QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Security Issues in Social Media: Challenges and Solutions

Mardin A. Anwer
Software and Informatics department, College of Engineering, Salahaddin University - Iraq
mardin.anwe@su.edu.krd *(Part time Lecturer at Lebanese French University)*
Rina Dinkha Zarro
Software and Informatics department, College of Engineering, Salahaddin University - Iraq
rina.zarro@su.edu.krd
Kamaran HamaAli Faraj
Computer department, College of Science, University of Cihan-Sulamani – KRG
Computer department, College of Science, University of Sulamani-KRG
kamaranfaraj@yahoo.com

ARTICLE INFO

Article History:

Received: 15 March 2017

Accepted: 1 April 2017

Published: 10 April 2017

DOI:

10.25212/lfu.qzj.2.2.41

Keywords: *Privacy, Personally and business Information, Social Media, secure architecture, secure hash function, two-factor authentication.*

ABSTRACT

The popularity of social networking becomes very important for the societies. It makes life easy and modified the traditional society (TS) to electronical society (ES). Thus, community by using of social networking in every day is more than usual and becomes part of our daily life and without doubt sharing with our life and all around human daily activity helped by Facebook and it is a new way of 21 century communicates. The average use of social media by a normal person is seven hours per day. Social media users share ideas, information and communicate with different people. This communication reveals a lot of information such as private and business information that makes it visible to anyone who wants to view it or it become cross information. Cross information means seen and exchange both of users' information. Subsequently, other people are intending to take advantage of this information. They can send spam or steal identities to sell it or use it for other purposes. This paper introduces new architecture to protect users' accounts that can be use in Facebook. We also introduce some techniques that can be used in any types of social media networking. In addition, our proposed system architecture is increasing the security issue by using of two-tier architecture (2TA) authentication especially enhances user privacy in social website. The new contribution of our proposed system will insure no fraud account or fake identity is created in the network related to the business, as well as, people related to this account, all data and information will be kept private and less spam attacks will be guaranteed. In order to evaluate the proposed architecture tests, some profiles of academic staff

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

and employees in the college of engineering–Salahaddin University were inspected.

1. INTRODUCTION

Online social networks are a kind of virtual communication (VC) that allows people to connect with each other. The importance of staying together as a community is the main idea of social network [1]. Unlike traditional media (TM), social media relies on user-generated content, which refers to any content that has created by end users or the public as opposed to professionals. TM such as radio, books, and network television (TV) is primarily design to be a broadcast platform (one-to-many), whereas social media is design to be a dialogue many-to-many (M2M) interaction [2]. There are many types of social network, which depend on its features. These features are geographic location like Orkut in Brazil, VKontakte in Russia or well-known globally, like Facebook and Twitter or business-oriented like LinkedIn and Xing [3]. Online social media is fully electronic because of participating users and publics and it is (M2M), but TV is semi electronic online social networking because of (one2Many), the traditional for example books is a book for a user. In 1997, the first social networking media emerged. It was called Sixdegrees.com. This site permits the user to create profiles, list their friends and surf the friends list [4]. Starting from 1997 to 2010 there are some 1.5 billion users of social networking websites [5].

This paper is included six sections; related work is outlined in section two, Section three is presenting different kinds of social media-where some statistical data will be introduced about the usage of these kinds, section four explains the privacy issue of using the social media, also the proposed architecture and analysis of the solutions related to security is detailed in section five, Section six is about finding and discussion when applying the proposed design. The final section draws conclusions of the research.

