# A two-layer security model for accessing multimedia content in social networks

Ali Pazahr
Department of Computer Science
Islamic Azad University
Ahvaz, Iran
+98 916 615 7215
Pazahr@iauahvaz.ac.ir

Dr. J. Javier Samper Zapater
IRTIC
University of Valencia
Valencia, Spain
+34 9635 43567
jsamper@irtic.uv.es

Dr. Francisco García Sánchez
Department of Informatics and Systems
University of Murcia
Murcia, Spain
+34 86888 8107
frgarcia@um.es

Parisa Ganjeh
Department of Psychology
Shahid Chamran University of Ahvaz
Ahvaz, Iran
+98 916 341 1750
parisaganje@yahoo.com

Dr. Carmen Botella
IRTIC
University of Valencia
Valencia, Spain
+34 9635 43424
Carmen.botella@uv.es

## ABSTRACT

Securing a website is nowadays one of the major concerns for system administrators. Security is also the most important challenge that Web developers have to face when designing a trustworthy platform to provide services for public users. It is well known that multimedia content on the Web is continuously growing and recently this media type is more and more commonly used in social networks. The access to multimedia content in the context of social networks should be both easy and secure. In this paper, a semantically-empowered security model for accessing multimedia content in social networks is presented. The application of this model ensures that (1) unauthorized users cannot access to private multimedia data, and (2) the overall level of trust among social networks users who share their private and sensitive data is enhanced. Two questionnaires were developed to select the most characteristic features to consider in our model to differentiate legitimate users and attackers. By using parametric considerations, both security and users' convenience are reached which makes our proposed model more effective.

## CCS Concepts

**• Security and privacy~Multi-factor authentication • Security and privacy~Social network security and privacy** • Computing methodologies~Feature selection • Information systems~Clustering

## Keywords

Reference Pattern; Test Pattern; Single Sign On; User Behavior; Multimedia; Security; Social Network

## 1. INTRODUCTION

With the increased use of multimedia in daily communications, it is necessary to develop efficient and secure access mechanisms that are specifically tailored for multimedia data access [1]. The importance of this issue is even more critical when the environment, in which users share their contents, is popular [2] [3]. Nowadays, social networks have numerous good advantages in many aspects and they are particularly well suited when there are chances for business purposes. However, in the use of social networks there are also some challenges worth considering [4]. Specifically, there are serious risks of people abusing the facilities provided by social networks and trying to access data they are not allowed to see. Although social networks can be the ideal environment for investors and common users to share their significant information and develop their ideas, the current security rules and frameworks do not properly face nor resolve the existing breaches [5]. For end users to fully trust in this environment, it is necessary to consider a safer platform along with some considerations such us those stated in [6] and [7] for all users' convenience: (i) limiting the amount of personal information user posts, (ii) remembering that the Internet is a public resource, (iii) being wary of strangers, (iv) being skeptical, (v) evaluating user settings, (vi) being wary of third-party applications, (vii) using strong passwords, (viii) checking privacy policies, (ix) keeping software, particularly user's web browser, up to date, and (x) using and maintaining anti-virus software.

Whereas information on social networks comprises multimedia data, it is a must to undertake an appropriate structure for security of data in order to establish a safe place for users [8]; otherwise they would avoid sharing their multimedia contents. Not providing the necessary security measures, and thus diminishing the users' trust, would be a weakness for a social network, since one of the most important reasons for investors to pay attention to such a type of websites is that they attract many potential users. Indeed, the interest of investors in social networks is tightly related to the amount of active users in such networks; problems in handling security issues would certainly decrease users' involvement in those websites [9].

This paper aims to fill in this gap with a framework to boost multimedia information security for online social networks (OSN) by taking advantage of semantic technologies. This framework introduces a reliable security architecture for multimedia information access control, which can be employed in every social network to decrease the probability of unauthorized access to users' private multimedia contents. We propose a model consisting of two layers of user's validation when they request access to multimedia data. The first layer comprises the traditional login and password combination. The second layer leverages the users' behavior in a social network through the application of semantic techniques in order to more accurately confirm the identity of those users.

