A Secure Framework for Multimedia Protection in Social Media Networks

Mohammad H. Al Shayeji, Ghufran A. Al Shiridah, and M. D. Samrajesh

***Abstract*—Social networking sites usage has seen a rapid growth in recent years worldwide. Social Media Networks (SMN) such as Flickr, YouTube, and Facebook allow millions of users to share their personal information and multimedia content with relatives, friends and other online users. User information, including multimedia content, is being attacked, sold and used illegally by individuals and organizations to increase their revenue. Users are not completely aware of who has access to their private information. In this paper, we propose a new security framework for SMN that protects multimedia content against various types of attacks and illegal usage. This is achieved by using anonymous databases and Captcha implementation at the server and by using two-level user authentication with auto-locking and security+ features. The proposed security framework has been evaluated under different scenarios including human-based attacks, automated program attacks and existing security frameworks. Our evaluation shows that the proposed framework is effective in providing a secure environment for storing and sharing multimedia content in SMN.**

***Index Terms*—Anonymous database, authentication, encryption, security, social media networks.**

I. Introduction

Social Networks is a complex network [1] made of entities which can be either individuals or groups of people who are connected through specific relations such as friendship, business relations, and shared hobbies. Social networks can be mathematically represented as a graph where the vertices represent the involved users and the edges represent the existing relations among them as shown in Fig. 1. In recent years, social networks have witnessed a massive growth leading to networks with millions of nodes [2]-[3].

The popularity of social networks poses a great threat to user information. The social networks user is not aware who accesses her private information [4]. Attackers can get access to her personal information using various methods. Social Media Networks (SMN) are essentially Internet based tools primarily used for entertainment, to facilitate personal collaboration and for the instant sharing of content represented in different forms including audio, image, and video [2].

Manuscript received September 14, 2012; revised October 25, 2012.

Mohammad H. Al Shayeji, Ghufran A. Al Shiridah, and M. D. Samrajesh are with Computer Engineering Department, Kuwait University, Kuwait (e-mail: alshayej@eng.kuniv.edu.kw, al.shiridah@ku.edu.kw, sam@differentmedia-kw.com).

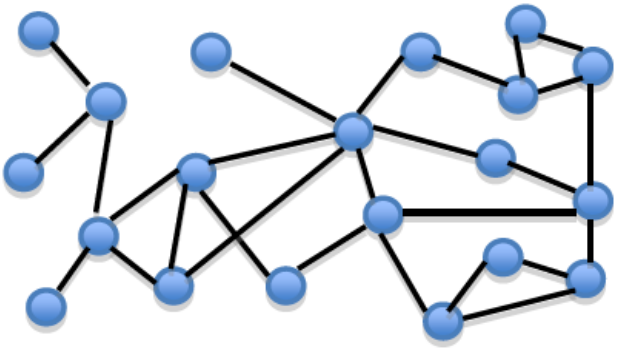

Fig. 1. A typical social network layout

The aim of this paper is to propose and evaluate a security framework that protects and secures multimedia content in SMN by partitioning the database into two separate anonymous databases and securing the server implementation using Captcha security technique. Additionally, a two-level user authentication with auto-locking and security+ feature is proposed.

The paper is structured as follows: section II describes the related work, and section III provides background information about SMN. The proposed security framework is presented in section IV while section V evaluates the proposed framework by introducing two scenarios of attacks. Finally, in section VI, we present our concluding remarks and suggestions for future work.

II. Related Work

A security framework to protect corporate information against threats related to social networks services was proposed in [5]. The framework was evaluated by considering a company with more than 1000 employees. However the proposed framework focused only on an organization. It considered well-known threats and prepared for unknown threats, related to social networks services usage, to handle security risks that arose from the combination of businesses and social networks services.

A study on threats to social networks, and the methods used by attackers and possible targets for such attackers, was presented in [6]. The study separated social networks into two parts and proposed a security framework. The proposed security framework was based on giving suggestions to the social networks users to pay more attention to the security of user information. This was done in the application layer using traditional security measures and this did not consider the security of multimedia content.

Misuse of social network sites by the irresponsible behavior of users was studied in [7]. Here they compared two

DOI: 10.7763/IJIMT.2012.V3.315

groups of fictive profiles and studied their success in creating new links in social networks. They also considered tools for protecting sensitive information in social networks. However, the study focused only on knowing how social networks users deal with their sensitive information and how their behavior can affect the ability of attackers to misuse information.

