ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.2

Automatic Control/Block Over User Comments on Online Social Network

Ankita Ramakant Godse[1], Snehal Bhagwat Nemade[2], Prerana Subhash Patil[3], Bhagyashri Popat Rane[4]
BE Student[1, 2, 3, 4]
Department of Information Technology
NDMVPS's Adv, Karmveer Baburao Ganpatrao Thakre College of Engineering, Nashik, Maharashtra, India

Abstract:
Nowadays, social media has become an important part of the day to day lives of human being. Most of the communication and information sharing is carried through social networks. With its easy structure and features, social media will continue to gain its popularity amongst people. But however good the technology, it certainly has its own loopholes. With the enormous data shared on social networks, there is one important issue which is needed to be considered that is privacy of the contents. All the huge data stored and shared on social network needs to be protected from outside attacks, malicious users, data misuse, etc. in this project we have proposed a User Control System (UCS) which focuses on giving the users privacy over their contents on social network. The UCS mainly focuses on image data privacy. The system provides certain privacy policies which the user may decide on accordingly. The image uploaded by the user is classified into separate albums created by the user. Each album has a predefined privacy policy. This helps the user to secure the data right after it is share and does not give any chance to misuse the data. When the image is given its policies the viewers and reviews by the viewers is handled according to them. The users I also allowed to choose the good reviews and discard the bad ones. This way the UCS controlled by the user itself helps safeguard data on social network in their own preferable ways.

Keywords: User Control System, policies, album

I. INTRODUCTION

Social media is a two-way communication which allows users connected over the media to communicate with one another. Sharing takes place on many social networks like Google+, Twitter, Facebook, etc. within the communication there can be any sort of information shared like some images, news, data, etc. the communication of this sort helps people to get information about the things around the world. But as every technology comes with its fair share of advantages and disadvantages, social network has one too. The important issue within social network is the security of user contents. Different sorts of information is shared on social network where the users are concerned about the confidentiality and integrity of their data. We come across many data misusing acts on social network. In this project we will be focusing on the image data shared on social network. Consider an example of a user uploading an image on social network. Even if the user applied the given privacy policies to the image there are chances that the image may still be stolen by a third party malicious user and can use the image against the good of the user. Such cases are no trivial problems. Most social networks provide security preferences to the user. But according to recent survey, it is seen that those privacy policies are not enough for the users to safeguard their data. Furthermore, if the systems are made more secure it may also complex the social network which in turn may become difficult to handle for the end users because of the system's complexity. Hence there has been an increasing demand for a secure social network with less complex and best security assurance. In this project we have proposed a User Control System (UCS) which aims to provide a secure environment to the users for their data over social network. The UCS gives the user ability to protect their data right from the point of uploading the image. The user is allowed to group and differentiate their images according to their needs. Also the user will be the one providing policies to their contents accordingly and also select as to who amongst their group can view the information, for what time and who amongst them are eligible to give their feedback to the data. The user can also choose amongst the feedbacks and discard any violating feedbacks before other person seeing it. This way, the user has a better control over the safety of their contents on social network.

