obscure privacy-violating features on Facebook [2].

In addition, social networks are a rapidly evolving technology and new features are constantly introduced. Often, all users are opted-in to these features despite their adverse privacy implications [2], meaning that users must frequently update their settings to maintain control of their data. Despite these problems, we find evidence that users do want better control of their privacy. The majority of users city privacy as a concern. We present two methodologies for enhancing security arrangement administration in online substance sharing destinations. To begin with, we present a component utilizing demonstrated bunching systems that helps clients in gathering their companions for gathering based strategy administration approaches. Second, we present an arrangement administration approach that influences a client's memory and supposition of their companions to set strategies for other comparative companions. Next, we aim to provide an improved approach for managing access to user data. 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)[11].

II. RELATED WORK

Most content sharing websites allow users to enter their privacy preferences. Unfortunately, recent studies have shown that users struggle to set up and maintain such privacy settings. One of the main reasons provided is that given the amount of shared information this process can be tedious and error-prone. Therefore, many have acknowledged the need of policy recommendation systems which can assist users to easily and properly configure privacy settings. Anna Cinzia Squicciarini developed an Adaptive Privacy Policy Prediction (A3P) [1] system, a free privacy settings system by automatically generating personalized policies. The A3P system handles user uploaded images based on the person's personal characteristics and images content and metadata. The A3P system consists of two components: A3P Core and A3P Social. When a user uploads an image, the image will be first sent to the A3P-core. The A3P-core classifies the image and determines whether there is a need to invoke the A3P-social. The disadvantage is inaccurate privacy policy generation in case of the absence of meta data information about the images. Also manual creation of meta data log data information leads to inaccurate classification and also violation privacy.

K. Strater and H. Lipford studies that online social networking communities such as Facebook and MySpace are extremely popular. These sites have changed how many people develop and maintain relationships through posting and sharing personal information. The amount and depth of these personal disclosures have raised concerns regarding online privacy. They expand upon previous research on users' under-utilization of available privacy options by examining users' current strategies for maintaining their privacy, and where those strategies fail, on the online social network site Facebook. Their results demonstrate the need for mechanisms that provide awareness of the privacy impact of users' daily interactions.[12]

Jonathan Anderson proposed a paradigm called Privacy Suites [2] which allows users to easily choose "suites" of privacy settings. A privacy suite can be created by an expert using privacy programming. Privacy Suites could also be created directly through existing configuration UIs or exporting them to the abstract format. The privacy

suite is distributed through existing distribution channels to the members of the social sites. The disadvantage of a rich programming language is less understandability for end users. Given a sufficiently high-level language and good coding practice, motivated users should be able to verify a Privacy Suite. The main goal is transparency, which is essential for convincing influential users that it is safe to use. Kambiz Ghazinour designed a recommender system known as YourPrivacyProtector [4] that understands the social net behavior of their privacy settings and recommending reasonable privacy options. It uses user's personal profile, User's interests and User's privacy settings on photo albums as parameters and with the help of these parameters the system constructs the personal profile of the user. It automatically learned for a given profile of users and assign the privacy options. It allows users to see their current privacy settings on their social network profile, namely Facebook, and monitors and detects the possible privacy risks. Based on the risks it adopts the necessary privacy settings.

III. PROPOSED SYSTEM

The proposed work is planned to be carried out in the following manner.

The figure shows the architecture of the content sharing sites. Firstly the user will upload a file which he wants to share in the group and the file can be any file may be text based or the multimedia based. The most important task is to encrypt the file before sharing so that anyone in the middle cannot misuse the file. And then the encrypted file is shared with only those group members which the user selects. The file once decided then the privacy policy will be created on that file. There can be two options to create a policy. The user can create a new policy or he can refer the policy defined previously. After policy creation the user will select the members from the group which he wants to share the file with.

