



Net-Chk: A SECURITY FRAMEWORK FOR SOCIAL NETWORKING APPLICATIONS

S.Thiraviya Regina Rajam¹ and S.Britto Ramesh Kumar²

Research Scholar, St. Joseph's College (Autonomous), Tiruchirappalli¹

Asst. Professor in Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli²

Abstract: The Online Social Network Services (OSNs) have experienced tremendous growth in recent years and become a de facto portal for hundreds of millions of internet users. These OSNs offer attractive means for digital social interactions and data sharing, but also raise a number of issues on security and privacy. While OSNs allow users to restrict access shared data, they currently do not provide any mechanism to enforce security and privacy concerns over data associated with multiple users. One fundamental issue in today's OSNs is to give users the ability to control the messages posted on their own private space to avoid that unwanted content is displayed. In this paper, the proposed framework called Net-Chk application, creates firewall in network security. This proposed application gives close wall security while accessing the Social Network sites. It enables the protection of shared data associated with multi users virtual environment in OSNs. And it also allows OSN users to have a direct control on the messages posted on their walls and a secured login method is provided to avoid hacking, Phishing and Social Engineering. It is achieved by using RSA Algorithm.

1. INTRODUCTION

A major security challenge on the Internet is the existence of the large number of compromise machines. Such machines have been increasingly used to launch various security attacks including spamming and spreading malware, DDoS, and identity theft. A typical OSN provides each user with a virtual space containing profile information, a list of the user's friends, plus web pages, such as wall in Face book, where users and friends can post content and send messages. A user profile usually includes information with respect to the user's birthday, gender, interests, education and employment history, and contact information. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in users own spaces, they unfortunately, have no control over data residing outside their spaces. For example, Facebook allows users to state who is allowed to insert messages in their walls (i.e., friends, fof, or defined group of friends) [1]. However, no content-based preferences are supported and therefore it is not possible to prevent unwanted messages, such as political or vulgar ones, no matter of the user who posts them [2]. To overcome all the issues, we propose a new application Net-Chk. Whenever users login to their account, it verifies the login id and graphical image authentication. It also provides a unique key to users when they need to access various features like chat, post, comment and video chat. Thus it provides secure login and secure access to various features in proposed application. In this paper Section 2 provides

summary of related works, Section 3 contains various attacks on social networks. Section 4 describes the proposed secure Net-Chk Framework. Section 5 discuss about the functionalities of proposed Net-Chk framework. Section 6 describes the major phases on proposed Net-Chk Application. Implementation and Results are displayed on section 7 and 8 respectively. Finally, this paper concludes on section 9.

2. RELATED WORK

In this section, I discuss the works related to privacy and security in OSN. I first focus on the studies that resolve the security issues in OSNs. Aaron et al.(2012) proposed Secure Social Aware: A Security Framework for Mobile Social Networking Applications in which he presented a framework called SSA, it allows for the interaction of social network information with real-world location-based services without compromising user privacy and security [3]. Through exchanging an encrypted nonce (EID) associated with a verified user location, SSA allows location based services to query the local area for social network information without disclosing user identity or any set of information which could be positively matched to users. Yan et al. (2010) have proposed a Collaborative Framework for Privacy Protection in Online Social Networks [4]. System architecture for a private OSN is proposed to protect privacy. In this architecture, community creators can collaborate to manage



and maintain their communities. The main task of cryptography in building a private OSN is to restrict the information available in an appropriate range. Users make use of relationships or social links to represent this range in a social network. Anna et al. proposed PriMa, an effective security and privacy protection mechanism for social networks. PriMa (Privacy Manager) automatically generates access rules for users profile information [5].

These access rules are generated on the basis of users' privacy preferences on their data in the profile, the sensitivity of the data with respect to the privacy settings of the user such as his privacy preferences for his profile data and the degree to which his profile data is at a risk of being expose to others, and the risk of disclosing such data to other users. Hence, PriMa reduces the chance of accidental disclosures due to outdated policies. A new attack called Identity Cloning Attack (ICA), which focuses on forging user profiles on OSNs, has been introduced.

