International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

A REVIEW ON PRIVACY OF PHOTO SHARING ON SOCIAL MEDIA NETWORKS

1. S CHITTIBABULU, ASSOC.PROFESSOR, ADITYA COLLEGE OF ENGINEERING, SURAMPALEM, MAIL ID: chittibabulu_cse@acoe.edu.in.2

2.J L SARWANI THEEPARTHI, ASSISTANT PROFESSOR (SENIOR GRADE), DEPT.OF CSE, ADITYA COLLEGE OF ENGINEERING AND TECHNOLOGY, SURAMPALEM Mail ID: sarwani.theeparthi@acet.ac.in

ABSTRACT

Photo sharing is an attractive feature that makes online social networks (OSNs) popular. Unfortunately, allowing users to freely post, comment, and tag a photo can violate their privacy. In this paper, we try to solve this problem and investigate the scenario where a user shares a photo with people other than himself (called co-photo for short). To prevent the possible loss of privacy of a photo, we develop a mechanism that allows each person in a photo to be aware of the posting activity and participate in the decision-making about the photo posting. To this end, we require an efficient facial recognition system (FR) that can recognize everyone in the photo. However, more sophisticated privacy settings may limit the number of publicly available photos for training the FR system. To deal with this dilemma, our mechanism attempts to leverage users' private photos to develop a personalized FR system that is specifically trained to distinguish possible co-owners of a photo without revealing their privacy. We also develop a distributed consensus-based method to reduce computational complexity and protect the private training set. We show that our system outperforms other possible approaches in terms of recognition rate and efficiency. Our mechanism is implemented as a proof-of-concept application for Android on Facebook's platform.

INTRODUCTION

With the great popularity of sharing and extensive use of social networking sites, users unknowingly disclose certain personal information. Social networking users may or may not be concerned that their personal information could be leaked or fall into the hands of malicious attackers and result in significant privacy breaches. In the last decade of the 21st century, the Internet has become extremely widespread and there are more and more web services that facilitate information sharing and collaboration. Social networking sites (SNSs) have become a borderless communication medium to stay in touch across borders. SNSs are a part of human culture and not just a web application. SNSs are used in almost all fields, such as news agencies, large and small companies, governments, famous people, etc., to communicate with each other. With the worship of sharing, Facebook has stood out as the most famous SNS in the world where people hang out for hours. With the extravagance of technology and services, sharing news, photos, personal likes and information with friends and family has become a breeze. At the same time, however, user privacy should also be considered. One issue related to Facebook users' privacy keeps popping up in the international press, either because of the company's privacy policies or because users are unaware of the consequences of sharing content. According to one study, simply disclosing a professional's date and place of birth on Facebook can be used to predict a U.S. citizen's Social Security Number (SSN). Often, users disclose a large amount of information by simply posting their friend list.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

For example, by using predictive algorithms, it is possible to infer private information that was not previously disclosed. Sometimes the sensitive information is even embedded in the photo as metadata and can identify the people in the photo by adding other information such as captions, comments and photo tags that could be analyzed. Even if the people in a photo are not explicitly identified by photo tags, the combination of publicly available information and facial recognition software can be used to infer a person's identity. This type of problem is called collateral damage: Users unintentionally compromise their own privacy or that of their friends when they conduct events on SNSs such as Facebook.

LITERATURE SURVEY

in 2006, Barbara Carminati, Elena Ferrari, and Andrea Perego [3] presented a system consisting of policies in the form of constraints on the type, depth, and trust level of relationships present in the access control model for Web-based social networks (WBSNs). The authenticity of the relationships is represented in terms of certificates, and a rule-based approach is used on the client side to provide access control where the user requesting access has full rights. The system does not use the relationship between users to grant access, as the relationship is not necessarily an important issue. Instead, the trust factor and the depth of the relationship between users are very important, based on which access is granted. A rule-based access control model is proposed for WBSNs, which allows setting access rules for online resources, where the relationship between authorized users in the network is specified in terms of relationship type, relationship depth, and trust level.

In this system, the certificates specified by users are stored and managed by the central node of the network, while the storage of access control and the implementation of access control are performed by a set of peripheral nodes. In 2009, Jonathan Anderson proposed a paradigm called Privacy Suites that allows users to easily select suites of privacy settings that can be created by an expert using privacy programming or by exporting them to an abstract format or through existing configuration UIs. A privacy suite can be verified through best practice, high-level language and motivated users, and then distributed to social site members through existing distribution channels. Barbara Carminati, Elena Ferrari, Raymond Heatherly, Murat Kantar-cioglub, Bhavani Thuraisingham [11] stated in 2011 that security and privacy issues must be considered when developing applications for online social networks that contain personal data.