2. Related Works

Many research and white papers discussed the security and privacy issues in social media network. They concluded many solutions related to this concern. Most of them agreed that the user should be aware of the information that posted in the social media. Kevin (2013) did an experiment on 486 students from the University of Cape Town (UCT), South Africa. The data also shows that UCT students perceive friends and total strangers to be their main audiences on Twitter; the attitude of UCT students towards Facebook remained positive, on the other hand, a less positive attitude was experienced from the students using Twitter; and Facebook is a more popular method for communication between students. The results obviously highlight the changes in usage, attitude and perception of Facebook [6]. Brad in 2011 inspected some of risks in three social media websites which are Facebook, Twitter and LinkedIn and identify. He presented possible solutions to help protect the user, user's personal information and user's company data [7]. Brand explained how is possible to identify the legitimate messages from the hoaxes by doing simple steps. Using an up-to-date email client and date antivirus/anti-malware software, also never open an attachment unless it is from someone you know are the main advices from Brand. Giles in 2007 highlighted and addressed privacy and security risks associated with Social Networking

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Sites. He provided recommendations on how to minimize these risks. He offered strategies to improve privacy and security without compromising the benefits of information sharing – thus increasing the overall social value of Social Networking Sites. He promoted Stronger Authentication and Access-control where appropriate Threats: Digital Dossier, Ease of Infiltration, Squatting, Spear Phishing, Stalking, SNS Spam, and Social Aggregators. Similarly, increase transparency of Data-handling [8].

In 2013, Bill et al discussed some of dangers when using social media and how to use these sites more safely. For example, he explained how many social networking sites allow user to use encryption called HTTPS to secure the connection to the site. Some sites like Twitter and Google+ have this enabled by default, while other sites require user to manually enabled HTTPS via account settings [9]. In the same year, Abhishek et al proposed an architecture for secure request response exchange of data between users. This architecture improves the customization of profiles. It suggests that only a proper knowledge of the hacking strategies will prove the best defense in the war against cyber-attacks. According to their architecture, the visitors or friends request for any information to the application between the visitor and the user. The application requests to the user for the response then the user can response from any one of the databases according to his trust on the person who has requested for the information [10].

3. Types of Social Media

Although there are many brands of social media which have its own unique architecture that shapes the types of interactions that can occur [11], they all have the same target, which is sharing a mutual interest and gain a method of interaction or information sharing through the service. Services vary in their scope, the pace of interaction and the type of content that is shared such as videos, images and text. The services control the type of connection between the users, items and data retention policies [12].

Indeed, small changes in the design of social media tools and policies around them can be vital to their success and failure [13]. Table one list the top ten social media on 2016 according to ebizmba website.

TABLE 1. Top 10 social networking sites in the world [13]

Rank	Site	Estimated Unique Monthly visitors
1	Facebook	1,100,000,000
2	YouTube	1,000,000,000
3	Twitter	310,000,000
4	LinkedIn	255,000,000
5	Pinterest	250,000,000
6	Google Plus+	120,000,000
7	Tumblr	110,000,000

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

8	Instagram	100,000,000
9	Reddit	85,000,000
10	VK	80,000,000

In this research will focus on Facebook, however Instagram is similar to Facebook where the user can view posts, images but still cannot be posted from a Web interface without a workaround [14].

4. Privacy Issues on Social Media

A main concern about using social networking sites is privacy. Privacy can be defined as the process of respecting the desires of individuals where compatible with the aims of the larger community. Privacy is not about what people expect but about what they desire. Privacy is not merely an individual right; it is an important component of any flourishing community [15]. When you are online, it means that nothing is private. The problem is that all the information, posts and images that is posted online can last for very long time. Consequently, these posts can be shared all around the world. In 2007, Pew Internet & American Life conclude from their study that 66 percent of teens restrict their online profile by making it private. They found 82 percent teens post their first name, followed by photos of themselves (79%), name of city (61%) and email address (29%). The situation is different for girls. They commonly do not post information that could help in finding their physical location [16]. During the last ten years, academics explored the threat to privacy linked to social media. Gross and Acquits in 2005 analysed 4,000 Carnegie Mellon University Facebook profiles and outlined the potential threats to privacy contained in the personal information [17].

There are privacy settings in every social media site. The user can control their privacy by selecting the best options that suite the user's situation. Figure 1 shows the privacy settings in Facebook.