II. LITERATURE SURVEY

Many researchers have contributed to the development of Automatic control/block over user comments on online social network. Techniques used by these researchers are summarized below: Privacy Suites [1] is proposed by Jonathan Anderson which allows users to easily choose suites" of privacy settings. Using privacy programming a privacy suite can be created by an expert. Privacy Suites could also be created directly through existing configuration UIs or exporting them to the abstract format. To the members of the social sites the privacy suite is distributed through existing distribution channels. Transparency is the main goal, which is essential for convincing influential users that it is safe to use. The disadvantage of a rich programming language is less understandability for end users. To verify a Privacy Suite sufficiently high-level language and good coding practice, motivated users are able. Privacy-Aware Image Classification and Search [2] is a technique to automatically detect private images, and to enable privacy-oriented image search introduced by Sergej Zerr. To provide security policies technique combines textual meta data images with variety of visual features. It uses various classification models trained on a large scale dataset with privacy assignments obtained through a social annotation game. In this the selected image features (edges, faces, color histograms) which can help discriminate between natural and man-made objects/scenes (the EDCV feature) that can indicate the presence or absence of particular objects (SIFT). A tag based access control of data [3] is developed by Peter F. Klemperer. It is a system that creates access-control policies from photo management tags. Every photo is incorporated with an access grid for mapping the photo with the participant's friends. A suitable preference can be selected by participants and access the information. Based on the user needs photo tags can be categorized as organizational or communicative. There are several important limitations. First, our results are limited by the participants recruited and the photos provided by them. Machine generated access-control rules are the second limitation. Algorithm used here has no access to the context and meaning of tags and no insight into the policy the participant intended when tagging for access control. Hence, some rules appeared strange to the participants who makes them to tag explicitly like private and public. A decentralized authentication protocol [6], is an access control system proposed by Ching-man Au Yeung based on a descriptive tags and linked data of social networks in 5 the Semantic websites. Here users can specify access control rules based on open linked data provided by other parties and it allows users to create expressive policies for their photos stored in one or more photo sharing. Detecting Rumors Through Modeling Information Propagation Networks in a Social Media Environment [8] proposed by Yang Liu and Songhua. In the midst of today's pervasive influence of social media content and activities, information credibility has increasingly become a major issue. Accordingly, identifying false information, e.g., rumors circulated in social media environments, attracts expanding research attention and growing interests. Many previous studies have exploited user-independent features for rumor detection. These prior investigations uniformly treat all users relevant to the propagation of a social media message as instances of a generic entity. Such a modeling approach usually adopts a homogeneous network to represent all users, the practice of which ignores the variety across an entire user population in a social media environment. Recognizing this limitation in modeling methodologies, this paper explores user-specific features in a social media environment for rumor detection. The new approach hypothesizes whether a user tending to spread a rumor message is dependent on specific attributes of the user in addition to content characteristics of the message itself. Under this hypothesis, the information propagation patterns of rumors versus those of credible messages in a social media environment are differentiable. To explore and exploit this hypothesis, we develop a new information propagation model based on a heterogeneous user representation and modeling approach. By applying the new approach, we are able to differentiate rumors from credible messages through observing distinctions in their respective propagation patterns in social media. The experimental results show that the new information propagation model based on heterogeneous user representation can effectively distinguish rumors from credible social media content. Our experimental findings further show that rumors are more likely to spread among certain user groups. Sentiment Computing for the News Event Based on the Social Media Big Data [9] proposed by Dandan Jiang, Xiangfeng Luo, Junyu Xuan, Zheng Xu. The explosive increasing of the social media data on the Web has created and promoted the development of the social media big data mining area welcomed by researchers from both academia and industry. The sentiment computing of news event is a significant component of the social media big data. It has also attracted a lot of researches, which could support many real-world applications, such as public opinion monitoring for governments and news recommendation for Websites. However, existing sentiment computing methods are mainly based on the standard emotion thesaurus or supervised methods, which are not scalable to the social media big data. Therefore, we propose an innovative method to do the sentiment computing for news events. More specially, based on the social media data (i.e., words and emoticons) of a news event, a word emotion association network (WEAN) is built to jointly express its semantic and emotion, which lays the foundation for the news event sentiment computation. Based on WEAN, a word emotion computation algorithm is proposed to obtain the initial words emotion, which are further refined through the standard emotion thesaurus. With the words emotion in hand, we can compute every sentence's sentiment. Experimental results on real-world data sets demonstrate the excellent performance of the proposed method on the emotion computing for news events

III. PROBLEM STATEMENT

The above literature survey gives an idea about the working of social network and several security points covered in it. From the study the image data uploaded by the user on the social network has certain privacy policies to choose the viewers. This ensures that the uploaded data is viewed by the users chosen by the uploader which gives security up to certain limits. One of the surveys mentions creation of albums for image uploading for security purpose. This way the user can create separate albums for different images, provide the privacy policies and ensure the data. But as the data uploaded in social network also gets the reviews of its viewers, it is not always necessary that it gets the best of the reviews. It may happen sometimes that the reviews may contain some sort of bad language which may violate the data uploader's view. In this way even if the data is secured it may still be used against the uploader who demands for further security. In this paper the exact issue is considered for providing further security. With our proposed system not only the user data is secured but also the reviews for the data can be handled by the data uploader which in turn helps against any sort of violation against the users.

IV. SYSTEM OVERVIEW

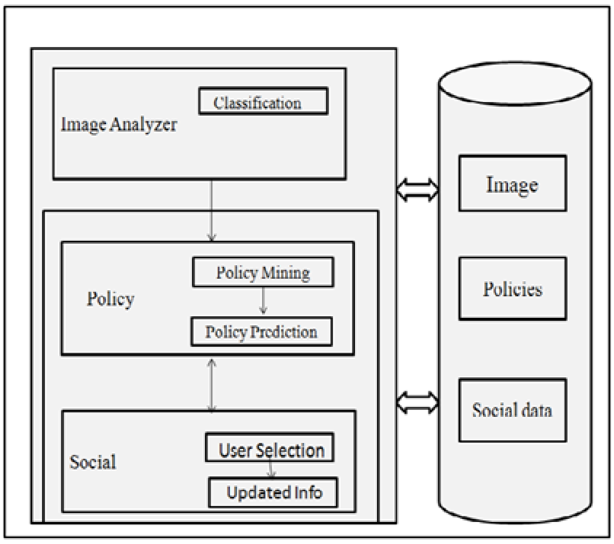

Figure.1. System Overview

The proposed User Control System (UCS), which includes policy prediction algorithm in Image Analyzer and Policy blocks. Our proposed System model contains 4 entities.

A. Image Analyzer

The Image Analyzer analyzes the users posted images and classifies the images according to the user requirements. The work of image analyzer is done by the user itself. First of all, user creates different albums to save the images. The albums can be family album, company album, etc. Now whenever the user posts any image on his account, he classifies the image into the desired album. The album is given its own privacy policies and people who may view the album. In such a way, the image analyzing takes place which is carried out by the user itself.

