Research Article Impact Factor: 4.226 ISSN: 2319-507X
Arpita R. Bhoyer, IJPRET, 2016; Volume 4 (9): 143-149 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURE SOCIAL DOCUMENT SHARING SYSTEM USING THREE LAYERED SECURITY MODEL

MISS. ARPITA R. BHOYAR

Department Of Computer Science and Engineering, Prof. Ram Meghe College of Engineering and Management, Badnera –Amravati (India)

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Social Network Services (OSNs) are today one of the most popular interactive medium for communication, sharing, and disseminating a considerable amount of human existence information. It involves exchange of several types of content, including free text, picture, audio, and video data. However, OSNs face a large number of attacks that affects the privacy and security of users. So, a new community network is designed for enabling privacy security for the OSN users by offering them a secured and favourable network. Here, we use a group key agreement problem where a user is only aware of his neighbours while the connectivity graph is arbitrary. Key agreement is a mechanism that allows two or more parties to securely share a secret key.

Keywords: Social Network Services (SNS), Security,

PAPER-QR CODE

Corresponding Author: MISS. ARPITA R. BHOYAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Arpita R. Bhoyer, IJPRET, 2016; Volume 4 (9): 143-149

1. INTRODUCTION

Network security is the field for securing computer network infrastructure. Though, it looks complex it plays a vital role in protecting computers from viruses and threats sent over the

network. In today's world many researches have been made to improve the security by inventing new technologies. These technologies mainly focus to be faster and efficient.

A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network. Here, we use a group key agreement problem where a user is only aware of his neighbours while the connectivity graph is arbitrary. Key agreement is a mechanism that allows two or more parties to securely share a secret key .It is very suitable for social networks.

2. PROPOSED WORK

In today's world, we use different social networking sites to connect with people for communication and sharing of data. It involves facebook, skype, we chat, twitter etc. But, there are many privacy issues regarding these social sites. So, for this purpose we use a secure social document sharing system using three layered security model. It suggests some possible solutions to secure social network services users from privacy and identity thefts attacks. To implement new security techniques we use:

1. Identity Verification

2. Graphical Password Authentication

3. Group Key Access Protection

3. RELATED WORK

It discusses the works related to privacy and security in OSN. For privacy protection mechanism for social networks OSN uses Privacy Manager. The (Privacy Manager) automatically generates access rules for users profile information. These access rules are generated on the basis of users' privacy preferences on their data in the profile, the sensitivity of the data with respect to the privacy settings of the user. Hence, Privacy manager reduces the chance of accidental disclosures due to outdated policies. A new attack called Identity Cloning Attack (ICA), which focuses on forging user profiles on OSNs, has been introduced. The key goal of an adversary in ICA is to obtain personal information about a victim's friends after successfully forge the victim,

and to establish increased levels of trust with the victim's social circle for future deceptions. In this attack, the adversary first tries to find ways to obtain a victim's personal information, such as name, location, occupation and friends list from his public profile on OSNs or his personal homepage(s). Then, the adversary forges the victim's identity and creates a similar or even identical profile on OSN sites. In order to detect fake identities on OSN sites, a detection process is designed .Existing approaches to Users often create memorable passwords that are easy for attackers to guess, but strong system-assigned passwords are difficult for users to remember .The alternative authentication method is using both "secret key" and "Graphical password schemes" as a passwords instead of text based schemes authentication, which humans can remember pictures better than text. The group key agreement with an arbitrary connectivity graph, where each user is only aware of his neighbours and has no information about the existence of other users. A group key agreement with these features is very suitable for social networks.

4. OBJECTIVE

- The objective of this project is to develop a secure social document sharing system using three layered security model.
- For this purpose, there is a use different security techniques which gives privacy security to social networks.
- The identification image and Security questions are easy to remember for real user and difficult for attacker.
- Account locking and notification system.
- Unbreakable Three layered security model.