The key goal of an adversary in ICA is to obtain personal information about a victim's friends after successfully forge the victim, and to establish increased levels of trust with the victim's social circle for future deceptions. In this attack, the adversary first tries to find ways to obtain a victim's personal information, such as name, location, occupation and friends list from his public profile on OSNs or his personal homepage(s). Then, the adversary forges the victim's identity and creates a similar or even identical profile on OSN sites. [6]. [7] showed that cloning of user profiles could be misused to infiltrate private networks, while [8] outlined yet another attack to infiltrate closed networks via HTTP cookie hijacking. The failures in the above discussed papers are rectified in our proposed paper. Persona uses a combination of attribute-based cryptography and public key cryptography to protect information. This allows near features like encrypted group messages without needing to know the entire list of group members, or the need for encrypting the message with the public key of every member in the group. No trust has to be put on the service operators that store the data, or on the application providers. In order to detect faked identities on OSN sites, a detection process is designed.

3. ATTACKS ON ONLINE SOCIAL NETWORK SERVICES

Online Social Network Services (OSNs) are today one of the most popular interactive medium for communicating, sharing, and disseminating a considerable amount of human existence information. Daily and continuous communications imply the exchange of several type of content, including free text, picture, audio, and video data. However, OSNs face a large number of attacks which affects the privacy and security of its users. In this section, I will

discuss the various attacks in OSNs. For instance, if users posts a comment in a friends space, they cannot specify which user can see the comment. In another case, when a user uploads a photo and tags friends who appear within the photo, the tagged friends cannot restrict who can see this photo. Spammers are always looking for ways to reach new victims with their unsolicited messages. In a social network, the first action a malicious user would likely execute to get in touch with his victims is to send them a friend request.

This might be done to attract the user to the spammer's profile to view the spam messages (on MySpace) or to invite user to accept the friendship and start seeing the spammer's messages in her own feed [9]. In Web, most identity management system models such as silo model, centralized model, and federated model are designed from organization's perspective [10]. The posted content can be re-distributed by the viewers, and eventually the content can be shared with unintended users who were not explicitly allowed to view that content. Such open sharing availability of social networking sites exposes the users to a number of privacy risk [11].

The primary goal of EASiER is to protect accidental or intentional information leak in OSN through encryption, specifically ABE, chosen for its expressiveness. Unlike traditional OSNs, which generally support one type of relationship such as friend, EASiER users define relationships by assigning attributes and keys to each other [12]. To protect information, users encrypt different pieces of data such as profile information, wall posts, etc. with attribute policies. Thus OSNs are suffered by various security and privacy attack. In this paper, I propose an idea to overcome the issues with content preference and security policies.

4. PROPOSED Net-Chk FRAMEWORK

The Framework defines the structure of components, their interrelationships, the principles and guidelines governing their design. Figure 1 depicts the proposed Net-Chk Framework that consists of Client Requester (CR), Authentication Server (AS), Communication Server (CS), Key Generator (KG), Image Matcher (IM), Access Control Manager (ACM), Attack Identifying Manager (AIM), Short Text Classifier (STC), Short Text Database Manager (STDM) and MController. Internet is used as the standard communication protocol between the CR and AS. The proposed system provides the necessary technical infrastructure such as acquiring user information, connectivity, authentication, access control and identifying the attacks in order to provide secure OSNs to users. The key generator and image matcher provides strong authentication by providing unique password.