B. Policy

Given an image, a user usually first decides who can access the image, then thinks about what specific access rights (e.g., view only or download) should be given, and finally refine the access conditions such as setting the expiration date. Correspondingly, the hierarchical mining first looks for popular subjects defined by the user, then look for popular actions in the policies containing the popular subjects, and finally for popular conditions in the policies containing both popular 13 subjects and conditions.

C. UCS-Social

UCS-social module the information of the friends of the user are updated according to the occurrence of different events such as event of birthdays, etc. The user selects a particular image which has been provided policy by the user and updates his information when needed.

D. Database

Database server has rich storage and computing resources. It stores the images, the different policies which have been provided to the images which the user is going to upload. In this paper, We are improving the Efficiency I.e. a good solution should not consume many resources of mobile Android users, and the POI search latency should be acceptable for online query. Accuracy i.e. query result contains the exact records matching the query. False negatives would bad effect on user experience, while false positives would increase communication cost. Additional computational cost is also required at the user side to filter out false positives. Security i.e. solution should be Worked on cipher text-only attacks and known-sample attacks.

V. SYSTEM MODEL OVERVIEW

1. **Input:** keywords.
2. **Processing:**

- In Tag based image search first put the input in the form of query then matching keyword to the given points index structure in databases.
- Collecting all point hash table, which is related to input keyword from the database.
- Filtering images that comes inside of hash table indexes.
- Applying nearest neighbour method on filtered images to find nearest one.

3. **Output:** Image collection(s) which are nearest to user input keyword.
4. **Functions:**readInput(), findCandidates(), readPoints(), filterImages(), findNearest(), displayOutput()

5. **Mathematical Model**

Let 'S' be system such that S = I, O, P, F

Where

I = T1, T2, T3.....

O = Nearest Set Images

P = p1, p2, p3,... set of consumers F = f1, f2, f3,....set of functions.

f1() is a function is used to read input query f2() is a function used to find candidates of given keyword

f3() is a function used to filter images based on relations between index hash table points

....

fN() is a function used to find final nearest Images

6. **Success:**

If given keyword is available in the database

7. **Failure**

If the given keyword not available in the database

VI. CONCLUSION

We have proposed a User Control System (UCS) which helps the user to achieve control over the privacy of the contents shared on social network. The system provides the user précised security policies without introducing too many complexities and keeping the system user friendly increasing the use of social media for content sharing. It helps the user to secure the image and control the reviews gained from the viewers to avoid any sort data misuse.

VII. REFERENCES

[1]. J.Anderson, L. Churc: Privacy suites, 2009.

[2]. S. Zerr, J. Hare, E. Demidova: Privacy-Aware Image Classification and Search, 2012

[3]. Peter F. Klemperer: A tag based access control of data, 2011.

[4]. B. Wang, Y. Hou, M. Li, H. Wang, and H. Li, Maple: Scalable multidimensional range search over encrypted cloud data with tree-based index, in Proceedings of the 9th ACM symposium on Information, computer and communications security. ACM, 2014.

[5]. J. Shao, R. Lu, and X. Lin, Fine: A fine-grained privacy-preserving location-based service framework for mobile devices, in INFOCOM. IEEE, 2014.

[6]. Ching-man: A decentralized authentication protocol, 2013.

[7]. Y. Zhu, D. Ma, D. Huang, and C. Hu: Enabling secure location-based services in mobile cloud computing, in Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing. ACM, 2013, pp. 2732.

[8]. Yang Liu and Songhua Xu: Detecting Rumors Through Modeling Information in a Social Media Environment, 2016.

[9]. Dandan Jiang, Xiangfeng Luo, Junyu Xuan, Zheng Xu: Sentiment Computing for the News Event Based on the Social Media Big Data, 2017.

[10]. F. Olumofin and I. Goldberg: Revisiting the

computational practicality of private information retrieval, in Financial Cryptography and Data Security. Springer, 2012, pp. 158172.

[11]. W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis: Secure knn computation on encrypted databases, in SIGMOD. ACM, 2009, pp. 139152.

[12]. A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill: Order-preserving symmetric encryption, in EUROCRYPT. Springer, 2009, pp. 224241.

[13]. D. Boneh and B. Waters: Conjunctive, subset, and range queries on encrypted data, in Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings, 2007, pp. 535554.

[14]. A. Acquisti and R. Gross, Imagined communities: Awareness, information sharing, and privacy on the facebook, in Proc.6th Int. Conf. Privacy Enhancing Technol. Workshop, 2006, pp. 3658. 25

[15]. S. Ahern, D. Eckles, N. S. Good, S. King, M. Naaman, and R. Nair: Over-exposed: Privacy patterns and considerations in online and mobile photo sharing, in Proc. Conf. Human Factors Compute. Syst., 2007, pp. 357366.

[16]. A. Besmer and H. Lipford: Tagged photos: Concerns, perceptions, and protections, in Proc. 27th Int. Conf. Extended Abstracts Human Factors Compute. Syst., 2009, pp. 45854590.