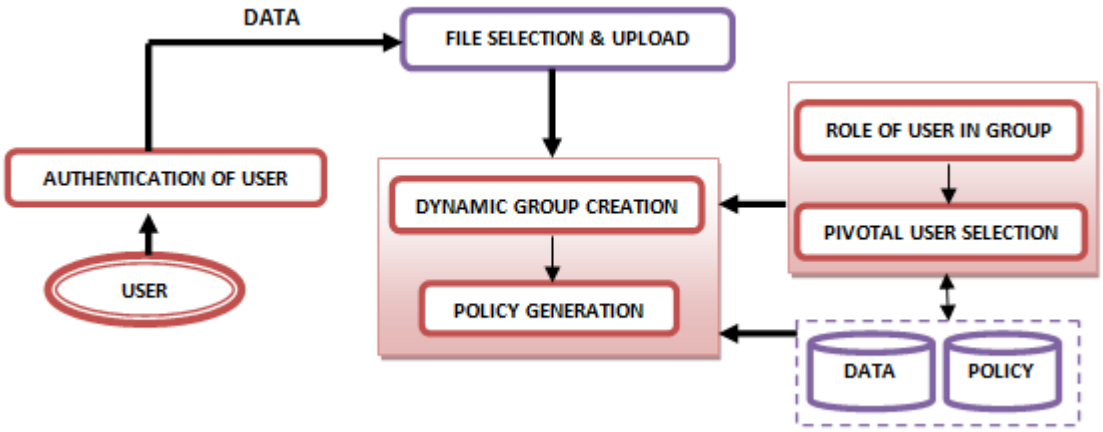

Figure 1: Architecture of Proposed Work

- **Modules:**

1. **Authentication User:** The authentication of the user is done to check whether the user or employee who I being added in the organization is a valid person or not. The authentication process of the user includes the mailing facility. The email id entered by the administrator is been verified by sending the mail to that user. And the email contains the password by which the new user can login into the system. In this way the new user or employee is been authenticated.
2. **Mailing facility**: This module provides us with the mail facility. This module is connected with the authentication module of the user. Whenever the new employee or user gets added in the organization the notification mail is been send to his email id for authentication purpose. The temporary password is been send in that email by which the new user can login to the system and update the new password.
3. **File hosting on server (File Management):** The file management is also the main aspect of the architecture. The file management includes the uploading of a file, downloading of a file and locking a file. Any user/member of the group can upload and download a file from the database. The lock on the file is also provided so that the multiple users can't be able to write the file simultaneously with the help of locks.
4. **File cryptography:** The files uploaded by the employees in the system can be any type of file. To keep the file safe from the unauthorized access, the file or document uploaded in encrypted using an encryption algorithm AES 256. This algorithm is used for encrypting a file and storing the file in ZIP format in the server or the database.
5. **Dynamic group creation:** This is a new feature which is implemented in our project. The group creation in our system is done dynamically which saves the time as compared to the simple static creation. The list of users appears when the group creation is to be done. Numbers of users which are authenticated are only visible in the list. Then the employee or user who wants to share a file with the members in the organization, then the user will select only that particular members and create a new dynamic group.
6. **Policy generation:** The policies are nothing but the permissions which are given on the file for the limited accessing of it. The access rights are decided by the

three permissions that are read, write and delete. Each file hosted or uploaded on the server is assigned with the access rights.

7. **Concurrency control and lock mechanism:** The concurrency control is the concept where multiple users are present at the same time to use the data of centralized database. And to prevent the corruption of the file, the concurrency control system is used. It enables only one user to write the data at a time, multiple users are not allowed to write the same file simultaneously. The reading of the same file by the multiple users simultaneously is allowed, but the writing of file is not allowed.

8.

- **Algorithms**

1. **AES 256 Encryption Algorithm:** The Advanced Encryption Standard (AES) is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world for sensitive data encryption. In AES encryption process, it uses different round keys. These keys are applied along with other mathematical operations on an array of data. This data is present in blocks of particular size. This array is called state array. This encryption process includes following process:
   1. First derive the different round keys from cipher key.
   2. Initialize the state array with block data or plaintext.
   3. Start with initial state array by adding round key.
   4. Perform the process of state manipulation in nine rounds.
   5. After tenth round of manipulation, we will get the final output as cipher text.

   By following above process we get the final encrypted text or cipher text.
2. **MD5 Hash Function:** The algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA. The MD5 algorithm is designed to be quite fast on 32-bit machines. In addition, the MD5 algorithm does not require any large substitution tables; the algorithm can be coded quite compactly.

