International Journal of Engineering & Technology, 7 (2.26) (2018) 57-62

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Safe sonet: a framework for building trustworthy relationships

Neethu. MR [1] *, N. Harini [1]

[1] *Department of Computer Science and Engineering, Amrita School of Engineering, Amrita VishwaVidyapeetham, Coimbatore*
**Corresponding author E-mail: cse17014@cb.students.amrita.edu*

Abstract

The advent of easy to use services and the ability to bridge boundaries in space and time has increasingly changed our social lives and com-munication habits. Being unaware of their audience people on social networks inconsiderately share many personal items. Generally Social Networking Sites (SNS) users depend on the SNS platform for managing their social identities. Although SNS providers have introduced privacy settings to protect users against threats, these are insufficient and the access control models are difficult to be understood by novice users [1]. Unexpectedly, even those who are aware of the security and privacy threats and the preventive tools that combat those threats, lack the motivation to utilize security features to protect themselves. The paper discusses a frame-work (Safe SoNet) that aims to provide a plat-form for secure sharing of posts. The objective of this framework is twofold. Firstly, to analyze user behavior by retrieving user information from various social networking sites, addressing transliteration issues. Secondly, apply the user behavior to quantify the trust score of a connect, which would in turn form a decision making parameter to decide on the peer with whom the information can be securely shared.

Keywords: *SNS Security; Transliteration; Machine Learning; Trust Modeling; Recommender.*

1. Introduction

The emergence and popularity of Online Social Networks (OSNs) in the recent years has made it more collaborative environment for information exchange. With the participation of hundreds of millions of Internet users there is also an increase in security threats that affect user's identity, privacy etc... The high levels of trust among users makes SNS perfect for illegal activity. Although site owners provide mechanisms for privacy settings, these are not enough to stop exposure of information that may cause risks for users. This is a challenge since it is hard to provide concrete methods to create trust and maintain it. While literature states that a large number of solutions have provided beneficial results, the following problems still prevails. In this paper, we discuss a scheme that analyses a large set of conversations between network of users, use them as training data, construct automated classification models and assess the level of trust that enables secure sharing of posts in OSNs. The trust model utilizes the reputation of the peers from the interaction he/she had with the user. To account for the uncertainty in the behavior of the person, the model evaluates the randomness and continuously applies it for refining trust score based on sentiment assessed using machine learning techniques.

- Comprehensive model to assess the sentiments in posts.
- Model can aid in computing trust and quantifying trust scores between peers
- Model can aid users to combine machine learning techniques with trust computing methodologies for experimenting varied levels of secure sharing.

The rest of the sections are organized as follows: Section 2 discusses related works, summary of findings and need for the proposed system. Section 3 de-scribes the architecture and the detailed working of the proposed scheme. Section 4 presents the Experimentation Results with related discussions. Final conclusions are included in Section 5.

Although literature states that a large number of solutions have provided beneficial results, the following problems still exists [2] specifies that social network still suffer from threats like spread of rumours, privacy leaks, spreading of virus, incite malignant group events.

2. Related work

WWW and OSNs are definitely opening up broader avenues for communication. Making friends with unknown peers may be considered as trendy but can pose a tangible threat to one's privacy, confidentiality etc. Online world is abysmal, what is projected to the users may not be real. Trusting someone so easily in the web world is not suggested. Hence users are required to be awareand vigilant. User's dependence on service providers may be risky.

A number of journals and article have come up with these issues and discuss how one could be victimized online. Survey reveals that machine learning algorithms have been adopted widely for data classification and prediction. [3] Discusses techniques that could be employed for feature selection and classification. [4], [5] Discusses the performance of three families of classification algorithms and also brings out the facts that the size of the sample and quality of data play a major role in determining the accuracy. Recent research reveals that deep learning algorithms facilitate modeling high level abstraction [9]. Literature reveals that a wide range of supervised learning algorithms is useful for sentimental analysis. But there is no consensus on which one to choose. Different studies use different data sets, natural language preprocessing techniques, evaluation measures etc...

Social networking sites are a major application driver with millions of users relying on them for keeping contacts and sharing information. This brings a clear demand for the need to set up right security measures. As the communication is online the peers may be known or unknown and do not have a face to face contact.

Copyright © 2018 Neethu. MR, N. Harini. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

There is no guarantee that a contact is a friend or a foe. A well designed trust model would enable one to compute the belief he/she can entrust upon the peers. [6] Presents an overview of existing challenges related to privacy and security issues in OSNs. [7] Proposes an access control scheme called Trust Based Access Control for Social Networks that facilitate data sharing with peers based on computed trust score based on interaction intensity. [8]discusses the fact that there are also posts which can be an offence to human psychology in OSN. With the escalation in the number of security threats and privacy violation attempts the existing system based purely on interaction intensity without consideration to factors like sarcasm, emotion etc...does not appear to be robust. Although there are many works carried out by researchers for enhancing security [11], proper implementation of these schemes is not there in any OSNs. This brings out a clear need for a new scheme that enhances security when sharing posts in OSNs.