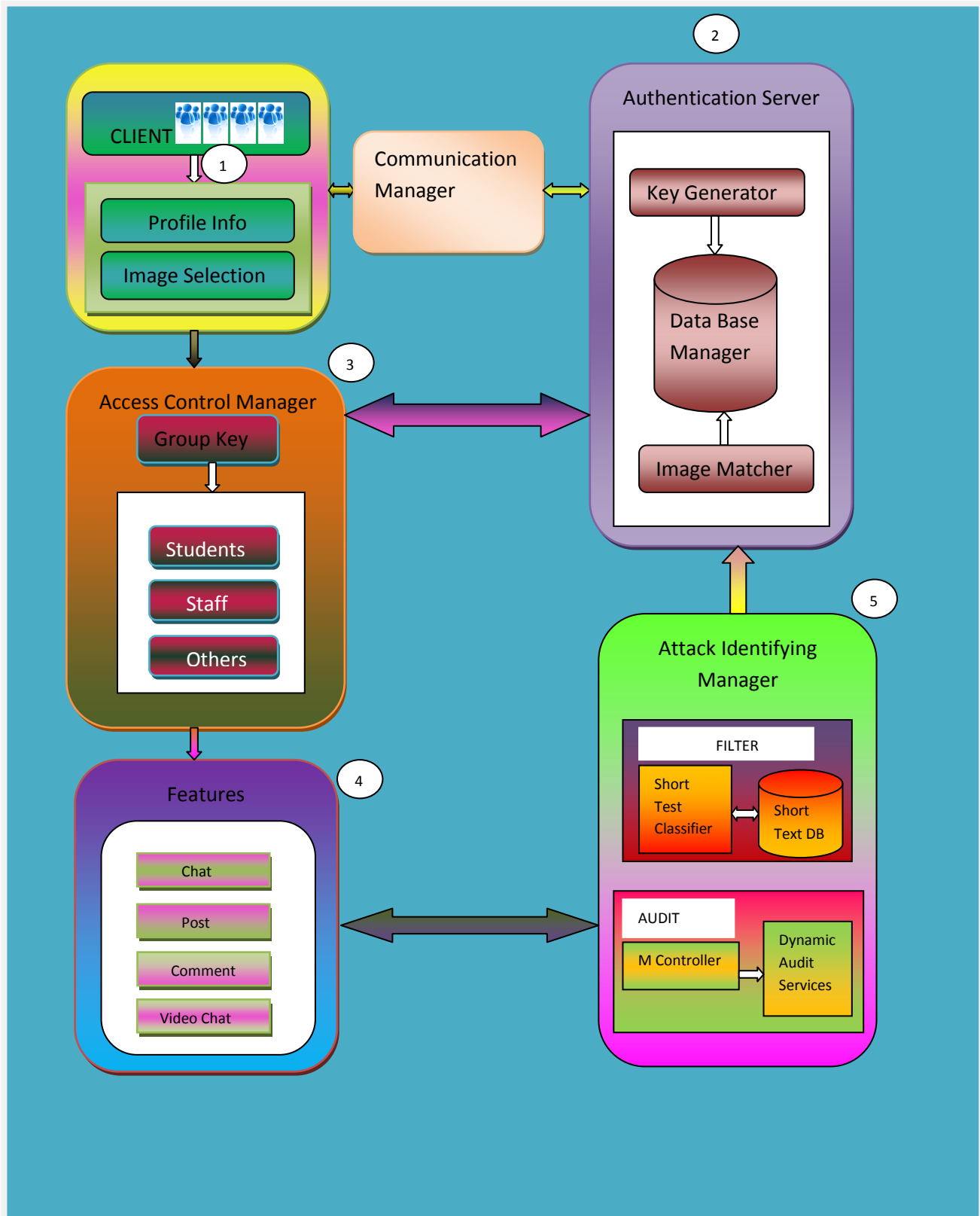


Figure1. Net-Chk Framework



5. FUNCTIONALITIES OF PROPOSED Net-Chk FRAMEWORK

The various functionalities of the framework are well presented in below.

CLIENT REQUESTER (CR) – The Client Requester is a user (i.e. student, staff, others) of OSNs. The client has made a request to AS for registration in proposed OSN. The Authentication server also allows the clients for registration over the internet. Once the registration process is completed, the Authentication server generates a unique key for the client and save all the client details in the Data Base Manager. During login the client provides correct answers for the security authentication in order to get the unique key to access any features in the server.

COMMUNICATION MANAGER (CM) – The Communication Manager (CM) acts as a communication medium between the client and server. It transfers the client request to the server and server response to the client. It acts as an intermediate between client and server. The requester interfaces are secured using Public Key Infrastructure mechanism.

AUTHENTICATION SERVER (AS) – The Authentication Server (AS) keeps a record of all registered clients. The authentication of the client is done by the authentication server by matching the images in proper order with the order of the images stored in the Data Base. After authentication, AS establishes connection with Data Base Manager for retrieving user's details, The information flow on the network is secure by encrypting and decrypting the message. The Authentication Server setup consists of a Key Generator, Image Matcher and Data Base Manager.