This paper is organized as follows. Section 2 discusses the state of the art that somehow deal with the access to multimedia content. The proposed security model is described in Section 3. In Section 4, the feature selection process and the proposed model is evaluated. Section 5 presents current frameworks and their weaknesses in comparison to the proposed model. Our final remarks and future work proposals are put forward in Section 6.

## 2. STATE OF THE ART

During the last few years, the concern about security and privacy issues in social networks has gained importance across the scientific community. In this section, a comprehensive analysis of the state of the art in this field is provided.

In [10] the authors argue that the detection of users' attributes based on users' communication streams can be achieved through users authenticity, what they tag, who do tag, and their behavior when they have an active session. The point in [11] is that it is also possible to characterize the user behavior in OSN by analyzing the data related to the users' interaction with friends and by leveraging click stream data for identifying patterns in an OSN.

In [12], monitored users aiming at accessing to multimedia data are classified into two groups, namely, actual and fake users. For classification purposes, the members of each group are analyzed so as to characterize their common properties. As mentioned in [13], it is important to observe both visible and latent user interactions to collect user behaviors and use them as a feature vector for checking authenticity of an active session's user.

According to what stated in [14] and [15] a few times a day, and in some conditions in a weekly fashion, data gathering approaches provide insights into user activity patterns and lay out an analytical foundation for further understanding of various properties of OSN by analyzing user's posting behavior.

In [16], a Dual-Level Identity and Authentication Model is proposed for the Internet Multimedia Communications. This model focuses on robust multimedia communication services in public Internet, thus requiring more sophisticated mechanisms to build more secure multimedia connections, both for voice and video communications. The research presented in [17] introduces some other security mechanisms such as Digital Rights Management (DRM), multimedia encryption, digital watermarking, digital fingerprinting, multimedia forensics, privacy preserving data mining, secure user interface, intrusion detection, etc.

The work in [18] proposes a security framework for multimedia protection in social media networks using both server and software implementations. The secure server implementation uses two separate anonymous databases with the Captcha security technique and RSA cryptographic algorithms. The secure software implementation is achieved by providing two levels of authentication with an auto-lock and security+ features. The proposed framework can handle both automated program attacks and human attacks. The architectural manifesto in [19] provides a solution to issues such as the "walled garden problem", the limitation of robustness, the scalable and dynamic resource access control in unsupervised environments, and the lack of well-defined explicit support for reputation tools, through the embedding of the identity notion into the overlay level. In addition, a favorable identity-based integration between applicative modules is allowed by the framework. Furthermore, it points out the need for an effective tag-based resource retrieval for a complete SNS (Social Network Services) design.

In [20] the authors demonstrate that users generally disclose very much private information on online communities, and different factors influencing this behavior were identified and studied. The results of an online survey investigating the relations between personality traits (based on the Five-Factor Model), usage patterns and information disclosure of participants in different types of online communities are also presented.

## 3. PROPOSED SECURITY MODEL

Given the flaws of current security approaches, in this work we propose a two layer security model for accessing to multimedia contents in social networks (see Figure 1). In a nutshell the system works as follows: First, users should enter their username and password on the login page and try to be authenticated to the website. After a successful login, the web application system logs users' interaction with the social network, that is, the system keeps track of their behavior. For this, a feature vector representing a particular user's behavior is built. Afterwards, the system can decide whether a user is legitimate or not by comparing the current feature vector against the reference one. Legitimate users are allowed to access to their multimedia contents while unauthorized users are denied all access.

