Volume 3, Issue 6, June 2017 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology

IRJIF IMPACT FACTOR: 3.821

NAIRJC JOURNAL PUBLICATION

North Asian International Research Journal Consortium

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi. All research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: -North Asian International Research Journal Consortium (NAIRJC) 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815, Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

IRJIF IMPACT FACTOR: 3.821

MY PRIVACY: ON PHOTO SHARING OVER ONLINE SOCIAL NETWORK

[1] PROF. DEEPALI PATIL, [2] RUCHIKA GHARAT, [3] TEJASHREE JADHAV, [4] SHEETAL KAMBLE & [5] PRATIKSHA ROKADE

[1] Professor, Nutan Maharashtra Institute of Engineering and Technology, Talegaon Dabhade, Department of Computer Engineering, Savitribai Phule Pune University, India

[2345] Research scholars, Nutan Maharashtra Institute of Engineering and Technology, Talegaon Dabhade, Department of Computer Engineering, Savitribai Phule Pune University, India

Abstract— ***Photograph sharing is an alluring component which advances Online Social Networks (OSNs). Sadly, it may release clients' security on the off chance that they are permitted to post, remark, and label a photograph openly. In this paper, we endeavor to address this issue and study the situation when a client shares a photograph containing people other than himself/herself (termed co-photograph for short). To anticipate conceivable security spillage of a photograph, we outline an instrument to empower every person in a photograph be mindful of the posting action and partake in the choice making on the photograph posting. For this reason, we require a proficient facial acknowledgment (FR) framework that can perceive everybody in the photograph. Notwithstanding, all the more requesting security setting may restrain the photographs' quantity freely accessible to prepare the FR framework. To manage this issue, our instrument endeavors to use clients' private photographs to plan a customized FR framework particularly prepared to separate conceivable photograph co-proprietors without releasing their protection. We additionally add to a disseminated accords based system to diminish the computational many-sided quality and ensure the private preparing set. We demonstrate that our framework is better than other conceivable methodologies as far as acknowledgment proportion and effectiveness. Our instrument is executed as a proof of idea Android application on Facebook's stage.***

Keywords— ***Social network, photo privacy, secure multi-party computation, support vector machine, collaborative learning***

1. INTRODUCTION

OSNS have become integral part of our daily life and has profoundly changed the way we interact with

each other, fulfilling our social needs–the needs for social interactions, information sharing, appreciation and respect. It is also this very nature of social media that makes people put more content, including photos over OSNs without too much thought on the content. However, once something, such as a photo, is posted online, it becomes a permanent record, which may be used for purposes we never expect. For example, a posted photo in a party may reveal a connection of a celebrity to a mafia world. Because OSN users may be careless in posting content while the effect is so far-reaching, privacy protection over OSNs becomes an important issue. When more functions such as photo sharing and tagging are added, the situation becomes more complicated. For instance, nowadays we can share any photo as we like on OSNs, regardless of whether this photo contains other people (is a co-photo) or not. These two policies will together mutually We show later that by performing local learning in parallel, efficiency and privacy could be achieved at the same time. Comparing with previous works, our contributions are:

1. In our paper, the potential owners of shared items (photos) can be automatically identified with/without user generated tags
2. We propose to use private photos in a privacy-preserving manner and social contexts to derive a personal FR engine for any particular user.
3. Orthogonal to the traditional cryptographic solution, we propose a consensus based method to achieve privacy and efficiency.

2. EASE OF USE

2.1 Related Work

We proposed to enable individuals potentially in a photo to give the permissions before posting a co-photo. We designed privacy –preserving FR system to identify individuals in a co-photo. The proposed system in featured with low computation cost and confidentiality of the training set. Theoretical analysis and experiment were conducted to show effectiveness and efficiency of the proposed scheme.