KEY GENERATOR (KG) – The Key Generator (KG) generates a unique key for every client once the authentication is given to the user.

It stores the unique key in the Data Base Manager inside the server. The key is encrypted using RSA algorithm for security reasons.

DATA BASE MANAGER (DBM) – The Data Base Manager (DBM) stores all the client details along with their

security unique key. The profile information of every user is stored in the database. It contains Image Matcher (a set of images) for verification of Graphical image authentication. All data inside the Data Base Manager is in encrypted form.

IMAGE MATCHER (IM) – The Image Matcher (IM) verifies the Graphical image authentication. It matches the image order selected by the client to the image order stored in the Data Base. If the order matches, it indicates to the server to give authentication to the client else server displays an error message to the client. The images inside the IM are stored in encrypted form.

6. MAJOR PHASES OF PROPOSED Net-Chk APPLICATION

There are three major phases involved in the proposed application to carry out the secure login. They are Registration Phase, Key Generation Phase and Authentication phase.

REGISTRATION PHASE

In this phase, the client requester is authenticated by registering oneself in the authentication server. At the time of registration, the user provides his personal data such as name, email, address, gender, birth date, login etc. Also user needs to answer a set of security authentication along with which user needs to arrange a set of random images in an order. After completing the registration, the user will be able to login to the website by entering login id and Graphical image authentication (i.e. arranging the set of random images in the same order which user arranged during the time of registration). Then the user will be able to login to their profile page. Thus secure registration is provided using this phase.

KEY GENERATION PHASE

In this phase, a Graphical User Key is generated during the registration phase which needs to be arranged by the user in any order. Once the registration is completed a unique key is generated for each user. And whenever the user tries to login to the website the key generator provides the Graphical image authentication in random order every time and the user needs to arrange the images in the same order which they arranged during registration. Once the user login to the website, in order to use any features in the website such as



uploading/downloading photos, chatting with friends etc. User needs to answer a set of security authentication which was answered during registration phase. If the answers are correct, key generator generates the unique key immediately to access the features in the application.

AUTHENTICATION PHASE

In this phase, the Authentication Server authenticates the user during the registration phase. Two factor authentication is followed such as graphical image authentication and security authentication. Once the registration is successful and if the user try to login to the website, user needs to provide the correct login and Graphical image authentication.

If the username and password is correct the server authenticates the user to access the website else displays a error message. Once the users log in to the website, in order to access any features they need a unique key. In order to get the unique key, users needs to click “find key” link, once the link is clicked it will display the set of security authentication which was answered during the registration. If the answers are correct, AS authenticates the user and provides the unique key else displays a error message. After getting the unique key, the user will be able to use the features such as chat, video chat, post etc in the proposed application.

if Admin gives permission. The admin gives permission by clicking the “active” option. After typing the username, user needs to choose the images in correct sequence as they have chosen in the registration phase. The login phase of Net-Chk is shown in the following figure 3. After logging in to the account successfully, users should provide their own unique key to use the various features of Net-Chk such as chat, etc. In order to get the unique key the user need to click on the “find key” button on the screen. It will lead the user to security authentication page, in which the user needs to answer for the security questions which were answered during the time of registration. The security authentication phase is shown in figure 4. After completing the security authentication, public key and private key will be automatically generated using RSA algorithm on the screen. The entries of each user are stored in the admin database.

7. IMPLEMENTATION

SOFTWARE

The software implementation is used in this application is

- Java Script
- HTML
- JSP.

HARDWARE

The hardware implementation is done on

- Microsoft Windows XP
- Professional version 2002
- Service packet 2
- Intel Pentium processor
- CPU 230@160 GHZ
- 1.60 GHZ
- 0.99 GHZ of RAM.