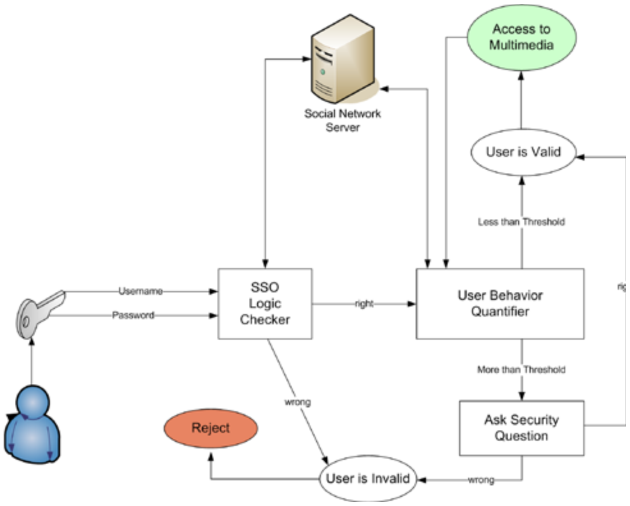


Figure 1. An overview of the proposed security model

## 3.1. First Layer: SSO

Single Sign On (SSO) is one of the simplest and most efficient mechanisms for user authentication [21]. Users try to login to the website of a social network by typing their user name and password on the login web page. In this step, login details are verified and if they are valid, then users can visit the main page of their profile; otherwise, the social network prevents their access to website.

The SSO method is a must as a first step for user validation, but it is not enough [22] [23]. In this work, we present a methodology for users' authentication based on their behavior, which cannot be forged by malicious users.

## 3.2 Second Layer: User behavior

Each user in a social network behaves differently. Tagging style, topics of interest, session duration, number of replies to a post, and so on and so forth, are only a few of the features characterizing the behavior of users in a social network. Consequently, it is possible to represent the behavior of a user by using a feature vector. Each time a user accesses to the social network, a "sample" is constructed in the form of a feature vector in the space of N dimensions, in which N is the number of features. The ultimate goal is to take advantage of these feature vectors in order to accurately identify legitimate users and let them access to their private multimedia data.

Each dimension of the feature vector is made up of an attribute (a.k.a. feature) describing one kind of user activity in an OSN. The numeric value of an attribute in the feature vector depends on the behavior of the user while browsing the social network. Concretely, from the moment the users sign up to the social network, their feature vectors are calculated on the basis of their particular interactions and activities within the social network. After a period of time, which depends on the duration of the user's activities, the initialization of a set of feature vectors for a given user is completed and they are stored as the so called "Reference Pattern".

Each sample in N-dimensional space is a representative of a feature vector for one user in each session. A sample feature vector, distinguished by red color, is shown in Figure 2.

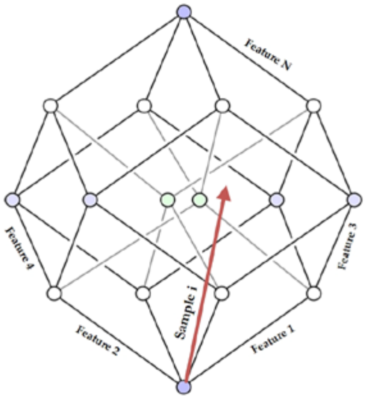


Figure 2. Samples in N-dimensional space of features

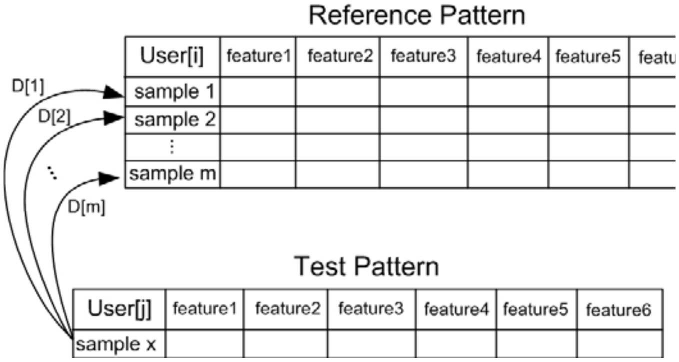
So, as the time goes by, the number of these vectors increases and, after a while, the reference pattern is fully defined with accurate values for each feature thus precisely characterizing social network users. Since each reference pattern is made for a particular user, it is straightforward to provide a "Reference Threshold" for this user, which stems from the values in the feature vector of samples. In this way, the "Reference Threshold" can be used as the single reference model with which to compare the results generated from the interactions of the users with the social network. In particular, this threshold can be seen as a geometric shaped-like sphere in the N-dimensional space; users whose feature vector falls out of this sphere are considered invalid, and valid otherwise.