2.1. Summary of findings

Review of the literature clearly revealed that a significant further research in social graph analysis, prediction of traffic demands, personalization of content, social ranking , architecture for open social network platforms are required to improve the current state of the art aspects in online social networks. With the growing interest of expanding a person's social circle, an intelligent recommender engine designed to facilitate secure sharing of posts based on segregation of friends/peers is the need of the day.

3. Problem statement

To conduct a comprehensive survey of potential behaviors of peers(interaction intensity ,emotions) in social networking sites and design a framework (Safe SoNet) that recommends trustworthy relations with whom posts can be shared.

Contributions

A close study of the work so far reveals the need for simple elegant framework that provides a systematic approach that guarantees secure sharing of posts in OSNs. The model proposed and presented in this paper is aimed at meeting this need. The main contributions of this paper can be summarized as follows:

- Comprehensive model to assess the sentiments in posts.
- Model can aid in computing trust and quantifying trust scores between peers by combining machine learning, tone analysis.
- Model uses data of multiple users collected from multiple OSNs to perform 1 and 2.

In sentiment analysis the focus is mainly on detecting the subjectivity or semantic orientation. Often it is useful to know exactly how one reacts emotionally to a particular event/message/entity. Emotion cues are not limited to only emotional word such as happy, sad etc… The degree to which the emotion has been expressed is to be thoroughly explored for accurate trust score calculation.

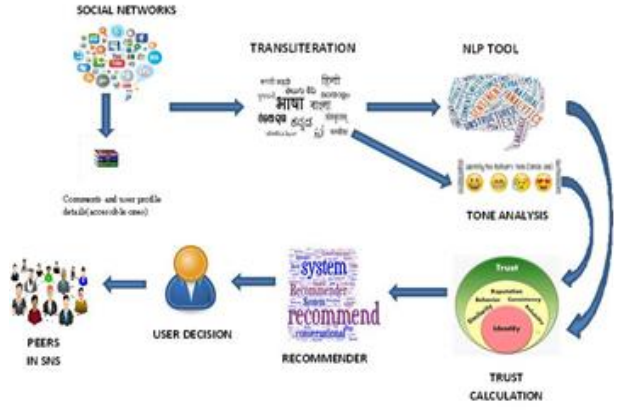


Fig. 1: Architecture of Safe Sonet.

4. Architecture of safe sonet

On the web, where the number of choices is overwhelming there is a need to filter, prioritize and deliver relevant information to right people in right time. An intentional or unintentional data exposure will lead to a large scale security breach. Locking down the account with the help of privacy settings does not necessarily mean secure sharing. Even today reports have come up with accounts being hacked, users being affected by privacy issues: Newburyport teens charged in cyber bullying case* , Cyber bullying leads to suspension of 28 middle-schoolers at McClure**. Many of these kinds of problems lead to the threat of human life also. Thinking twice before writing anything on this open social forum is mandatory.

The scientific and technical objective of this work may be more precisely is depicted as follows:

1) Gather pro le and interaction information from OSN.
2) Apply specific data classification and correlation technique.
3) Perform tone analysis.
4) Assess trust score.
5) Design and implementation of framework for presenting measurement results.

Safe SoNet provides a platform for secure sharing of posts in OSNs using machine learning and trust computation algorithms. Fig [1] provides the architecture diagram of the framework. The scheme is designed as a flexible three tier model to include a variety of learning, trust evaluation algorithms to offer differentiated security levels for sharing posts in OSNs.

The tool graph api explorer and instagram graph api were used to collect data from Facebook and instagram respectively. the collected dataset was in-put to basic transliteration engine and the results were further applied to a classifier module for semantic analysis. Added to these, bluemixwatson service was used to perform tone analysis on the dataset. Matrix like reliability and credibility were evaluated to assess the consistency and the trust one can entrust on his or her connect. Detailed experimentation was carried out with different weightage values for reliability and credibility. The outcome of this was used to assign trust value for a peer in the network. The final trust score were computed by the recommender engine based on tone analysis. This final score was used by the system to predict if the post could be shared with him or her.

4.1. Machine learning for evaluation

Machine learning algorithms have been used by researchers for pattern recognition, text classification etc... A combination of information retrieval andmachine learning technology has been reported to improve the accuracy of the modern classification schemes. Machine learning aim at retrieving, classifying (supervised, semi supervised and unsupervised) and summarizing data. The classification process commences with transliteration process that converts comments/tweets written in state languages like Tamil, Malayalam etc..to English. The statistics collected from Facebook using authors account re-veal that nearly 50% of the comments were made in mother tongue, combined with English (fig [2]). That is, most of the social network users prefer informal-languages.