Security and privacy design issues on Online Social Networks (OSNs) is discussed in [8]. The paper presented the unique security and privacy design challenges brought by the core functionalities of OSNs. However the paper only highlighted few opportunities of utilizing social network theory to mitigate the security and privacy design conflicts.

Most of the above work focuses on online social networks while our work focuses on the social media networks in particular. Additionally, the existing solutions attempted to secure either the structure of the social networks or to protect user information from being misused by attackers. However, our proposed solution protects the multimedia content in the SMN on both the server as well as the application side by providing additional level of security.

III. Background

Social media networks can be defined as those social networks that use multimedia content shared for social interaction. There are different types of social media networks including; social bookmarking, social news, social networking and social photo and video sharing. The rapid growth of multimedia content and transmission in digital form in SMN has a variety of challenges including unauthorized access; this creates a need for multimedia security and protection in SMN [9]. Many techniques and algorithms for protecting multimedia data have been presented in [10]. In our framework we propose using Captcha, Captcha prevents automated program from accessing the servers using distorted image that consists of letters and digits which need to be typed to ensure human access. This technique is being used by many applications [11] such as online polls, email services and much more.

Cryptography is necessary when communicating through any un-trusted medium and this includes the Internet [10]. Cryptographic schemes Hash Function, and the Public Key Cryptography uses two keys, one for encryption and the other for decryption that uses RSA and Diffie-Hellman algorithms [10]. Database encryption is achieved in SMN by transforming plain text into a partially encrypted text making information unreadable for unauthorized persons and intruders [11].

IV. Proposed Framework

The proposed security framework consists of 4 major components as shown in Fig. 2. These components are described below in detail.

A. SMN Website Design

In the design component of the framework, the developers of the SMN design the web application and decide the hardware and software resources required for SMN. Additionally identify the main objectives of the SMN website and the target audience.

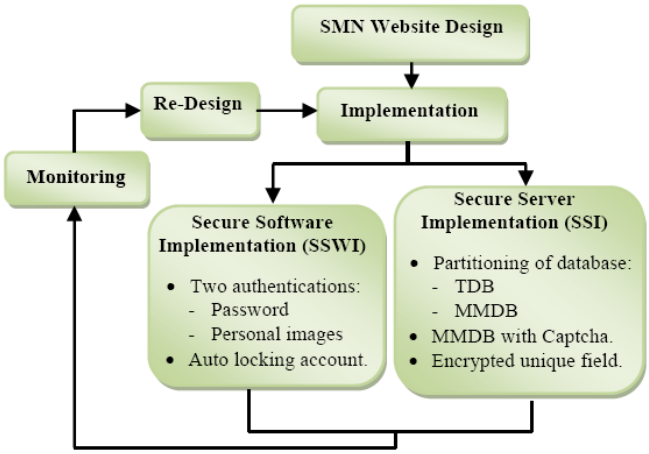

Fig. 2. Proposed SMN security framework

B. Implementation

The implementation component of the framework consists of two sub-components: Secure Server Implementation (SSI) and Secure Software Implementation (SSWI).

1) Secure server implementation (SSI)

Databases represent an important component in SMN, thus its security is crucial [13]. Privacy and data confidentiality in SMN databases is vital. This sub-component guarantees the protection of SMN database from the automated program attacks that target the server side of SMN. The implementation is based on the following.

a) Partitioning of database

To achieve maximum security to the content of SMN database, database is separated into two anonymous databases; Multimedia Database (MMDB) for multimedia content, and Text Database (TDB) for text content. In an anonymous database the identifying information is removed from the original database to protect personal or private information [13]. This type of databases is widely used in medical applications [14] to protect sensitive information of patients to maintain confidentiality. If an attack succeeds in accessing one of the databases, it is of no use unless the attacker succeeds in accessing the other database and combines the entire database to generate useful information. In our framework, we use Captcha to prevent automated program from accessing the MMDB.