On the other hand, when a new login happens, the social network system should generate a new feature vector representing this user behavior. This feature vector is called the "Test Pattern". Much like the reference pattern, the test pattern comprises some samples made up of the user session activities. All the values of both the reference and test patterns can be named as "Model Parameters".

In order to perform the second layer validation, the social network system has to compare the test pattern with the reference pattern in each session, before the user is allowed to access any private multimedia content. For comparison purposes, it is necessary to measure the distance between the test pattern represented as one sample and all the samples constituting the reference pattern, finding the minimum distance between both patterns. In Formula 1, the way these distances are calculated is detailed. In the formula *D* is the vector that stores the distance between the test pattern and reference pattern, *n* is the number of features, *TP* is a vector of test pattern, and *RP* is a vector of reference pattern. By the calculation of this relation, one distance is estimated and one part of *D* is initialized. When the estimate of *D's* is completed, it is necessary to find the minimum value among *D's*, namely, the "Test Threshold".

$$D[i] = \sqrt{\sum_{j=1}^{n} (TP[i][j] - RP[i][j])^2}$$

Formula 1. Calculation of Distances between Test Pattern and Reference Pattern



| User[i] | feature1 | feature2 | feature3 | feature4 | feature5 | featu |
|---|---|---|---|---|---|---|
| sample 1 | | | | | | |
| sample 2 | | | | | | |
| ⋮ | | | | | | |
| sample m | | | | | | |

| User[j] | feature1 | feature2 | feature3 | feature4 | feature5 | feature6 |
|---|---|---|---|---|---|---|
| sample x | | | | | | |

**Figure 3. Distances between Test Pattern and Reference Pattern**

Figure 3 depicts the distances between a sample (*sample x*) in the test pattern and all the samples comprising the reference pattern. In each session of the current user, *sample x* in the test pattern, which is built based on the current user's activities, is compared against *sample 1* in the reference pattern thus resulting in the calculation of D[1]. Next, the same goes for *sample 2*, producing D[2], and the remaining samples obtaining as a result all the other D[i]s.

In the next stage, if the test threshold (calculated as the minimum of all *D's*) is less than a given reference threshold, considering a suitable tolerance for reference pattern, the system concludes that the current user is valid (i.e., the system recognize that the user is legitimate) and so s/he can directly access multimedia data. Otherwise, having probability of estimation fault, the system proceeds to the next stage. This is the point that system has suspicion to the user during the multimedia access, i.e., whether s/he is valid or not.

The algorithm does not end to this point. Now, it is the time to ask a security question [24] to current user which was designed during signing up process.

## 3.3 Focus of Research

A question that could emerge is "why estimate the model parameters if it is possible always ask a security question to user at the beginning of accessing to other multimedia information?" The response to this question is to decrease of the frequency of asking security questions. These types of questions can annoy valid users whereas we can ignore these questions by detecting right authenticated users through their behaviors.

In Figure 1, our complete model is described. First, user types his/her username and password. The SSO Logic Checker, which evaluates SSO information, passes the user to the main page of his/her profile on the OSN, if s/he is validated. After signing into website, and setting up a new session for user, the component User Behavior Quantifier, compares test pattern as current user behavior with the reference pattern vector available on social network server. If it is inferred that the test threshold is less than the reference threshold, then it permits the user to have access to multimedia resources, once s/he is validated.

## 3.4 Finding features which best describe the user personality and distinct a specific user

We used two questionnaires "NEO Five-Factor Inventory (NEO-FFI)" and "Facebook Personality Behavior (FPB)". The first one is known and used by many researchers [25]. It asks 60 questions from the users and it is intended to measure the Big Five personality traits: Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness to Experience. The second one was prepared by us based on our necessity. It is made according to the operations happening in Facebook as our social media case study. It asks 44 questions from the users, each of them can be used as a feature for our security software system, effective for identifying of a user. We asked the questions that using them, we could measure the rate of the five factors and the factors' influences on the users' behavior on a social network.

We chose 67 people among the students of Islamic Azad University, Ahvaz branch and asked them to answer both questionnaires in three different times with the time interval of three months.

As a result, the features which we could select from the FPB questionnaire based on the evaluation were as below:

1- The level of using block list.

2- The people whom the user sends friend request to.