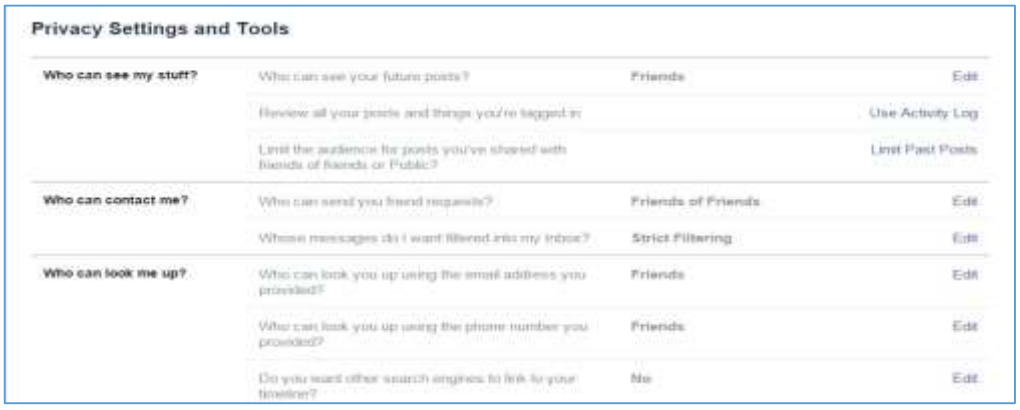

FIGURE 1. Privacy Settings in Facebook

An Instagram users can set their privacy preferences such that their posted photos and videos are available only to the user's followers that requires approval from the user to be their follower. Such actions will appear in referenced user's "Updates" page so that users can keep track of "likes" and comments about their posts. Given these functions, Instagram is regarded as a kind of social awareness stream [18]. Like other social media platforms such as Facebook and Twitter [19]

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

In Twitter social media site, the user has the option of publicly displaying their tweets or keeping them private. Figure 2 shows the privacy Settings in twitter.

FIGURE 2. The Privacy Settings in Twitter

In spite of, the security provided in privacy settings, there are lots of threat regarding this matter. In July 2009, the wife of the chief of the British secret service MI6 posted highly revealing details on her Facebook page. This information included Family details, personal photos and location of their home. This led 200 million people to access this information. This resulted to national security risk Sophos survey 2010 [20].

5. Privacy Solutions and Proposed Architecture

In this section, two-tier authentication for signing in a social network will be introduced. Then some techniques that might be adopted to increase the privacy in social media networks.

5.1 Proposed Architecture for social network

Toward ensuring that the user post correct information in their timeline or be sure that he is the person that he claim to be, the proposal is to scan any ID that confirm this information. Asking the user to scan his or her ID will prevent user to create fake account and pretend to be someone else. Let's suppose that an employee who works in organization AB want to create a Facebook page and introduce himself as an employee in AB Company. It is important that the employee create his account while he is at his office and during week work time. As it is obvious from the diagram when the employee start creating his account in social media the IP address and the location of the company will be automatically discovered. In this case, no user will claim working in specific company even if he steals or use one of another employee ID. This will make the job easy for the government to trace any fake account or any person that involved in blackmail. All the information in the ID will be extracted using OCR engine. In addition, if the phone of the user was lost or stolen, the person who has the phone cannot access the user account because he must use ID for logging in as shown is figure3. When the user enters his username and password to the system these data will be encrypted using secure hash function (SHA-2). A hash function or one-way hash function can be defined as a function that takes an input as arbitrarily long string of bits (or bytes) and produces a fixed-size result [21]. There are SHA-0, SHA-1, SHA-2. SHA-1 is fast, but its speed is a weakness because brute-force attacks can perform faster. Therefore, using SHA-256 (SHA-2) provides more protection against brute-force attacks in spite of

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

being a slower hash than SHA-1. Figure 3 present the proposed architecture for signing up Facebook as an example.