The separation of the database incurs additional effort in maintaining and monitoring the database. Also it can degrade performance due to the need to merge the data. However, it achieves a higher level of security and protection for the user's private information and database content. Moreover, separation of the databases allows parallel access thus minimizing the performance degradation due to the data merging mentioned above.

b) Encryption

Even when database is anonymous, data confidentiality is required. The data owner would not be pleased if an unauthorized user viewed her wedding video even if the unauthorized user didn't know the identity of the video's owner. Data confidentiality is about protecting user data from

unauthorized access [13]. It can be achieved through having access policies and standard cryptographic tools. In our case RSA (Rivest, Shamir and Adleman) [10], cryptographic technique is applied on the unique 'username' field which is used to link the two anonymous databases. RSA's mathematical strength derives from the ease in calculating large numbers and the difficulty in finding the prime factors of those large numbers [10].

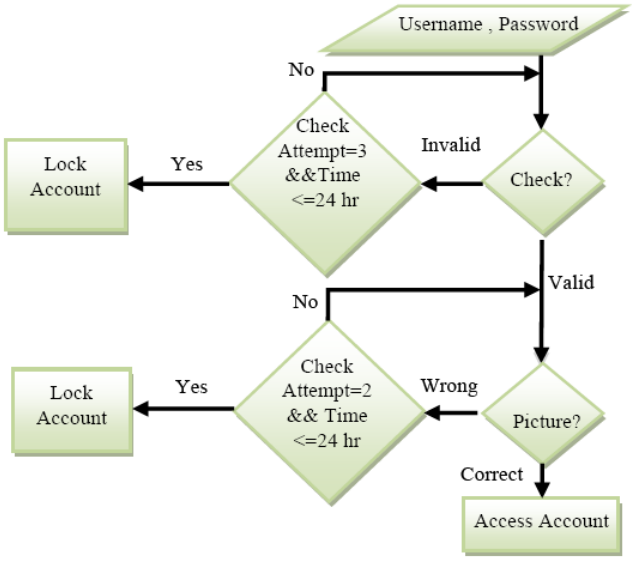

Fig. 3. Secure software implementation (SSWI)

2) Secure software implementation (SSWI)

This sub-component focuses on handling the human attacks by providing an additional level of authentication, including auto-locking and security+ features to protect the user's account as shown in Fig 3. The process of signing up is made by entering a unique username then a password. Next, the user is required to upload 10 personal images. This provides the second level of security. When the signup process is successfully completed, the user becomes a member in the SMN website. When an existing user needs to access her account, the user has only three opportunities within 24 hours to enter the correct password. If she fails, the account is automatically locked. This auto-locking feature within a short period of time provides a higher level of protection for the accounts from human attacks.

After the user passes the first level of authentication, the screen displays 10 random images two of which is selected from the personal images that the user has uploaded during account creation. The user is required to choose the correct personal images she uploaded earlier. The user has only two chances to choose the correct pictures within 24 hours. If she fails, then the account is locked. Moreover, the second level of authentication is more secure and each time the user chooses the wrong pictures, the page is re-loaded with new images selected randomly. Considering the following conditional probability equations: [15]-[16].

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \text{ for } 0 \le k \le n \quad (1)$$

$$p[a \wedge b] \vee p[a \wedge b] = \frac{1}{\binom{n}{k}} \quad (2)$$

where 'p' is the probability of success, 'a' and 'b' the events, 'n' is the set of images, 'k' is number of images chosen. The probability of choosing the right image is at minimum, since 2 images should match and the number of attempts is restricted to 2.

The auto-locking feature provides additional higher level of security. Once the account is locked, a notification e-mail or message is send to the owner of the account informing that the account has been locked for security issues. Only the owners of the account can un-lock the account. Furthermore security+ feature is invoked for the next 24 hours to provide additional security to recently un-locked accounts, this safeguard from attackers trying to re-attack. In this process each of the 10 uploaded images are vertically equally divided into two segments and during the above time period the vertically segmented picture is displayed for user authentication. Additionally yet another optional settings that can be activated during the un-locking of account, is that SMN requests the owner of the account to update the uploaded personal images. The above additional security features provide enhanced security in SMN.

C. Monitoring

This component of the proposed framework is responsible for keeping track of the access to the SMN. The monitoring helps the developers to find attempts to attack SMN. Monitoring is performed using various analysis software tools that are installed on SMN. Software, hardware resources up-gradation is identified in this component.

D. Re-Design

This component of the proposed framework deals with re-designing the SMN to apply the enhancements or updates that had been identified during the monitoring phase. Re-designing hardware or software resources based on the current need is an essential component in the framework as it makes the SMN website perform efficiently.