2.2 Motivation

In Mavridis et al. study the insights of photograph sharing on informal communities and propose a three domains show: "a social domain, in which characters are elements, what's more, kinship a connection; second, a visual tangible domain, of which faces are elements, and co-event in pictures a connection; and third, a physical domain, in which bodies have a place, with physical closeness being a connection." hey demonstrate that any two domains are very corresponded. Given data in one domain, we can give a decent estimation of the relationship of the other domain. In Stone et al., interestingly, propose to utilize the logical data in the social domain and co photo relationship to do programmed FR. They

characterize a pair wise restrictive arbitrary field (CRF) model to locate the ideal joint maximizing so as to mark the contingent thickness. In particular, they utilize the current marked photographs as the preparation tests and join the photograph co event measurements and standard FR score to move forward the exactness of face annotation.

3. SYSTEM ARCHITECTURE

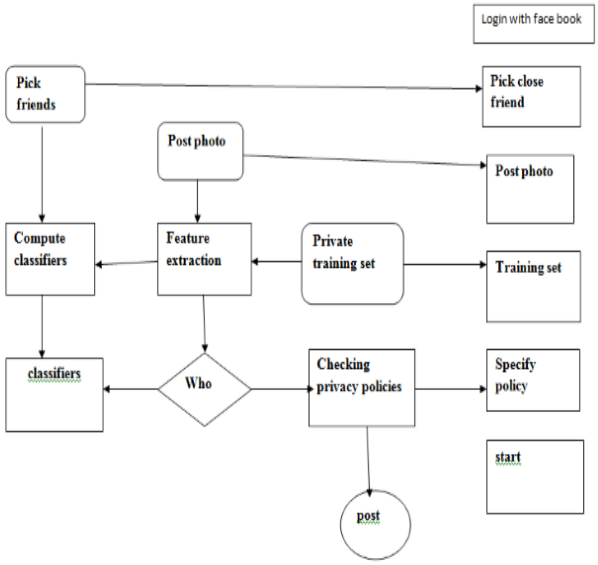

Figure1. System Architecture

4. DESIGN OF SYSTEM

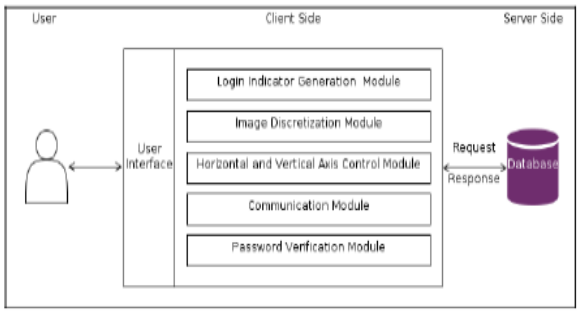

Figure2. Design of system

4.2.1 Image Discretization Module.

This module divides each image into squares, from which users would choose one as the pass-square. As shown in Figure 5, an image is divided into a 7 *11 grid. The smaller the image is discretized, the larger the password space is. However, the overly concentrated division may result in recognition problem of specific objects and increase the difficulty of user interface operations on palm-sized mobile devices.

4.2.2 Login Indicator Generator Module.

This module generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual materials (such as colors and icons) for users during the authentication phase. In our implementation, we used characters A to G and 1 to 11 for a 7*11 grid. Both letters and numbers are generated randomly and therefore a different login indicator will be provided each time the module is called.

The generated login indicator can be given to users visually or acoustically in our system we are sending these patterns on users email.

4.2.3 Horizontal and Vertical Axis Control Module.

There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers.

4.2.4 Communication Module.

This module is in charge of all the information transmitted between the client devices and the authentication server. Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe from being eavesdropped and intercepted.

4.2.5 Password Verification Module.

This module verifies the user password during the authentication phase. A pass Horizontal scroll bar (on the right/blue) and vertical bar (on the left/green).square acts similar to a password digit in the text-based password system. The user is authenticated only if each pass-square in each pass-image is correctly aligned with the login indicator.