Three Layered Security Model:

The proposed work contains a novel based three-tier framework namely, Key Generator (KG), ECC in OSN, and Two Factor authentication. Each phase has its own mechanism and acts as a base for the very next level. Asymmetric Key Generator (KG) using Elliptic Curve Cryptography Algorithm (ECC), simply called Key Generator (KG) generates a unique key for every client once the authentication is given to the user. It stores the unique key in the Data Base Manager inside the server. The key is encrypted using ECC algorithm for security reasons. The basic idea of the proposed framework is to embed the concept of key generation with the existing ECC algorithm to be used in the OSN's. Besides, that the framework also presents a two factor authentication

to the users to protect them from privacy and identity theft attacks. OSN user's an advanced security a new level is introduced with the framework using two factor authentications. Two factor authentication means a user can have two passwords whereas one password is of alpha numeric and the other is a graphical image.

5. OPERATIONS

To develop a secure social document sharing system using three layered security model we use different security techniques. These are as follows:

Techniques:

- User management
- Identity verification
- Graphical Password Authentication
- Group Key Access Protection
- Account Locking/unlocking system

User Management:

It includes-

- Registration
- Login/Logout
- Send friend request
- Accept friend request
- Group management
- Upload/encrypt documents
- Download/decrypt document
- Password

Identity Verification:

- Identity verification technique is used to verify user's identity using his security questions and answers.
- User will register his personal information in the form of security question and answers.
- System will randomly select any one question and its answer to encrypt his personal information in database.
- When user wants to perform any operation regarding particular module ie uploads, downloads, edit profile etc user have to prove his identity using security questions and answer.
- If user specifies correct answer, he will be considered as legal user.

Graphical Password Authentication:

- In this system, user have to select level wise authentication images from image collection.
- User can upload his own image categories as well as icon images.
- If user don't want to upload his own images, he can use ready-made images uploaded by admin.
- At the time of authentication, shuffled image matrix of image collection will be displayed by the system.
- If user clicked on correct images, the user will be considered as correct user.

Group Key Access Protection:

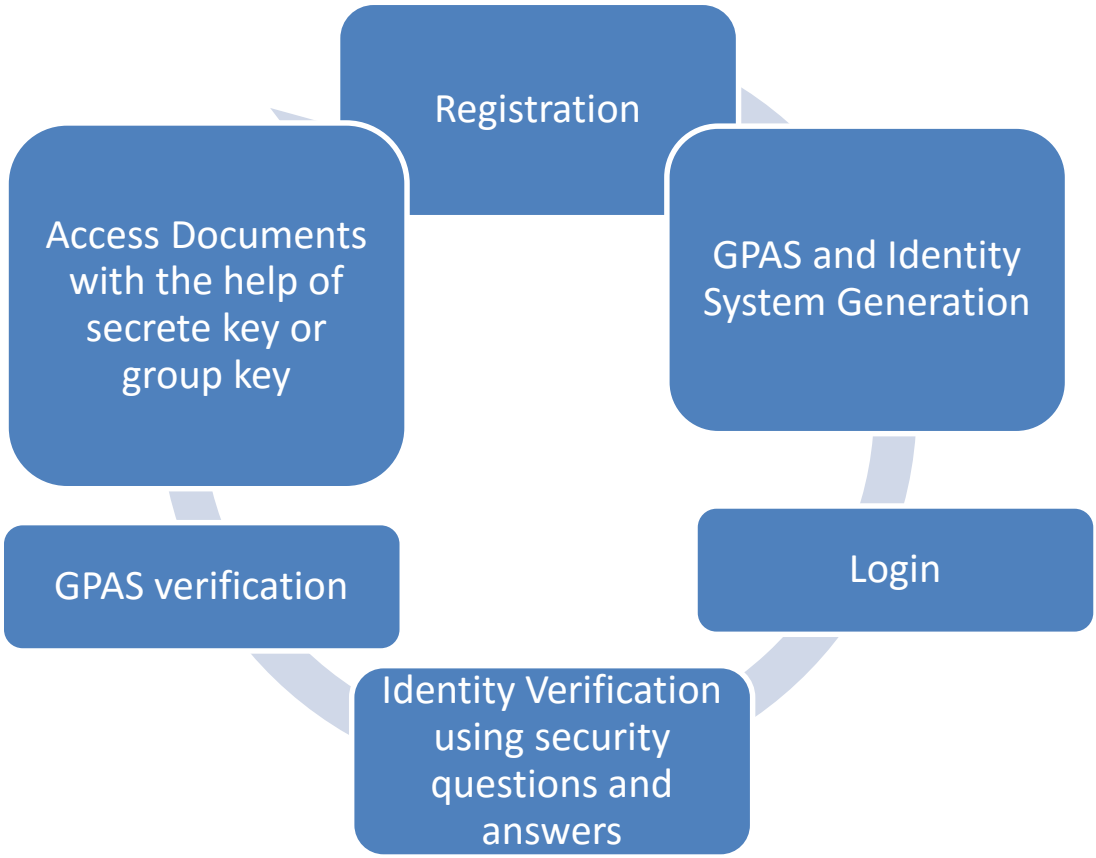
- Every user will create group secrete keys and send it on email ids of group members.
- When group member wants to access friend's document, he/she have to specify his group key to decrypt the document.