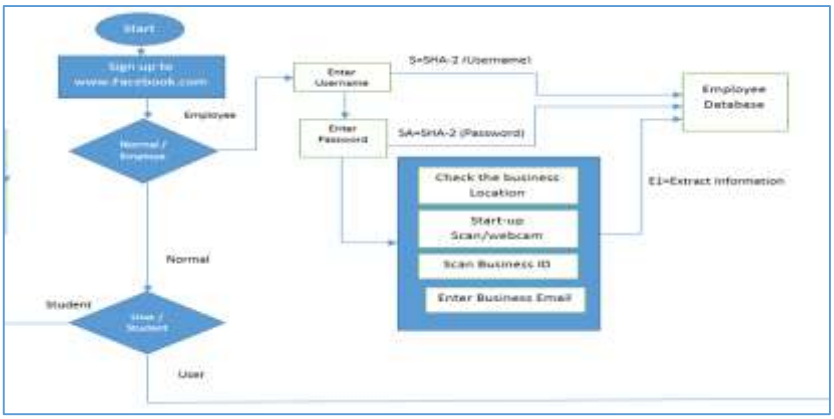

FIGURE 3. The proposed architecture for signing up in social media (Facebook as an example)

The same process is required for normal user. For normal user, it has to categorize them as student or user (any other type except employee and student). If the user is a student, then he should create his account while he is at school. In this case, the location of the school and the ID will be officially identified. For other users, they can create their account at home and use passport for introducing themselves and use their Gmail, yahoo, Hotmail or any ordinary email account. The process of logging in required the user to enter the username, password and his ID. The username and password will be hashed again using SHA-2 and will be compared with the one that is saved in the social media database. If they are correct, then the system will ask the user to scan or upload the ID that is used before in the signing up process. The extracted information for the ID will be compared with the one is saved in the database. If they are the same then the access is granted. When the user enters the work email, a copy of his email should be directed to HR (Human Recourse) office or the manager. Using business email confirm the identity of the user as an employee in this company. This means the responsible is aware of the employees who use their work identity in their social media account. Figure 4 shows the general two tier architecture of our proposed system. Database as a backend is sql server and the middleware is C# for communicate backend and frontend. The connected frontend is a scanner to scan ID and send it to database. Two tier architecture is more than enough for the staff academy of college of Engineering- Salahaden University. The new contribution of our proposed system is security on 2TA. Nevertheless, Figure 5 shows the process of signing in of users.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