5. PROPOSED DESIGN

In this paper, we proposed to empower people conceivably in a photograph to give the constants before posting a co-photograph. We outlined a security protecting FR framework to distinguish people in a co-photograph. The proposed framework is highlighted with low calculation expense and classification of the preparation set. Hypothetical investigation and analyses were directed to show adequacy and proficiency of the proposed plan. We expect that our proposed plan be extremely helpful in ensuring clients' security in photograph/picture sharing over online informal communities. Then again, there dependably exist exchange off in the middle of protection and utility. For instance, in our present Android application, the co-photograph must be post with consent of all the co-proprietors.FR preparing will deplete battery rapidly.

6. IMPLEMENTATION DETAILS

A log in/out button could be used for log in/out with Facebook. After logging in, a greeting message and the profile picture will be shown. Our prototype works in three modes: a setup mode, a sleeping mode and a working mode. Running in the setup mode, the program is working towards the establishment of the decision tree. For this purpose, the private training set Xi and neighborhood Bi need to be specified. Xi could be specified by the user with the button “Private training set”. When it is pressed, photos in the smart phone galleries could be selected and added to Xi. To setup the neighborhoodBi, at this stage, a user needs to manually specify the set of “close friends” among their Facebook friends with the button “Pick friends” as their neighborhood. In our application, each user

picks up to 30 “close friends”. With Xi and Bi specified, the setup mode could be activated by pressing the button “Start”.

7. ALGORITHM

Algorithm Classifier Computation Algorithm

Initial as $\mathcal{C}_i = \emptyset, \forall i \in \mathcal{N}$;
for $i \in \mathcal{N}$ **do**
  for $j \in \mathcal{B}_i$ **do**
    if $u_{ij} \notin \mathcal{C}_i$ **then**
      $u_{ij} = F(X_i, X_j)$;
      $u_{ji} = -u_{ij}$;
      $\mathcal{C}_i = \{u_{ij}, \mathcal{C}_i\}$; $\mathcal{C}_j = \{u_{ji}, \mathcal{C}_j\}$;
    end
  end
end
for $i \in \mathcal{N}$ **do**
  for $k, j \in \mathcal{B}_i \parallel k \neq j$ **do**
    if $u_{kj} \notin \mathcal{C}_k$ **then**
      $u_{kj} = F(X_k, X_j)$;
    else
      Request u_{jk} from user j;
    end
    $\mathcal{C}_i = \{u_{jk}, \mathcal{C}_i\}$;
  end
end

Figure 3. Algorithm

According to Algorithm, there are two steps to build classifiers for each neighborhood: firstly find classifiers of {self, friend} for each node, then find classifiers of {friend, friend}. Notice that the second step is tricky, because the friend list of the neighborhood owner could be revealed to all his/her friends. On the other hand, friends may not know how to communicate with each other. For this consideration, when building classifiers of {friend, friend}, all the local training results are send to the neighborhood owner, who will coordinate the collaborative training processes by forwarding local training results to right collaborators. In this manner, friends need not to know who they are working with and how to talk with them.

8. TECHNOLOGY OVERVIEW

8.1. Apache tomcat

Apache Tomcat**,** often referred to as Tomcat Server, is an open-source java Servlet Container developed by the Apache Software Foundation (ASF). Tomcat implements several Java E specifications including Java Servlet, JavaServer Pages (JSP), Java EL, and WebSocket, and provides a "pure Java" HTTP web server environment in which Java code can run. Tomcat is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation, released under the Apache License 2.0 license, and is open-source software.

8.2. JAVA

Java is a functional computer programming language that provides high protection of data. It is a platform independent language. It is used as object oriented language which helps to create applications in a very efficient manner. It is **Write Once Run Anywhere** type of language which reduces the task of compiling code each time it is executed on new system. It is also used for creation of web based applications or develop business applications.