TABLE I: FRAMEWORK COMPARISONS

S#	Framework	Type of Solution	SMN	Multimedia
1	Gilberto Tadayoshi [5]	Security Framework	✓	×
2	WeiminLuo [6]	Study and Security Framework	✓	×
3	Susanto, H [17]	Security Architecture	×	✓
4	A Secure Framework for Multimedia Protection in Social Media Networks – Proposed Solution	Security Framework	✓	✓

V. EVALUATION OF THE FRAMEWORK

A. Automated Program Attack

The existing single database server SMN has its advantages and disadvantages. The main advantages of this structure are: (1) it saves money, (2) it is easy to maintain,

and (3) the time needed for monitoring is less. In addition, this traditional architecture has the advantage of being straightforward and easy to implement [17]. However, the centralized management of SMN leads to bottleneck that affects network performance [18]. Moreover when attacker access the database through an automated program the probability of accessing the database is high since these automated programs can discover the passwords that consist of characters and numbers easily, even if the database is protected using other security tools.

The proposed server implementation overcomes the above weakness, by having two anonymous databases with the encrypted unique field in both databases. The probability of accessing the MMDB is very low since it is protected using Captcha security technique. Moreover when the automated program attack accesses the TDB or MMDB it has no useful information since the databases are anonymous. Additionally unauthorised merging the data in the two databases is not possible since the unique fields are encrypted.

B. Human Attack

The software side implementation in existing social media networks [19]–[22] depends on only one level of authentication. Hence, if a human attacker knew the username of any account, then he may discover the password of that account by trying to enter various combinations of the password several times until he succeeds. The probability of success is high when the attacker knows the person of that account or any other related information about her. Moreover the password consists of only characters and numbers.

The proposed implementation provides more security. When an attacker tries to access any account he faces difficulties in passing through the new security implementation, he has only three chances in 24 hours to enter the correct password after that the failed account is locked and he cannot access the account unless un-locked. Moreover, when the attacker discovers the password and completes the first level of authentication, he faces the second level of authentication, which is requires the attacker to choose two personal images the user had uploaded when creating the account. The probability of attacker choosing the correct images is minimum since the images are displayed along with 8 other images that are randomly chosen from the database.

The attacker has only two chances in 24 hours to retry and in each chance when the attacker fails to choose the correct images, the images are changed randomly. The permutation of 'n' images using equation (1) (2),

$$\binom{n}{k}=45$$

The probability of choosing the correct pictures in either attempt is minimum since attacker has to choose 2 correct images.

$$P\ (P_1\ V\ P_2) = (1/45) = 0.022 = 2.2\%$$

Moreover, the locked account is un-locked only by the owner. Once the account is un-locked, the *'Security+ feature'* is activated on the next login and it is enabled for the next 24 hours to provide enhanced security, additionally the uploaded images can be updated by the owner while unlocking.

C. Other Exiting Frameworks

Currently available security frameworks for social media networks are more general and do not consider the importance of multimedia content. Table I shows the comparison of the framework and their support for SMN and Multimedia.

VI. Conclusion and Future Work

The growth of SMN and multimedia content have contributed to a wide spread misuse of multimedia content, the challenge is to have a more secure SMN. We have proposed a security framework for multimedia protection in SMN using both server and software implementation. The secure server implementation uses two separate anonymous databases with Cpatcha 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 the human attacks.

Our evaluation of the framework shows that the proposed framework is effective in providing a secure environment for sharing and storing multimedia content in SMN. In future we plan to conduct large scale simulation study on SMN based on the proposed framework for further evaluations.

References

[1] M. E. Newman, "The Structure of Complex Networks," *SIAM Review*, vol. 45, no.2, 2003.

[2] P. Campisi, E. Maiorana, and A. Neri, "Privacy Protection in Social Media Networks a Dream That Can Come True?" in P*roc. the 16th international conference on Digital Signal Processing (DSP'09). IEEE Press, Piscataway, NJ, USA*, pp. 254-258, 2009.