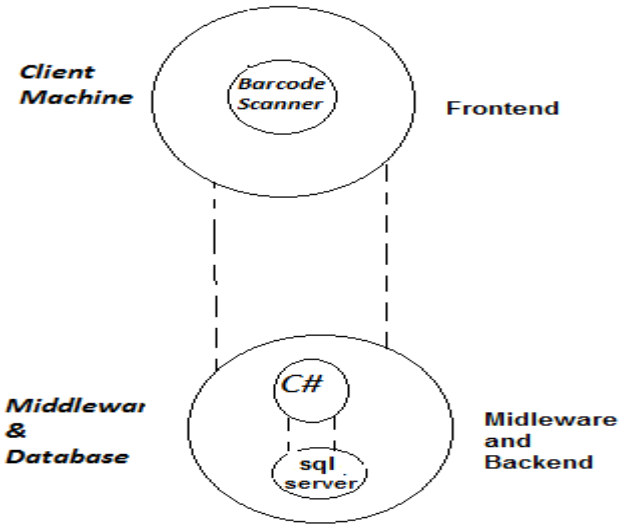

FIGURE 4. Two tier architecture

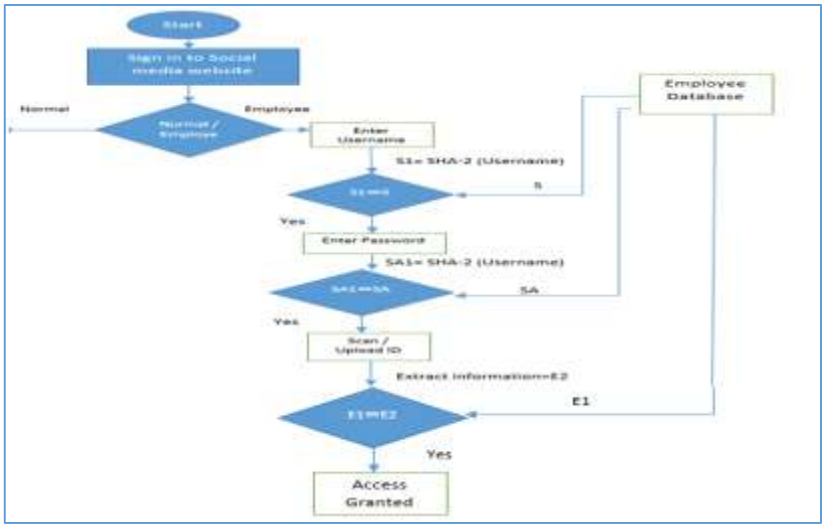

FIGURE 5. The process of signing in

5.2 Technique for Ensuring Security in Social Media

In Instagram, there is the problem of viewing all followers and following. Talking about privacy term it can be said that Facebook introduce more privacy option for their users. Thus, Instagram can provide options that make the account as private and private followers and following. Figure 6 shows the recommend type of account as proposed.

Photos and videos that the user share in social network can give others a clear picture of user's life. It is easy to share photos that show your house number, street name, children's names or office location. Yet, these pictures can be used for other issues. Many social media network users claim that their pictures are downloaded and then uploaded by unknown person or using these pictures as type of threating. Some of social media user upload their pictures in many occasion and some of them might be embarrassing. Today many employers look online profile before giving the job offer, because they do not want to see only one side of employee's personality. The president of a consulting company in Chicago decided to

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

check one of the candidate's Facebook page, and found descriptions of marijuana, shooting people and obsessive sex. Finally, the candidate was rejected for this [22].

FIGURE 6. The recommend type of account

The better solution for this issue is adding an option called 'Allowing download picture' or 'Allow screenshot the picture'. This will restrict the public from using these picture for unwanted matter. Figure 7 shows the setting after adding this option.

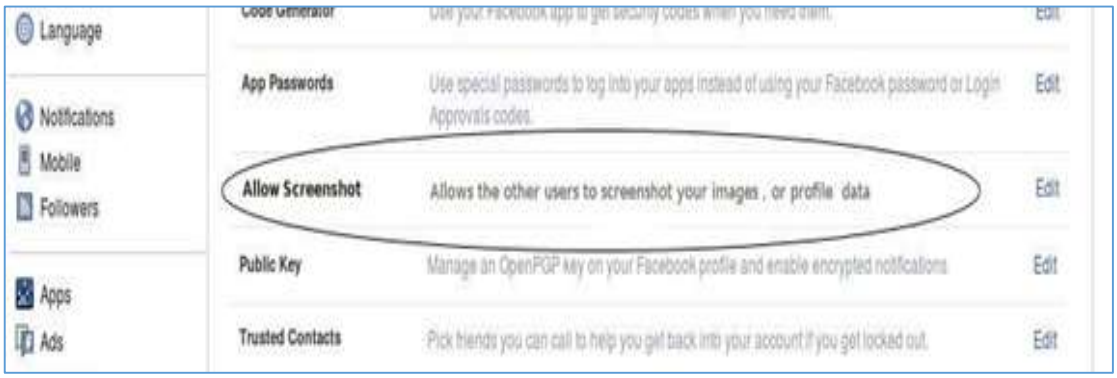

FIGURE 7. Social media settings after adding "Allowing" option

Also, a message can be added to notify the visitor that the account is protected from screen shot as shown in figure 8.