8.3. XAMPP

XAMPP stands for Cross-Platform (X), Apache (A), MySQL (M), PHP (P) and Perl (P). It is a simple, lightweight Apache distribution that makes it extremely easy for developers to create a local web server for testing purposes. Everything you need to set up a web server – server application (Apache), database (MySQL), and scripting language (PHP) – is included in a simple extractable file. XAMPP is also cross-platform, which means it works equally well on Linux, Mac and Windows. Since most actual web server deployments use the same components as XAMPP, it makes transitioning from a local test server to a live server is extremely easy as well. Web development using XAMPP is especially beginner friendly, as this popular PHP and MySQL for beginners course will teach you.

9. MATHEMATICAL MODEL

9.1. Relevant mathematics associated with the Project

Let S is the Whole System Consists:

S = U,SP,TS,PP,PF .

1. U is the set of number users.

U=U1,U2.....Un.

2. SP is the set of special policy.

SP=SP1,SP2.....SPn.

3. TS is set of number tranning set.

TS=TS1,TS2..TSn.

PF is set of numbers of post photo.

PF=PF1,PF2.....PFn

Step 1: user interface with GUI.

Step 2: user specify policy for security and privacy.

SP=SP1,SP2.....SPn

Step 3: user use training set for posting a photo.

TS=TS1,TS2.....TSn.

Step 4: After getting permission post a photo.

PF=PF1,PF2.....PFn.

10. RESULT

10.1 Send friend request Module result:

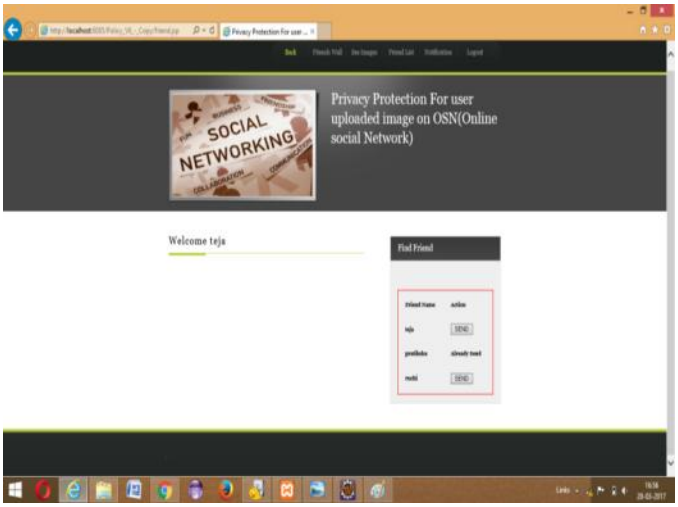

Figure 4. Sends a friend request to your friend.

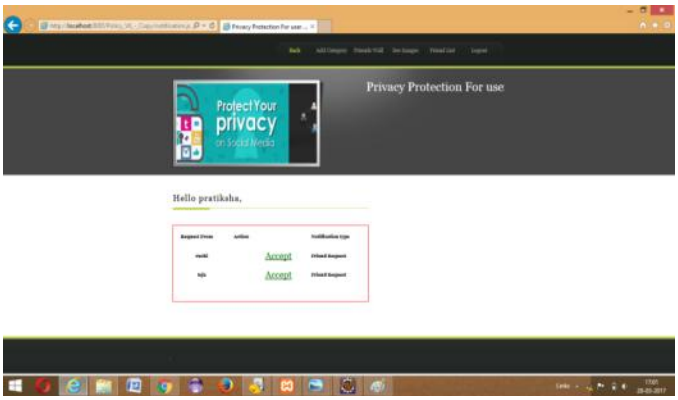

Figure 5. Accepts a friend request.