In addition to text classification, fine grained emotions in text is also used by Safe SoNet to predict emotion based sentimental outcome which in turn is used to assess the trust score of the peer. The present version of the framework includes naive bayes, C4.5, SVM for classification process.

4.2. Trust evaluation

The model uses a systematic procedure to evaluate the trust relationship be-tween peers. The computation of trust scores is based on the results of applying a supervised machine learning algorithm that classified the interactions one has had with his or her peer for

over a period of time. A statistical approach using machine learning algorithms (Bayesian, SVM, Max entropy) is adopted by the model in addition to emotion analysis methods. Trust values are computed using the scheme discussed in [8]. The result of the trust recommender engine is used to compute the credibility of the peers connected to the user. A threshold based filtering in applied on the peer list to build reliable and unreliable lists.

4.3. Modelled metrics

The behaviour of the users is monitored and utilized to compute trust score which in turn is used by the recommendation engine to recommend users with whom particular posts can be shared. Nevertheless any other metric can be accommodated in the model with equal ease. The model considers interaction among peers and emotions expressed in posts as strong indicator for peer segregation.

5. Results and discussion

A meticulous experimental study was carried out on safe SoNet using data-sets containing interactions between users collected from different online social networking sites like Facebook, instagram and twitter with standard classifier algorithms and emotion analysis scheme. For privacy reasons analysis pertaining to authors account only is discussed in the paper. To strengthen the dataset it was ensured that records with positive, negative and neutral sentiments, varied tones requiring transliteration were added adequately throughsocial media. The heterogeneous data log thus collected assisted in precise analysis. An in-depth analysis of the log revealed that comments were written in more than one language and quite a few were posted from fake accounts. Transliteration procedure was performed in the data-set to translate comments posted in different mother tongue to English. This helps one to strengthen our data-set in terms of quality and size of training data.

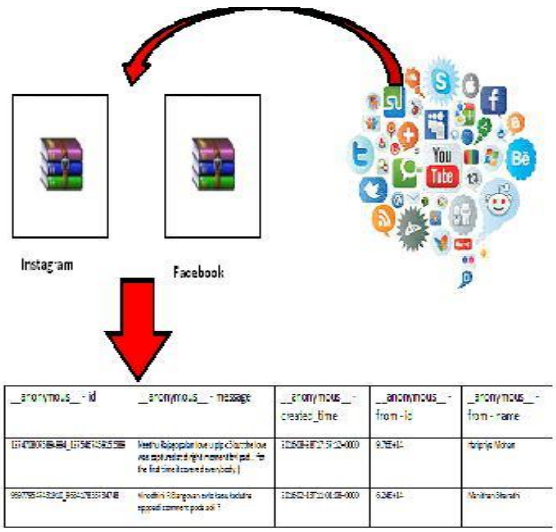


Fig. 3: A) Data-Set Collection.

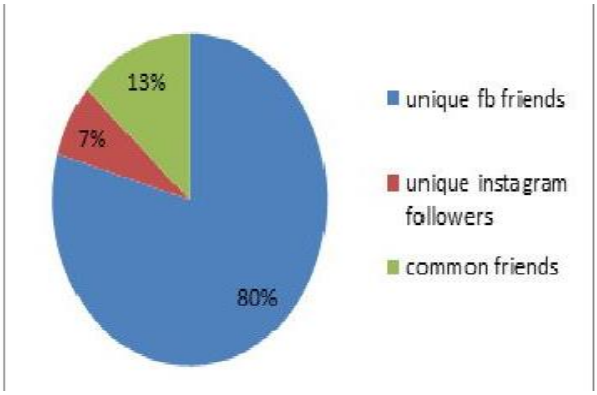


Fig. 3: B) Uniqueness in Friends.

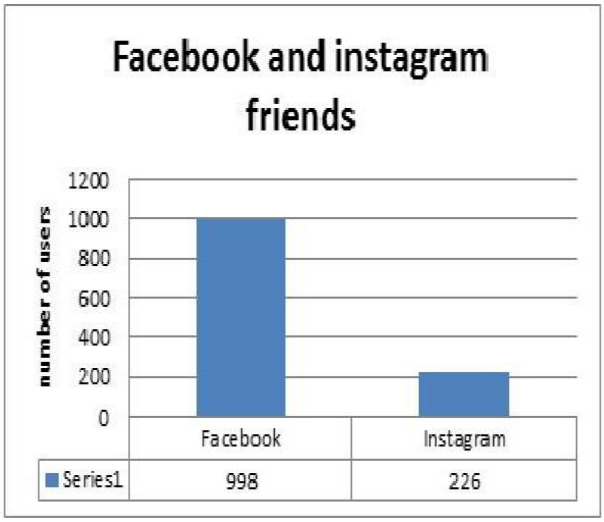


Fig. 3: C) Number of Users /Friends in.