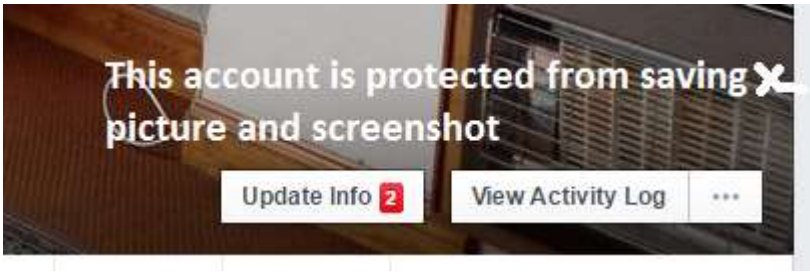

FIGURE 8. Warning message about downloading picture

If the user want to control the process of allowing friend or public to save photo then an option of allow saving would be added. Figure 8 illustrate this option.

To know the number of users that download the picture a button can be added for this matter as shown in figure 10.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

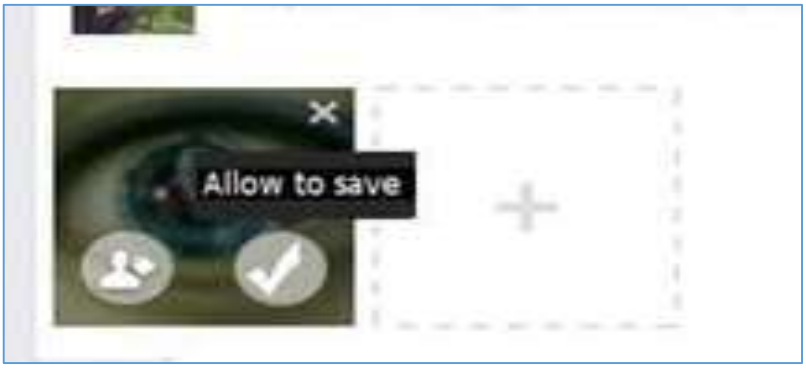

FIGURE 9. Permission setting for downloading and saving image

FIGURE 10. Notifying the user about the number of downloading picture

However, there are many other website which is similar to Facebook and Instagram where they ask people to log in to their account to check new photos of their friends. When the user opens these websites, it looks like a normal social media account such as Facebook. Then after, the user enters the user id and password, without knowing that the account details are being stolen by a hacker. In Instagram, if you have a public account, anyone can see your images. With a private account, only your approved followers can see the photos and videos you share. This option secures your picture from unauthorized users.

6. Finding and discussion

It was very important to select an organization or company to investigate the social media account of their staff. Nonetheless, working in college of engineering and planning unit give us the idea of selecting it as a case study. In addition, the fact of trusting a person to inspect their account would not be easy in any other place. That is why the college of engineering is selected. Although, there are many types of social media, but Facebook is selected because it is widely used by both academic staff and employees. Before applying the proposed architecture, all pages named as college of engineering Salahaddin University's Facebook were located. Unsurprisingly it was found that there is more than one page. This means that the college could not control the problem of creating other fake account created by unauthorized persons. Moreover, it was found that every page claims that it is an official one and users were confused about the official one. Figure 11 shows the different copies of the existing college page.

After locating the official page of the college, the page information was checked. The result was that not all the provided information is correct as shown in figure 12.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

FIGURE 11. Different copies of college of Engineering- Salahaddin University Facebook page

FIGURE 12. Page information of college of Engineering- Salahaddin University Facebook page

Next, after obtaining permission from some academic staff and employees of the college, the information that they provided related to their identity, academic title, position and place of work was investigated for authenticity and authority checking. While reviewing 65 accounts (academic and employees) the following are discovered:

Most of the employees (nearly 70%) do not provide work and personal information about themselves. Where this was less in academic staff nearly 30% as shown in figure 13.

FIGURE 13. Lack of provided information in both academic and employees

Nearly 60% of provided information from academic staff is fake. Some entered academic title which is not correct. There are lots of irrelevant information about their background an example is shown in figure 14. While this occurred less in employee's profile (nearly 20%).