[3] R. Gross and A. Acquisti. "Information Revelation and Privacy in Online Social Networks," in *Proc. the 2005 ACM Workshop on Privacy in the Electronic Society (WPES '05). ACM, New York, NY, USA*, pp. 71-80, 2005

[4] B. Krishnamurthy and C. E. Wills. "Characterizing privacy in online social networks," in *Proc. the First Workshop on Online Social Networks (WOSN '08). ACM, New York, NY, USA*, pp. 37-42, 2008

[5] G. T. Hashimoto, P. F. Rosa, E. Filho, and J. Machado, "A Security Framework to Protect against Social Networks Services Threats," in *Proc. the 2010 Fifth International Conference on Systems and Networks Communications (ICSNC '10). IEEE Computer Society, Washington, DC, USA*, pp. 189-194, 2010

[6] W. Luo, J. Liu, J. Liu, and C. Fan, "An Analysis of Security in Social Networks," in *Proc. the 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC '09). IEEE Computer Society, Washington, DC, USA*, pp. 648-651, 2009

[7] J. Nagy and Pe. Pecho, "Social Networks Security," *IEEE – Third International Conference on Emerging Security Information, Systems and Technologies*, 2009.

[8] C. Zhang, J. Sun, X. Zhu, and Y. Fang. "Privacy and Security for Online Social Networks: Challenges and Opportunities," *Network. Mag. of Global Internetwkg*. vol. 24, no. 4, July 2010

[9] R. Ridzo and D. Levicky, "Multimedia security and multimedia content protection," *51st International Symposium ELMAR*, pp. 28-30, September 2009.

[10] G. C. Kessler. (1998). *An Overview of Cryptography*. [Online]. Available: http:/garykessler.net/library/crypto.html

[11] L. Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using Hard AI Problems for SECURITY," *LNCS, Advances in Cryptology — EUROCRYPT 2003*, vol. 2656, 2003.

[12] L. Bouganim and Y. Guo, "Database encryption," *Encyclopaedia of Cryptography and Security. Springer,* 2010
[13] A. Trombetta, Wei Jiang, Elisa Bertino, Lorenzo Bossi, "Privacy-Preserving Updates to Anonymous and Confidential Databases," *IEEE Transactions on Dependable and Secure Computing,* pp. 578-587, July/August, 2011.
[14] L. Sweeney, "Guaranteeing anonymity when sharing medical data, the Data fly system," in *Proc. Journal of the American Medical Informatics Association,* 1997.
[15] W. A. Rosenkrantz, "Introduction to Probability and Statistics for Scientists and Engineers," *McGraw-Hill Series in Probability and Statistics, International Edition*.
[16] Binomial Coefficient. (2012). [Online]. Available: http://en.wikipedia.org/wiki/Binomial_coefficient.
[17] H. Susanto and F.Muhaya, "Multimedia Information Security Architecture Framework," *5th International Conference on Future Information Technology (FutureTech),* 2010.
[18] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and Security for Online Social Networks: Challenges and Opportunities," *IEEE Network*, July/August 2010.
[19] Facebook. [Online]. Available: http://www.facebook.com
[20] MySpace. [Online]. Available: http://www.myspace.com
[21] YouTube. [Online]. Available: http://www.youtube.com
[22] Flickr. [Online]. Available: http://www.flickr.com

Mohammad H. Al Shayeji received his B.Sc. (Eng), from University of Miami , and M.S. (Computer Science) from University of Central Florida. He got his Ph.D. in the field of Computer Science and Engineering from University of Southern California. Currently he is working as Assistant Professor in Computer Engineering Department, College of Engineering and Petroleum, Kuwait University. He has several publications in different international Journals and Conferences. His research interest includes VOD, Video Servers, Multimedia DMS, and Distributed Systems.

Ghufran A. Al-Shiridah holds a BS in Computer Engineering from Kuwait University and she is undergoing MS in Computer Engineering from Kuwait University. She is a member of IACSIT, IEEE-CS and ACM. She is senior Computer Engineer, Teaching Assistant and website administrator in the Computer Engineering Department, College of Engineering and Petroleum, Kuwait University. She has some publications in some international Conferences and Journals. Her research interest includes Data Mining, Social Networks, Complex Networks, Information Management and Security.

M. D. Samrajesh received his B.Sc, from Bharathiar University, and MCA from Bharathidasan University. He got his M.Phil in the field of Computer Science from MS University. He is a member of IACSIT, IAENG, CSI. He has many publications in various national and international Conferences and Journals. His research interest includes Software Engineering, Distributed Systems, and Video-on-Demand.