10.2 Website Host:

Figure 6. Home page of website

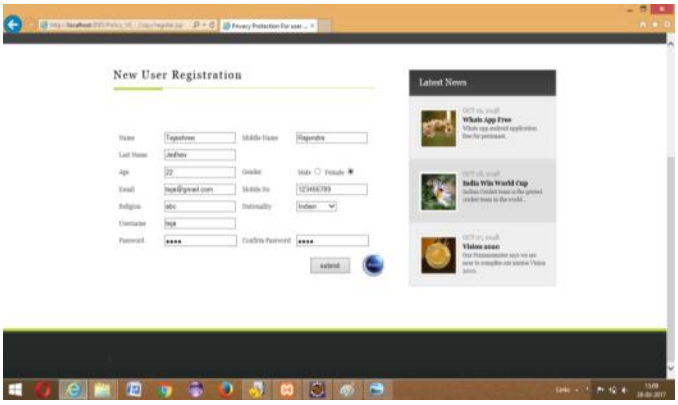

Figure 7. User registration

10.3 Server Module:

Figure 8. Login page of admin

11. APPLICATIONS

In this, according to security perspective, it will be providing a very high security as compared to existing system. It can be used to take the user its own decision for posting its photo.

12. CONCLUSION

Photograph sharing is a standout amongst the most prevalent elements in online informal organizations, for example, Facebook. Lamentably, imprudent photograph posting may uncover security of people in a posted photograph. To control the security spillage, we proposed to empower people possibly in a photograph to give the consents before posting a co-photograph. We planned a security safeguarding FR framework to recognize people in a co-photograph. The proposed framework is highlighted with low calculation expense and privacy of the preparation set. Hypothetical examination and trials were directed to show adequacy and effectiveness of the proposed plan. We expect that our proposed plan be exceptionally helpful in ensuring clients' protection in photograph/picture sharing over online informal organizations. Then again, there dependably exist exchange off in the middle of protection and utility. For instance, in our present Android application, the co-photograph must be post with consent of all the co-proprietors. Idleness presented in this procedure will enormously affect client experience of OSNs. Moreover, neighborhood

FR preparing will deplete battery rapidly. Our future work could be the way to move the proposed preparing plans to individual mists like Dropbox and/or icloud.

REFERENCES

[1]. I. Altman. Privacy regulation: Culturally universal or culturally specific? Journal of Social issues, 33(3):66–84, 1977.

[2]. A. Besmer and H. Richter Lipford. Moving beyond untagging: photo privacy in a tagged world. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10, pages 1563– 1572, New York, NY, USA, 2010. ACM.

[3]. S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein. Distributed optimization and statistical learning via the alternating direction method of multipliers. Found. Trends Mach. Learn., 3(1):1–122, Jan. 2011.

[4]. B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In R. Meersman, Z. Tari, and P. Herrero, editors, On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, volume 4278 of Lecture Notes in Computer Science, pages 1734–1744. Springer Berlin Heidelberg, 2006.

[5]. J. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro. Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks. Multimedia, IEEE Transactions on, 13(1):14–28, 2011.

[6]. K. Choi, H. Byun, and K.-A. Toh. A collaborative face recognition framework on a social network platform. In Automatic Face Gesture Recognition, 2008. FG '08. 8th IEEE International Conference on, pages 1–6, 2008.

[7]. K.-B. Duan and S. S. Keerthi. Which is the best multiclass svm method? an empirical study. In Proceedings of the 6th international conference on Multiple Classifier Systems, MCS'05, pages 278–285, Berlin, Heidelberg, 2005. Springer-Verlag.

[8]. P. A. Forero, A. Cano, and G. B. Giannakis. Consensus-based distributed support vector machines. J. Mach. Learn. Res., 99:1663– 1707, August 2010.

[9]. B. Goethals, S. Laur, H. Lipmaa, and T. Mielik?inen. On private scalar product computation for privacypreserving data mining. In In Proceedings of the 7th Annual International Conference in Information Security and Cryptology, pages 104–120. Springer-Verlag, 2004.

[10]. L. Kissner and D. Song. Privacy-preserving set operations. In IN ADVANCES IN CRYPTOLOGY - CRYPTO 2005, LNCS, pages 241–257. Springer, 2005.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- North Asian International Research Journal Consortium (NAIRJC)
221, Gangoo Pulwama - 192301
Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com