The implementation of the Registration phase is shown below. Any users who have Email Id can register in this Social Network. The following figure 2 shows the registration phase. User can access the Social Network, only

SOCIAL NETWORK

[Home](#) | [New User](#)

Registration

Name	<input type="text" value="Vijay"/>
Gender	<input checked="" type="radio"/> Male <input type="radio"/> Female
Date of Birth	<input type="text" value="7"/> <input type="text" value="Jun"/> <input type="text" value="1989"/>
E-mail ID	<input type="text" value="vijay1989@gmail.com"/>
City	<input type="text" value="Tachy"/>
About your Interest	<input type="text" value="I want to"/>
Security Question 1	<input type="text" value="What is your nick name?"/>
Answer1	<input type="text" value="vijay"/>
Security Question 2	<input type="text" value="What is your favorite tourist sp"/>
Answer2	<input type="text" value="rockfort"/>
Security Question 3	<input type="text" value="What is your profession"/>
Answer3	<input type="text" value="developer"/>

Login Information


Username	<input type="text" value="vijay"/>
Select Images Here (This will generate the Graphical Password)	
	
<input type="password" value="*****"/>	
<input type="button" value="Register"/> <input type="button" value="Reset"/>	

Figure 2. Registration phase of Net-Chk

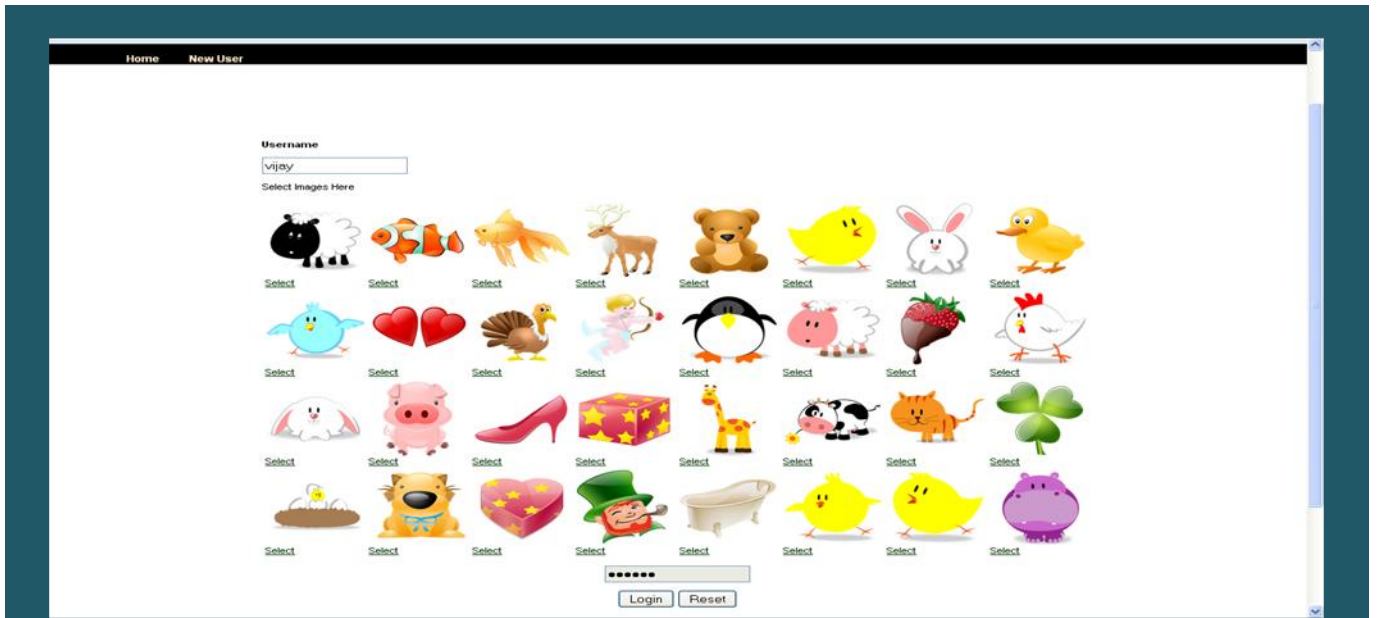


Figure 3. Login phase

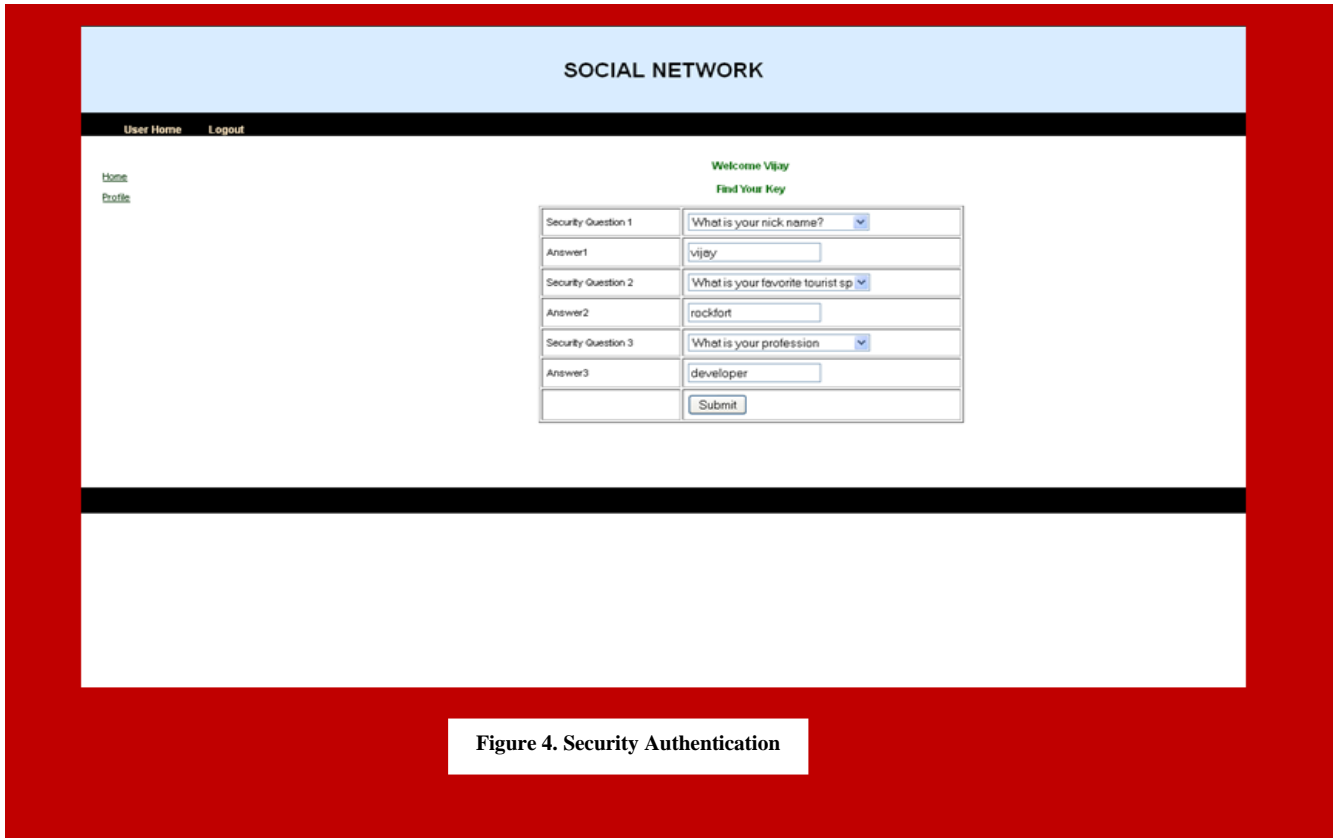


Figure 4. Security Authentication



achieved during the login phase of the proposed application. The security level increases with the number of images chosen by the user. For example, if a user chooses 10 images, the security level will be high and if a user chooses 3 images the security level will be low. Security level is achieved completely even if the user count increases. In this graph, x-axis represents the users count and y-axis represents the level of security. This graph clearly indicates that the security level is up to 96% even if the number of users increases. This is achieved through two factor authentication such as graphical image authentication and security authentication.