3- The level of posting on the other people's wall.

4- The level of tagging friends on the photos or posts.

5- The level of permitting search engines to link to the account's wall to access the posts.

6- The people whom the user mostly sends private message to.

The results of both questionnaires are discussed in the evaluation section.

Hence with the updated system by our methodology, users firstly answer the questionnaires and based on it, in the next times in which each user logs into the social network, the security system will be trained frequently by user's activities with the time interval of 5 minutes according to the 6 recently mentioned features.

# 4. EVALUATION

## 4.1 Feature Selection Evaluation

By using IBM SPSS, we did "repeated measures" test over the NEO-FFI. It was proved that the 5 subscales are identical and invariant in the time period of 6 months for the three tests. It is determined according sig. values of the tables 1-5 which all of them are above 0.05 that means the difference is not meaningful except the table for Agreeableness that we did not use it for our evaluation.

The repeated measures test was run for the all questions of FPB, and proved that in all questions except 41, the difference is not meaningful and in fact, these behaviors are consistent over the time. Then, we had to find the features through personality traits which are relatively stable. For that, we categorized NEO-FFI subscales into some groups to know who has, to what extent each of traits. Then, we evaluated correlation and significance of personality subscales with “one-way ANOVA” test. As a result, we found 7 questions expressing the features, among 44 questions which could have meaningful correlation with the subscales.

The questions 11, 26, 28 and 33 had meaningful correlation with Extraversion subscale. The Neuroticism subscale had meaningful correlation with the questions 3 and 44. The Openness subscale had meaningful correlation with the question 22. Therefore, we can use 6 features related to 3 subscales for our security model.

We used “k independent sample” nonparametric test (Kruskal Wallis) to measure the difference among three groups for the 6 meaningful questions. We used a nonparametric test because some of subscales were containing of 2 groups or one of their groups had less than 2 people frequency. Accordingly, in the recent test, the higher average value that group had, the more that feature value it had. For instance, about the question 3, the more use of block list, is meaning the more having of person’s Neuroticism which is interpretable.

| Effect | Value | F | Hypothesis df | Error df | Sig. |
|---|---|---|---|---|---|
| Pillai's Trace | .021 | .711 | 2.000 | 65.000 | .495 |
| Wilks' Lambda | .979 | .711 | 2.000 | 65.000 | .495 |
| Hotelling's Trace | .022 | .711 | 2.000 | 65.000 | .495 |
| Roy's Largest Root | .022 | .711 | 2.000 | 65.000 | .495 |

Table1: Confirms the tests have no difference in the subscale Neuroticism

| Effect | Value | F | Hypothesis df | Error df | Sig. |
|---|---|---|---|---|---|
| Pillai's Trace | .035 | 1.181 | 2.000 | 65.000 | .314 |
| Wilks' Lambda | .965 | 1.181 | 2.000 | 65.000 | .314 |
| Hotelling's Trace | .036 | 1.181 | 2.000 | 65.000 | .314 |
| Roy's Largest Root | .036 | 1.181 | 2.000 | 65.000 | .314 |

Table2: Confirms the tests have no difference in the subscale Extraversion

| Effect | Value | F | Hypothesis df | Error df | Sig. |
|---|---|---|---|---|---|
| Pillai's Trace | .023 | .768 | 2.000 | 65.000 | .468 |
| Wilks' Lambda | .977 | .768 | 2.000 | 65.000 | .468 |
| Hotelling's Trace | .024 | .768 | 2.000 | 65.000 | .468 |
| Roy's Largest Root | .024 | .768 | 2.000 | 65.000 | .468 |

Table3: Confirms the tests have no difference in the subscale Openness

| Effect | Value | F | Hypothesis df | Error df | Sig. |
|---|---|---|---|---|---|
| Pillai's Trace | .122 | 4.524 | 2.000 | 65.000 | .014 |
| Wilks' Lambda | .878 | 4.524 | 2.000 | 65.000 | .014 |
| Hotelling's Trace | .139 | 4.524 | 2.000 | 65.000 | .014 |
| Roy's Largest Root | .139 | 4.524 | 2.000 | 65.000 | .014 |