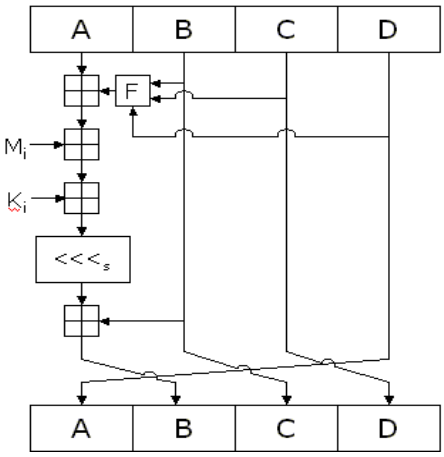

Figure 2: MD5 Algorithm

- **Execution Snapshots:**

➢ **Login Page**

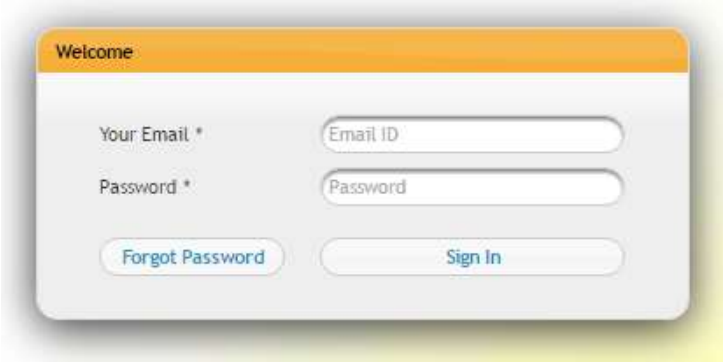

Figure 3: User Login Page

➢ **Main Page**

Figure 4: Home Page

- **Create new user page**

Figure 5: Create new user page

- **Dynamic group creation page**

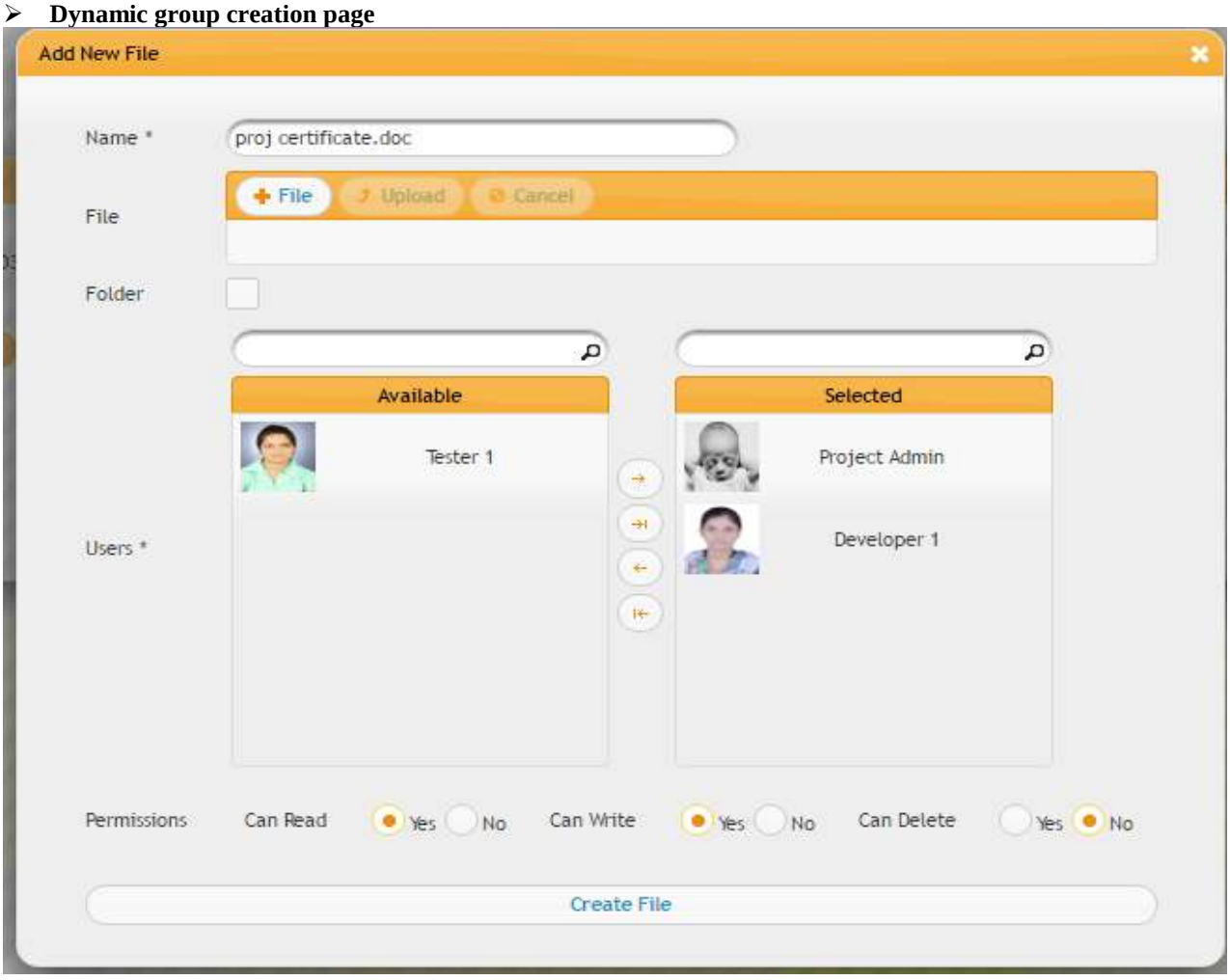

Figure 6: Dynamic group creation page

➢ **File creation page**

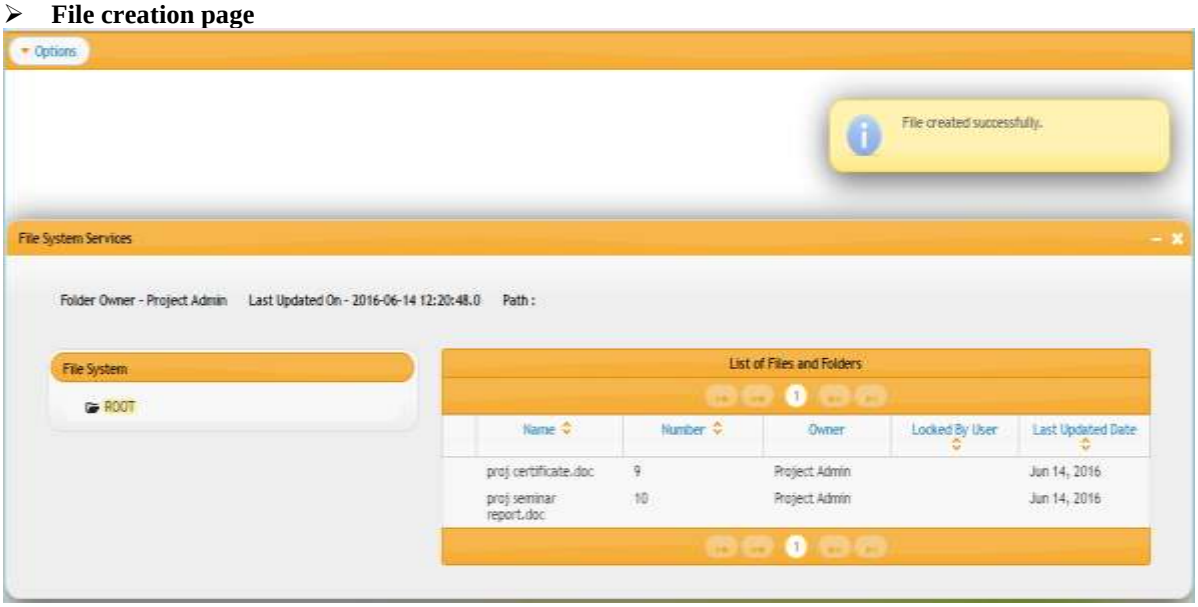

Figure 7: File creation page

➢ **Lock allocation page**

Figure 8: Lock allocation page

IV. RESULTS FOR EXISTING SYSTEM AND PROPOSED WORK

The four text files of different sizes are used to conduct four experiments, where a comparison of three algorithms AES, DES and RSA is performed.

Evaluation Parameters

Performance of encryption algorithm is evaluated considering the following parameters.

A. Encryption Time

B. Decryption Time

The encryption time is considered the time that an encryption algorithm takes to produces a cipher text from a plain text. Encryption time is used to calculate the throughput of an encryption scheme, is calculated as the total plaintext in bytes encrypted divided by the encryption time. Comparisons analyses of the results of the selected different encryption scheme are performed.

- **Experimental Results And Analysis**

Experimental result for Encryption algorithm AES, DES and RSA are shown in table-2, which shows the comparison of three algorithm AES, DES and RSA using same text file for four experiment.