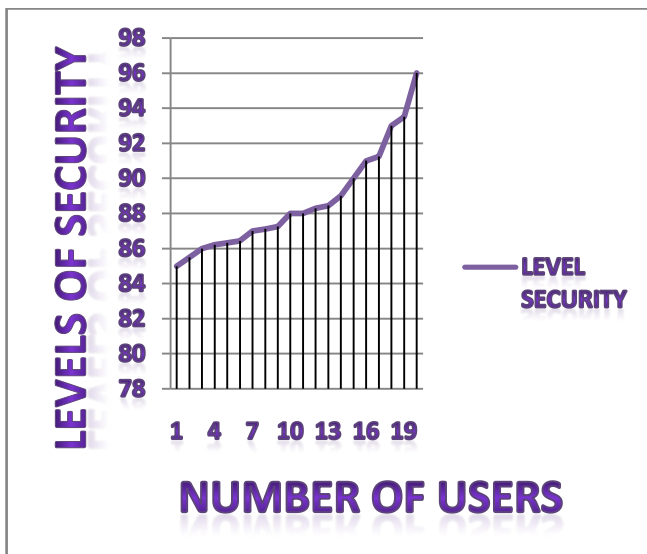


Figure 5. Levels of Security

9. CONCLUSION

In this paper I examined both attack and protection strategies for social networking sites. A number of practical attacks have been outlined by researchers in the last five years and a fast number of actual attacks have been observed in-the-wild. Many empirical studies [9] have shown that average OSN users have difficulties in understanding also the simple privacy settings provided by today OSNs. Given the emerging threats of social networking usage I hence explored mitigation strategies for these attacks. In this paper, I have presented a new application Net-Chk to provide a unique key to each users in order to make the login process more secured. Also data are encrypted using the RSA algorithm. And a secure authentication is provided to the users by generating a unique key and a Graphical image authentication. The proposed application provides more security and privacy to the OSNs users. Two level authentication is done to provide secure login to the users. Public key and private key are generated to the users in

encrypted form. In future enhancement, access to all features in Net-Chk will be done in a secured way.

REFERENCES

- [1] Hongxin Hu, Gail-Joon Ahn and Jan Jorgensen, " Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks" *American Journal of Applied Sciences*, volume 4, issue 8, 2007, pp.538-542.
- [2] Marco Vanetti, Elisabetta Binaghi, Elena Ferrari, Barbara Carminati, and Moreno Carullo. "A System to Filter Unwanted Messages from OSN User Walls," in Proc..IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, volume 25, issue 2, 2013.
- [3] Aaron Beach, Mike Gartrell, Baishakhi Ray, Richard Han," Secure Social Aware: A Security Framework for Mobile Social Networking Applications," in Proc. IEEE International Conf. on 2012 , pp. 439-446.
- [4] Yan Zhu, Zexing Hu, Huaixi Wang, Hongxin Hu, Gail-Joon Ahn, "A Collaborative Framework for Privacy Protection in Online Social Networks," in Proc. 6th Annu. IEEE International Conf. on 2010 , pp. 1 – 10.
- [5] Anna Squicciarini, Federica Paci, Smitha Sundareswaran, "PriMa: An Effective Privacy Protection Mechanism for Social Networks," in Proc. 3rd Annu. IEEE International Conf. on 2010.
- [6] Lei Jin,Hassan, Takabi,James, B.D. Joshi,"Towards Active Detection of Identity Clone Attacks on Online Social Networks," in Proc. 7th International Conf. on Digital Object Identifier: 10.1109/ECDC.2013.6556739, 2013, pp. 1-12.
- [7] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda,"Automated identity theft attacks on social networks," in Proc. 18th International World Wide Web Conf. on 2009.
- [8] Markus Huber, Martin Mulazzani, and Edgar Weippl," Automated friend injection attacks on social networking sites," in Proc. of IFIP/SEC 2010.
- [9] Gianluca Stringhini, Christopher Kruegel, Giovanni Vigna,"Detecting Spammers on Social Networks," in Proc. IEEE Digital Object Identifier: 10.1109/INFCOMW.2009.5072127, 2009, pp. 1-2.
- [10] K. Strater and H. Richter, "Examining Privacy and Disclosure in a Social Networking Community," in Proc. 3rd Symp. Usable Privacy and Security (SOUPS '07), 2007, pp. 157-158.
- [11] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D.Starin," Persona: An online social network with user-defined privacy," in Proc. ACM SIGCOMM Computer Communication Review, 2009, pp. 135–146.
- [12] Sonia Jahid, Prateek Mittal, Nikita Borisov," EASiER: Encryption-based Access Control in Social Networks,," in Proc. 3rd Annu. IEEE International Conf. on Social Computing (socialcom)Digital Object Identifier: 10.1109/PASSAT/ SocialCom.2011.158, 2011, pp. 1302 – 1309.