Table4: Confirms the tests have no difference in the subscale Agreeableness

| Effect | Value | F | Hypothesis df | Error df | Sig. |
|---|---|---|---|---|---|
| Pillai's Trace | .015 | .492 | 2.000 | 65.000 | .614 |
| Wilks' Lambda | .985 | .492 | 2.000 | 65.000 | .614 |
| Hotelling's Trace | .015 | .492 | 2.000 | 65.000 | .614 |
| Roy's Largest Root | .015 | .492 | 2.000 | 65.000 | .614 |

Table5: Confirms the tests have no difference in the subscale Conscientiousness

## 4.2 Model Evaluation

As mentioned in the previous subsection, our aim is to establish a more secure mechanism in accessing to multimedia contents in social networks, which can be reached by implementing of proposed model. Another purpose of our work is diminishing the number of security questions from valid users, because in many cases these questions are asked in order to solve a raised doubt to current user where it is not needed. By the estimation of a rate *R*, showing that the detection has been wrong or right, and then repeating this for the other users, we can analyze the system and evaluate our model. Formula 2 represents the rate of right detections among all active users.

$$RD = \frac{(\sum_{j=1}^{m}(T[j])) * 100}{\sum_{i=1}^{n}(T[i])}\ \%$$

Formula 2. Rate of right detections

By the Formula 2, it can be estimated the rate of right detections *RD*, in which *m* is the number of right detections, *n* is the number of all active users, working in the OSN, and *T* is a vector of test thresholds. If the system gets the state of multimedia access, but the current user is invalid, this recognition would be actually wrong, otherwise is right.

Another measurement for the system evaluation would be “False Positive” for the whole system, in which the response of our model for valid user detection process is positive and it casts doubt to user as a suspicious user, but the user is valid. In this case, it has to be asked a security question. We try to minimize the number of these conditions by choosing a correct and accurate feature vector. If the model parameters help us to decrease the number of false positive items, our model would be more successful, because our main focus is on diminishing the security questions when user is valid.

Another sight to analyze the proposed model is evaluating the model’s efficiency. Here, we want to measure the Model’s Validity Range (MVR) in order to understand the extent of whole “Invalid Behavior Detection”, i.e., if suspicion detections are correct.\

$$RS = \frac{b * 100}{a}\ \%$$

Formula 3. Rate of findings of suspicious users

Formula 3 allows us to understand to what extent user suspicions have been confirmed, by the calculus of RS, in which $b$ is the number of suspect users and $a$ is the number of all active users who have activity on the OSN.

In one hand, more number of detections increases security level of the OSN in accessing to multimedia data, but it would be more persecutor for valid users. On the other hand, obviously, a less number of detections decreases security level, but it would be less annoying for valid users. There is a trade off in getting a suitable RS value for invalid user detections. Therefore, we have to estimate a MVR between two numbers, $\mathrm{RS}_1$, with the most optimistic state and lowest RS value, and $\mathrm{RS}_2$, with the most pessimistic state and highest RS value. Based on this range, we can conclude that the proposed model is effective in both considered aspects of the security and the convenience for users.

## 5. RELATED WORKS

All social networks have considered a specific security structure [26] [27] [28] for users' communications [29] [30] [31], however most of them have an abstract mechanism [32] for accessing to uploaded multimedia contents after a successful login, providing categorized permissions for each user [33]. In a normal situation there is no problem about multimedia exposure, but the problem will rise when a fake authorized user tries to access to all multimedia information accessible by an actual user. With the current architectures, a stranger can easily request multimedia information by clicking on related links after a successful login. For that, it is sufficient the username and the password of an actual user, which s/he can get from an actual user by asking him/her, or stealing by hacking his/her account. So, about users' authentication, current security models often work only on base of SSO and almost there is no appropriate checking about user validation after login. Consequently, user can navigate all sections of a user profile and have access to all private multimedia resources. This is an actual tragedy.

For a legitimate access, in this work a more effective mechanism based on two security layers is proposed.

In this paper, six features were introduced to distinguish the right user: (i) the level of using block list, (ii) the people whom the user sends friend request to, (iii) the level of posting on the other people's wall, (iv) the level of tagging friends on the photos or posts, (v) the level of permitting search engines to link to the account's wall to access the posts, and (vi) the people whom the user mostly sends private message to.