Therefore, improving access control systems for social networks is an important concern. However, current OSNs only provide users with a very simple access control system that allows them to, for example, mark a particular item as public, private, or accessible to their direct contacts, but lack flexibility by not specifying access control requirements. Therefore, a neugranular OSN access control model based on semantic web technologies is proposed, in which social network-related information is encoded using ontologies. Semantic Web Rule Language (SWRL) can be used to specify the security policies in the form of rules expressed in the ontology, and these can be enforced by simply querying the permissions. In 2013, Kambiz Ghazinour proposed a recommender system known as Your Privacy Protector [17] which helps to understand the privacy settings behavior and recommend appropriate privacy options. The user's personal profile is created based on parameters such as user's interests, user's privacy settings and user's personal profile for photo albums and based on this user's

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

profile the privacy options are assigned. The user is given permission to view their current privacy settings, which are monitored by the system, and if a risk is detected, it makes the necessary privacy settings.

EXISTING SYSTEM

A survey was conducted to study the effectiveness of the existing countermeasure of un-tagging and shows that this countermeasure is far from satisfactory. Therefore, they provide a tool that allows users to restrict their photos from being viewed by others when they post them in order to protect their privacy. However, this method leads to a large number of manual tasks for end users. Squicciarini et al. propose a game-theoretic method in which privacy policies are enforced collaboratively over shared data. This occurs when the user i's appearance has changed or the photos in the training set have changed by adding new images or deleting existing images. The friendship graph may change over time.

PROPOSED SYSTEM

During the process of privacy regulation, we strive to adjust the achieved level of privacy to the desired level. Unfortunately, with most current OSNs, users have no control over the information that appears outside their profile page. In their paper, Thomas, Grier, and Nicol explore how the lack of shared privacy control can inadvertently reveal sensitive information about a user. To mitigate this threat, they propose adapting Facebook's privacy model to ensure privacy for multiple parties. This work explores flexible access control systems based on social contexts. However, in current OSNs, a user does not have to ask permission from other users who are in the photo when posting a photo. Besmer and Lipford's paper explores the privacy concerns of sharing photos and tagging features on Facebook. A survey was conducted in to examine the effectiveness of the existing countermeasure of untagging and shows that this countermeasure is far from satisfactory: users worry about offending their friends if they untag. Therefore, as a complementary privacy strategy, they offer a tool that allows users to prevent others from seeing their photos when they post them. However, this method leads to a large number of manual tasks for end users. Squicciarini et al. propose a game-theoretic method in which privacy policies are jointly enforced over shared data. In our proposed one-versus-one strategy, a user must make classifications between himself, his friend, and his friend, his friend, also known as the two loops in the algorithm. 2. In the first loop, there is no privacy concern about Alice's friend list because the friend graph is undirected. However, in the second loop, Alice must coordinate all of her friends to create classifiers between them.

PROPOSED SYSTEM ALGORITHMS

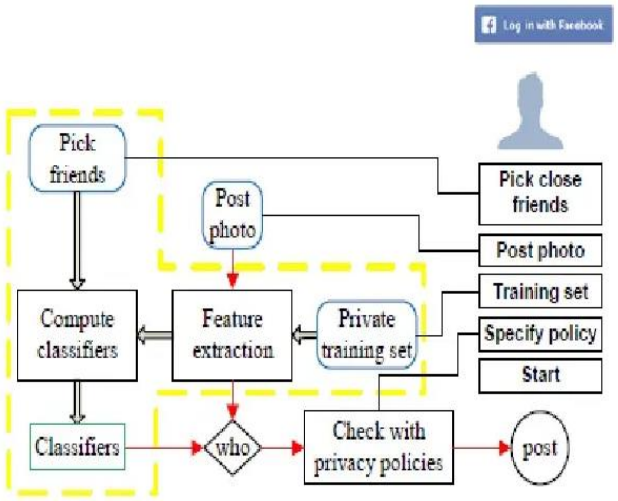
According to the algorithms: There are two steps to create classifiers for each neighborhood: first find classifiers of fself, friendg for each node, then find classifiers of ffriend, friendg. Note that the second step is tricky, since the neighborhood owner's friend list might be known by all his friends. On the other hand, the friends may not know how to communicate with each other.

HOMOMORPHIC ENCRYPTION ALGORITHM

Homomorphic encryption is a form of encryption that allows calculations to be performed on the ciphertext to produce an encrypted result that, when decrypted, matches the result of operations performed on the plaintext. Homomorphic encryption would allow the concatenation of different services without disclosing the data for each of them.

SYSTEM ARCHIECTURE

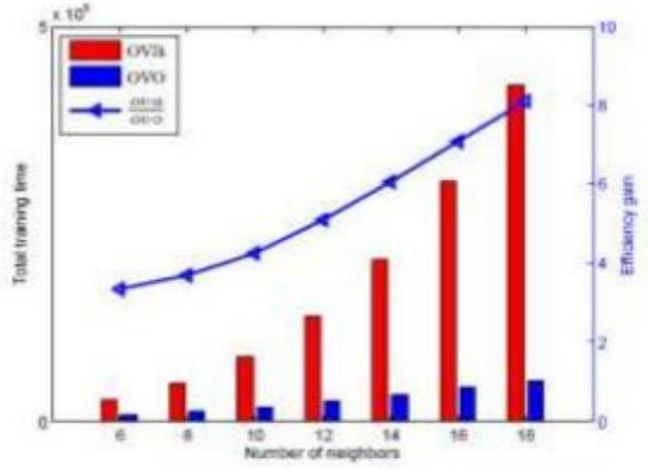
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362



System structure of our application

NETWORK-WIDE PERFORMANCE

Introduction In a little world system, there are three info parameters: the aggregate number of vertex N, the normal hub degree D what's more, rewire likelihood p. In whatever remains of this area, we utilize D furthermore, the quantity of neighbors reciprocally to signify the normal number of clients in one's neighborhood [10]. To develop a little world system, to start with we organize the vertices and associate them in a ring. At that point we associate each vertex with its D closest neighbors.