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

FIGURE 14. Irrelevant information in Introduction

To start applying the proposed architecture, the employees in the deanery were asked to open new account using their ID information. Each employee, provided a scanned copy of their ID. Eventually, the authenticity of the information was guaranteed and accessing or request made to the college site where more secure and controlled. The following figure shows the differences between the existing Facebook architecture and proposed architecture according to some security aspects.

As it is shown from the chart, the proposed architecture provides accurate information about the user that want to create account associated to his business. It is crucial that all staff in collage identify themselves with correct information, so it is easy for their colleagues and students to find them. This is also true for any other search engine. As a result, the provided architecture guaranteed two main security aspects. First, when creating accounts related to any company or governmental establishment, the authentication using ID will insure no fraud account is created in the network related to the business, as well as, people related to this account. This will insure all the news and announcements will all be authentic.

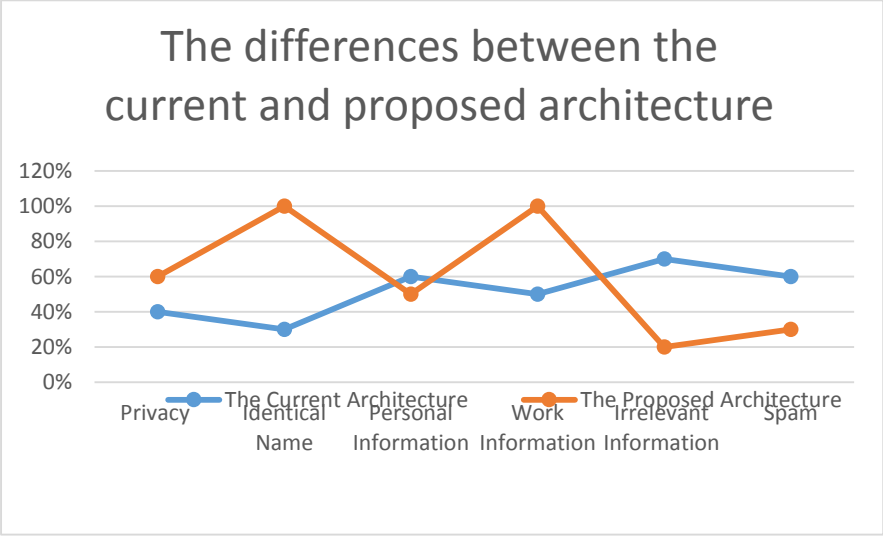

Figure 15. The differences between the current and proposed architecture

Second, the architecture will guarantee the accounts want to associate to the main business account will all be checked and authorized by IT administrator. In this case, all data and information will be kept private and less spam attacks will be guaranteed. In addition,

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

following the above techniques will prevent fraud and hacker to download another user's picture and pretend to be them. By following the techniques, the user can give permission to people who know to download their pictures and create private account.

7. Conclusion

Several seminar-evaluations were hold in Software engineering department regarding social media and the entire seminar participant realized that will be very easy to create fake accounts under specific name. As there is no authentication and authorization checking. That is why it is difficult to be sure that the named account referred to the correct person or business. This means that the security in social media is weak and vulnerable to hackers. Hackers can use these accounts to send spam, spread malware, and steal identities in the quest to acquire personal information for financial gain. In this paper, some techniques to secure user account are suggested. Moreover, a different architecture is proposed for handling security. In this architecture, two-tier authentication is required. When the user signup to the social media site, user name, password and information in the ID card must be entered. The information on the ID is extracted and saved in a specific database based on user's type which is employee or student or normal user. This means-costuming database depends on the type of user to grant access depending on user credentials.

8. Acknowledgment

We would like to thank all who give us the permission to access their account and express their fears of using social media. They inspire us to think deeply about writing a research about providing secure privacy in social media network.