With the previous efforts, it was possible for invalid users to do a successful login and have their activities without any mechanism of invalid user detection. But using the mentioned features, even after a successful login which can be occurred by stealing users account information, system can detect the invalid users using the features and prevents continuing their activities.

## 6. CONCLUSION AND FUTURE WORKS

There is no system that can guaranty a certain security for social networks. One of the main purposes of every security model is efficiency enhancement of available frameworks to get higher level of security. Our assessment about other security models for social networks as mentioned in the section V exposes that generally social networks provide their service to global users just through a user name and password which has considerably weak point. On the other hand, there are several methods of accessing to user's authentication information such as social engineering to know user name and password of an account, then a regretful result would be the ability of accessing to all user's multimedia contents by an invalid user.

In the presented model, the security architecture of a social network could be not only based on an SSO authentication, but also a psychological analysis of users' behavior during their activities on the social network.

We believe that the proposed model on OSN will have great results, since a set of user behaviors cannot be faked by an invalid user easily, and each user has his/her specific sight to have activity during a session. The proposed approach provides a convenient platform for a valid user when s/he tries to access his/her multimedia information, without asking unreasonable security question. We try to adjust the sensitivity of the system to valid users, as they remain convenient and secure in OSN. We want to find an appropriate feature vector for our model in which all of its parts are discriminant. The choice of right features has a prominent influence to achieve a correct result. The features must describe one distinct user based on his/her behavior and we have to train the system in how to run the process of feature measurement and feed it to the previous earned vector in order to update it and make it more accurate.

The results of the evaluation, depicts that selecting a vector of proper features leads to right detection of invalid users when they try to have an illegal access to another user account and it is more convenient and accurate to distinguish the actual users, rather than other security models. We could get this conclusion by running two questionnaires. Therefore, even if an invalid user is successful to login to OSN, our security model can detect and get him/her away of OSN.

To improve the proposed system, we have to set up a complete case study on some social networks with a large number of users. As a future work, we will do experiments about this level of users. For implementing of the questionnaires, we had cultural restrictions since they were accomplished in a specific geographical area which the results may be somehow different in comparison to a global system. Later, we will try to establish a more complete system in order to achieve better results. Another effort for the future would be quantify an accurate MVR for our model. This can help to increase the confidentiality ratio of the system besides the security level of OSN in accessing multimedia contents.

## 7. ACKNOWLEDGEMENT

This work has been partially supported by the Spanish MINECO Grant RACHEL TEC2013-47141-C4-4-R.

## 8. REFERENCES

[1] Pei Q., Yan D., Ma L. LZ and LY. A Strong and Weak Ties Feedback-Based Trust Model in Multimedia Social Networks. *Oxford Journals, Comput J*. 2015. http://comjnl.oxfordjournals.org/content/58/4/627.full.pdf+html.

[2] Murugeswari D. TB. Developing Multimedia Services in Mobile Social Networks from Security and Privacy Perspectives. In: *National Conference on Advanced Networking and Applications.* ; 2015.

[3] Zhang K. Exploiting Multimedia Services in Mobile Social Networks from Security and Privacy Perspectives. *IEEE Commun Mag*. 2014.

[4] Zhang Z. A Quantitative and Qualitative Analysis-based Security Risk Assessment for Multimedia Social Networks. *Int J Netw Secur*. 2014.

[5] Yap J. Security rules for social networks won't resolve breaches. 2013. http://www.zdnet.com/security-rules-for-social-networks-wont-resolve-breaches-7000010912.

[6] McDowell M. Staying Safe on Social Network Sites. 2013. http://www.us-cert.gov/ncas/tips/ST06-003.

[7] Donkersley T. Cyber Security II- Protecting Your Social Media Networks - AZ Tech Beat. 2013. http://aztechbeat.com/2013/04/cyber-security-protecting-your-social-media-networks.

[8] Oxenhandler D. Designing a Secure Local Area Network. 2016. https://www.sans.org/reading-room/whitepapers/bestprac/designing-secure-local-area-network-853.