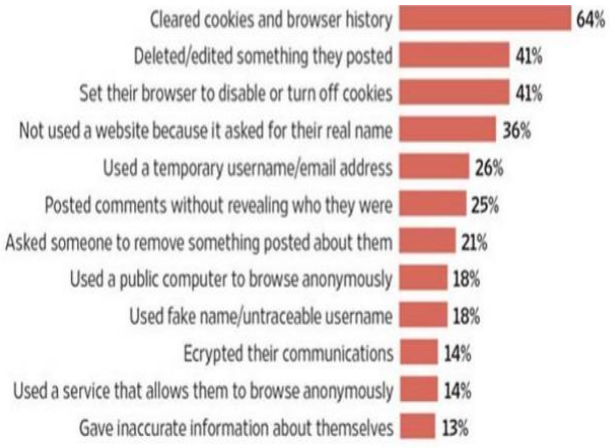


At long last, for every vertex, with likelihood p, its existing edge is rewired with another haphazardly chosen vertex. It is appeared in [14] that the rewire likelihood is very identified with the geodesic separation (the normal most limited separation between any two vertices). We need to demonstrate that in a little world system, there exist a part of finish subgraphs, which enormously lessens the setup time by reusing the current classifiers. Due to asset confinements, we recreate on a system with 3000 vertices. The calculation cost is measured by aggregate calculation.

PRIVACY METRICS

Measuring privacy in social networks is a difficult task. It's not inherently clear which information can lead to considerable damage such as identity theft. Other risks are even harder to assess: comments and pictures which are harmless for some people can be harmful for others. One common approach to define risk is by the following formula: risk = negative consequence × likelihood They define the privacy risk score based on the following two premises:

1. The more sensitive data a user reveals, the higher his privacy risk.
2. The more people know some piece of information about the user, the higher his privacy risk.



CONCLUSION

Online social networks help people to socialize

with the world. But users should be aware of threats that can be faced due to lack of proper privacy settings. In this paper a novel method for collaborative sharing of data in OSNs is discussed as well as a method to resolve privacy conflicts that can occur while multiple persons share a data. Evaluation results show that privacy risk and data sharing loss are minimized in this approach. Various websites offer services such as uploading, hosting, and managing for photo-sharing (publicly or privately). These functions are provided by websites and applications that facilitate the upload and display of images. The term may even be useful for online photo galleries that are positioned up and managed by individual users, including photo blogs. The system used a toy system with two users to demonstrate the principle of the design. It is very efficient than existing system. The system can reduce the privacy leakage by using opensource and Homomorphic Encryption Algorithm. The proposed system features a low computation cost and confidentiality of the training set. Future enhancement can be done by using extended futures of opensource APIs in more efficient privacy training set.

REFERENCES

[1] Open Social. specs. http://www.opensocial.org/specs, 2010.

[2] Open Social. website.http://www.opensocial.org, 2010.

[3] Face book help centre.http://www.facebook.com/help/.

[4] http://www.facebook.com/press/info.php?Statistics, 2010.

[5] World Wide Web Consortium (W3C). Platformfor privacy preferences (p3p) project.http://www.w3.org/P3P/

[6] Kaihe Xu, Yuanxiong Guo, Linke Guo, YuguangFang, Xiaolin Li, "Privacy control in photo Sharing", IEEE Transaction on Dependable and Secure Computing, Volume: PP , Issue: 99, pp-1-1, 2015

[7] Anna Cinzia Squicciarini, "Privacy Policy Inference of UserUploaded Images on Content Sharing Sites", IEEE Transactions on Knowledge And Data Engineering, Vol. 27, no. 1, January 2015.

[8] Nithya Sara Joseph" Collaborative data sharing in online social network resolving privacy risk and sharing loss" (IOSR-JCE) eISSN: 2278- 0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VI (Sep-Oct. 2014), PP 55-61

[9] J. Lydia Jeba, R. Nandhini " A Novel Approach Of MPAC Model For Online Social Network" (IJEAT) ISSN: 2249 – 8958, Volume-3, Issue-3, February 2014

[10] A. k. Rachel Praveena, B. Dr. S. Durga Bhavani,C.k.Suresh Babu,International journal of computer science & Network Solutions December.2013-Volume 1. No4 ISSN 2345-3397.

[11] Raynes-Goldie. (2011). Annotated Bibliography: Digitally mediated surveillance, Privacy and social network sites. (misc)

[12] A. A. Sattikar, Dr. R. V. Kulkarni"A Review of Security and Privacy Issues in Social Networking" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2784-2787.