Account Locking/Unlocking System:

- At the time of authentication, user have to specify correct password within 3 attempts.
- If user is unable to specify correct password within 3 attempts, the system will get locked automatically and notification will be sent on users email id.

- User can unlock his account by logging into system with correct password.

WORKING DIAGRAM:



6. CONCLUSION

Technology has to be developed enormously by offering the user high security and privacy. Hence, in this paper a new community network is proposed with three components embedded with one another to prevent user from privacy and identity theft attacks. In future, this work can be extended as a middleware application that analyzes more factors like security levels, security policies, trust rating and monitoring malicious attacks. Also there is a group key agreement problem, where a user is only aware of his neighbours while the connectivity graph is arbitrary. In addition, users are initialized completely independent of each other. A group key agreement in this setting is very suitable for applications such as social networks.

7. REFERENCES

1. Aaron Beach, Mike Gartrell, Baishakhi Ray, Richard Han," Secure Social Aware: A Security Framework for Mobile Social Networking Applications," in Proc. IEEE International Conf. on 2012, pp. 439-446.

2. Van Zhu, Zexing Hu, Huaixi Wang, Hongxin Hu, Gail-JoonAhn, "A Collaborative Framework for Privacy Protection in Online Social Networks,"in Proc. 6thAnnu. IEEE International Conf. on 2010, pp. I - 10.

3. Anna Squicciarini, Federica Paci, SmithaSundareswaran, "PriMa: An Effective Privacy Protection Mechanism for Social Networks," in Proc. 3'dAnnu.IEEE International Conf. on 2010.

4. Salehi-Abari, J. Thorpe, and P. van O orschot, "On purely automated attacks and click-based graphical passwords," in Annual Computer Security Applications Conf. (ACSAC), 2008.

5. K. Yongdae, P. Adrian and G. Tsudik, "Group Key Agreement Efficient in Communication", IEEE Trans. Computers, vol. 53, no.7, pp. 905-921, 2004.

6. E. Bresson, O. Chevassut and D. Pointcheval, "Provably Authenticated Group Diffie-Hellman Key Exchange the Dynamic Case", Proc. 7th Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT'01), vol. 2248, pp. 290-309, 2001.

7. Y. Amir, Y. Kim, C. Nita-Rotaru and G. Tsudik, "On the Performance of Group Key Agreement Protocols", ACM Trans. Inf. Syst. Secur., vol. 7, no. 3, pp. 457-488, Aug. 2004.

8. A. Beimel and B. Chor, "Communication in Key Distribution Schemes", Proc. Advances in Cryptology (CRYPTO'93), vol. 773, pp. 444-455, 1994.