[9] Group SAPSI. *Information Supplement: Best Practices for Implementing a Security Awareness Program*.(2014). https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf.

[10] Pennacchiotti M. PA. A Machine Learning Approachto Twitter User Classification. In: A Machine Learning Approachto Twitter User Classification.; 2010.

[11] Benevenuto F. *Characterizing User Behavior in Online Social Networks.* Computer Science Department, Federal University of Minas Gerais, Brazil.; 2009.

[12] Gyarmati L. TT. Characterizing User Groups in Online Social Networks. 2008.

[13] Jiang J. *Understanding Latent Interactions in Online Social Networks.*; 2010.

[14] Guo L. *Analyzing Patterns of User Content Generation in Online Social Networks.* Yahoo! Inc. USA, ACM; 2009.

[15] M. Maia, J. Almeida VA. *Identifying User Behavior in Online Social Networks.* Federal University of Minas Gerais, Brazil: ACM; 2008.

[16] H. Jinlong L Bin. *Dual-Level Identity and Authentication Model for Internet Multimedia Communications.* Network Research Center, South China University of Technology, China.; 2011.

[17] S. Lian, D. Kanellopoulos GR. *Recent Advances in Multimedia Information System Security.*; 2008.

[18] M. H. Al Shayeji , Gh. A. Al Shiridah MDS. A Secure Framework for Multimedia Protection in Social Media Networks. *Int J Innov Manag Technol*. 2012;Vol. 3:No. 6.

[19] L. M. Aiello GR. *Secure and Flexible Framework for Decentralized Social Network Services.*; 2010.

[20] J. Schrammel, Ch. Köffel MT. *Personality Traits, Usage Patterns and Information Disclosure in Online Communities.* CURE - Center for Usability Research and Engineering, Hauffgasse 3-5, 1110 Vienna, Austria; 2009.

[21] Malécot E Le. *Online Social Network Platforms: Toward a Model-Backed Security Evaluation.* NICT, Japan.; 2012.

[22] Gabillon A. *A Privacy Model for Social Networks.*; 2011.

[23] Benjamin Greschbach, Gunnar Kreitz SB. *The Devil Is in the Metadata – New Privacy Challenges in Decentralised Online Social Networks.* KTH Royal Institute of Technology, Stockholm, Sweden.; 2012.

[24] Hak JK. Online Social Media Networking and Assessing Its Security Risks. *Int J Secur Its Appl*. 2012;Vol. 6(No. 3.).

[25] Coulter R. Social Media and Security: Two Factor Authentication. 2013. http://socialmediatoday.com/robertmcoultergmailcom/1313606/social-media-and-security.

[26] Ehinome JI. *A New Social Media Security Model (SMSM).* University of East London, London, United Kingdom.; 2013.

[27] Ed Novak QL. *A Survey of Security and Privacy in Online Social Networks.* The College of William and Mary, Virginia, United States.; 2012.

[28] Polakis I. *All Your Face Are Belong to Us: Breaking Facebook's Social Authentication.* ACSAC '12 . Orlando, Florida USA: ACM; 2012.

[29] S. Sun KB. *The Devil Is in the (Implementation) Details: An Empirical Analysis of OAuth SSO Systems.* University of British Columbia, Vancouver, Canada.; 2012.

[30] Pfoutz J. The Advantages and Disadvantages of Single-Sign-On (SSO) Technology (mini-whitepaper). 2012. http://secureconnexion.wordpress.com/2012/08/24/the-advantages-and-disadvantages-of-single-sign-on-sso-technology-mini-whitepaper.

[31] Inc. A. Why Business-Driven Single Sign-On for the Enterprise? 2013:P. 2. http://www.aveksa.com/wp-content/uploads/2013/07/WP-Business-Driven-SSO.pdf.

32] Wall K. Choosing and Using Security Questions Cheat Sheet. 2013. https://www.owasp.org/index.php/Choosing_and_Using_Security_Questions_Cheat_Sheet.

[33] Wikipedia. Revised NEO Personality Inventory. 2015. https://en.wikipedia.org/wiki/Revised_NEO_Personality_Inventory.