Table 1: Comparisons of DES, AES and RSA of Encryption Time

	AES	DES	RSA
153 KB	1.642	3.023	7.312
196 KB	1.713	2.432	8.498
312 KB	1.823	3.122	7.854
868 KB	2.111	4.237	8.213

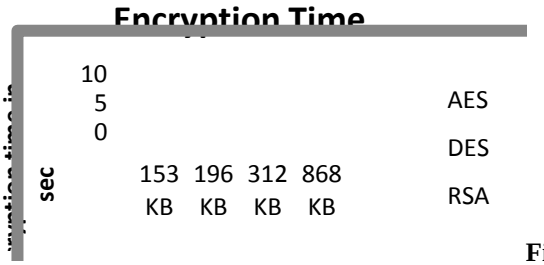

Figure 9: Graph of encryption time required by AES, DES and RSA

Table 2: Comparisons of DES, AES and RSA of Decryption Time

	AES	DES	RSA
153 KB	1.023	1.132	4.965
196 KB	1.433	1.255	5.934
312 KB	1.622	1.376	5.167
868 KB	1.827	1.265	5.187

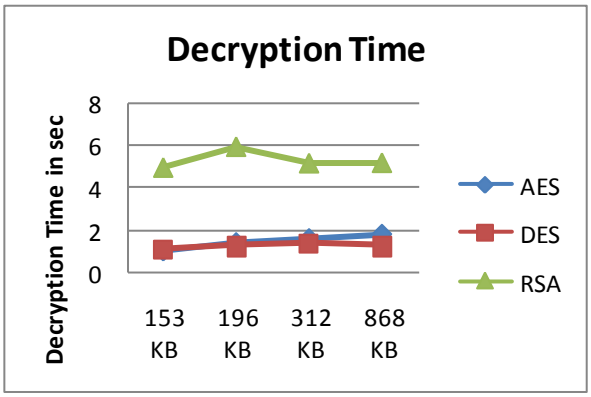

Figure 10: Graph of decryption time required by AES, DES and RSA

V. CONCLUSION

In this paper, we acquainted with enhancing protection by strategy era in substance sharing locales. To begin with, we will display a way to deal with encode a document for the client's security information and the client will have the capacity to transfer any kind of record on substance sharing destinations like content and additionally sight and sound records. Second, the arrangements will be produced taking into account RBAC which will determine the entrance rights to the clients of specific record. We have also discussed methods for secure data sharing across organizations with crisis management in the public health domain as an application area. These organizations could be government organizations, financial institutions, hospitals or universities. As we have stated there is a strong need for organizations to share data and form the big picture so that the data may be analyzed and effective decisions be made. We identified ten functions for data sharing across organizations.

REFERENCES

[1] Anna Cinzia Squicciarini, Dan Lin, Smitha Sundareswaran, and Joshua Wede, "Privacy Policy Inference of User-Uploaded Images on Content Sharing Sites", IEEE Transactions on Knowledge and Data Engineering, Vol. 27, NO. 1, January 2015.

[2] J. Bonneau, J. Anderson, and L. Church, "Privacy suites: Shared privacy for social networks," in Proc. Symp. Usable Privacy Security, 2009.

[3] A. Kapadia, F. Adu-Oppong, C. K. Gardiner, and P. P. Tsang, "Social circles: Tackling privacy in social networks," in Proc. Symp. Sable Privacy Security, 2008.

[4] Kambiz Ghazinour, Stan Matwin and Marina Sokolova, "Yourprivacyprotector: A Recommender System For Privacy Settings In Social Networks", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 2, No 4, August 2013.

[5] Alessandra Mazzia Kristen LeFevre and Eytan Adar, "The PViz Comprehension Tool for Social Network Privacy Settings", Tech. rep., University of Michigan, 2011.

[6] Peter F. Klemperer, Yuan Liang, Michelle L. Mazurek, "Tag, You Can See It! Using Tags for Access Control in Photo Sharing", Conference on Human Factors in Computing Systems, May 2012.

[7] C. A. Yeung, L. Kagal, N. Gibbins, and N. Shadbolt, "Providing access control to online photo albums based on tags and linked data," in Proc. Soc. Semantic Web: Where Web 2.0 Meets Web 3.0 at the AAAI Symp., 2009, pp. 9–14.

[8] Sergej Zerr, Stefan Siersdorfer, Jonathon Hare, Elena Demidova , "I Know What You Did Last Summer!:Privacy-Aware Image Classification and Search" , Proceedings of the 35th international ACM SIGIR conference on Research and development in information retrieval, 2012.

[9] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in Proc. 6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006, pp. 36–58.

[10] L. Church, J. Anderson, J. Bonneau, and F. Stajano, "Privacy stories: Confidence on privacy behaviors through end user programming," in Proc. 5th Symp. Usable Privacy Security, 2009.

[11] H. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view," in Proc. Conf. Usability, Psychol., Security, 2008.

[12] K. Strater and H. Lipford, "Strategies and struggles with privacy in an online social networking community," in Proc. Brit. Comput. Soc. Conf. Human-Comput. Interact., 2008, pp.111–119.

[13] R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh, "Capturing social networking privacy preferences," in Proc. Symp. Usable Privacy Security, 2009.

[14] S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair, "Over-exposed: Privacy patterns and considerations in online and mobile photo sharing," in Proc. Conf. Human Factors Comput. Syst., 2007, pp. 357–366.

[15] Mehmet Erkan Yüksel and Asım Sinan Yüksel, "An Application for Protecting Personal Information on Social Networking Websites", The Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2010.