References

[1] Das B., Sahoo J. (2012) "Social Networking Sites – A Critical Analysis of Its Impact on Personal and Social Life", International Journal of Business and Social Science Vol. 2 No. 14. www.ijbssnet.com

[2] Porter, J. (2008). "Designing for the Social Web". Thousand Oaks, CA: New Riders Press

[3] Wüest C.,(2010) "The Risks of Social Networking" Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf

[4] Boyd, d. and Ellison, N. B. (2007). "Social network sites: definition, history, and scholarship". Journal of Computer-Mediated Communication, 13(1). Retrieved from http://jcmc.indiana. edu/vol13/issue1/boyd. ellison.html

[5] Kreutz, C. (2009). "The next billion – the rise of social network sites in developing countries". Retrieved from http://www.web2fordev.net/component/content/article/1-latest-news/69-social-networks .

[6] Johnston K., Chen M., Hauman M., (2013) "Use, Perception and Attitude of University Students Towards Facebook and Twitter" ,The Electronic Journal Information Systems Evaluation Volume 16 Issue 3 2013, (201-211) , ISSN 1566-6379 201 ©Academic Publishing International Ltd Reference this paper as: available online at www.ejise.com

[7] Dinerman B.,(2011)" Social networking and security risks", GFI White Paper.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

[8] Hogben G.,(2007),"Security Issues and Recommendations for Online Social Networks". ENISA, October 2007 E. Retrieved from http://www.ifap.ru/library/book227.pdf

[9] Wyman B., Scrivens W., Hoffman P., Spitzner L.,(2013)" Social Networking Safely "Retrieved from http://www.securingthehuman.org

[10] Kumar A., Kumar G., Rai A., Sinha S. (2013) "Social Networking Sites and Their Security Issues" International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 1 ISSN 2250-3153 www.ijsrp.org.

[11] Lessig, L. (2006). (2009)." 4 reasons why e-records are still a mess£. Federal Computer Week. Code 2.0. New York: Basic. Lipowicz, A. Retrieved from: http://www.fcw.com/Articles/2009/03/09/policy-email-records.aspx.

[12] Hansen, D. L., Shneiderman, B., & Smith, M. A. (2011). "Analyzing social media networks with NodeXL: Insights from a connected world". Burlington, MA: Morgan Kaufmann.

[13] http://www.ebizmba.com/articles/social-networking-websites

[14] Danielle S. (2013), "Moving on from Facebook Using Instagram to connect with undergraduates and engage in teaching and learning"

[15] Lenhart A.,Madden M.,(2009), "Teens, Privacy and Online Social Networks
" . Retrieved from http://www.it.cornell.edu/policies/infoprivacy/definition.cfm

[16] Lenhart A., Amanda B., Madden B., Mary M.. (2007). "Teens, privacy &online social networks". Retrieved from http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks/1-Summary-of-Findings.aspx

[17] Gross, R. and Acquisti, A. (2005). "Information revelation and privacy in online social networks". Proceedings of WPES'05 (pp. 71–80). Alexandria, VA: ACM.

[18] Naaman M., Boase J., Lai C.-H. 2010. "Is it really about me?: message content in social awareness streams In CSCW".

[19] Hu Y., Manikonda L., Kambhampatihttp S., (2013) " What We Instagram: A First Analysis of Instagram Photo Content and User Types ".Retrieved from : //149.169.27.83/instagram-icwsm.pdf

[20] Lewis J.,(2009) MI6 chief blows his cover as wife's Facebook account reveals family holidays, showbiz friends and links to David Irving. Retrieved from http://www.dailymail.co.uk/news/article-1197562/MI6-chief-blows-cover-wifes-Facebook-account-reveals-family-holidays-showbiz-friends-links-David-Irving.html

[21] STALLINGS, W.(2002) "Cryptography and Network Security". Prentice Hall.

[22] Maloney-Krichmar, D., & Preece, J. (2005). "A multilevel analysis of sociability, usability and community dynamics in an online health community". Transactions on Human– Computer Interaction, 12(2), 1–32.