Table 1: Table of Notations

Sl no	Notations	Particulars
1	R	Reliability of the user
2	N	Average negativeness of the comments
3	P	Average positiveness ofthe comments
4	n	negativity of the comment
5	p	positivity of the comment
6	Cn	Number of comments posted by user in the wall of the peer.
7	Ci	Number of positive comments
8	Cn-i	Comments are negative.
9	u	User
11	T	Transaction
12	Tin	Transaction from peers to user
13	Tout	Transaction from user to peer
14	Cr	Credibility of the peer
15	Tr	Trust value of the user
16	p(u,v)	transaction between the user u and a friend node v
17	p(u,i)	total number of transaction of u with all the friend node i in the social network
18	p(v)	friend node v

A detailed description of the data log obtained with a few 1000s of comments and 100s of connects collected from the authors account is shown in figs [3.a.c] The structure of the dataset, percentage of connects in different social net-works, overlap in peer list is depicted in figure [3.a].

A detailed description of the procedure used to assess the trust score together with numerical results is presented in tables 5a [13] and 5.b [13] respectively. The automated classification approach assisted in the detection of negative peers. The behavior of the author's connects collected from Facebook, instagram etc... is brought out in thefig[4].

Table 2: Equations of Reliability, Credibility and Trust Score

Reliability of the peer:
Average positiveness of the comments: $P=\frac{\sum p}{C_i}$
Average negativeness of the comments: $N=\frac{\sum n}{C_{n-i}}$
Credibility of the peer: $S=T_{in}-T_{out}$
$Cr(p(u,i)) = \frac{1}{i}(\sum S_p - S_o) * 100$
Trust value of the peer: $Tr(p(u,v)) = \frac{T_{out}(p(v))}{\sum(p(u,i))} * 100$

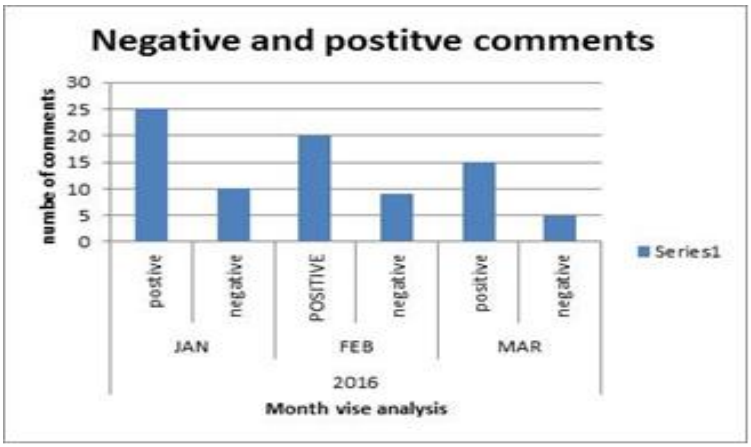


Fig. 4: Predicting Emotion Based Sentiment.

Table 3: Naive Bayes

Instances: 1554								
Attributes: 528								
Test mode: split 75.0% train, remainder test								
Correctly Classified Instances 378 97.4227 %								
Incorrectly Classified Instances 10 2.5773 %								
Kappa statistic 0								
Mean absolute error 0.055								
Root mean squared error 0.1585								
Relative absolute error 100 %								
Root relative squared error 100 %								
Total Number of Instances 388								
TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
1.000	1.000	0.974	1.000	0.987	0.000	0.500	0.974	0
0.000	0.000	0.000	0.000	0.000	0.000	0.500	0.026	1
0.974	0.974	0.949	0.974	0.962	0.000	0.500	0.950	Weighted Average
=== Confusion Matrix ===								
a b <-- classified as								
378 0 | a = 0								
10 0 | b = 1								

Table 4: SVM

Instances: 1554								
Attributes: 528								
Correctly Classified Instances 380 97.9381 %								
Incorrectly Classified Instances 8 2.0619 %								
Kappa statistic 0.3276								
Mean absolute error 0.0206								
Root mean squared error 0.1436								
Relative absolute error 37.484 %								
Root relative squared error 90.5721 %								
Total Number of Instances 388								
TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
1.000	0.800	0.979	1.000	0.990	0.443	0.600	0.979	0
0.200	0.000	1.000	0.200	0.333	0.443	0.600	0.221	1
0.979	0.779	0.980	0.979	0.973	0.443	0.600	0.960	Weighted Average

Table 5: J48

Instances: 1554								
Attributes: 528								
Correctly Classified Instances 387 99.7423 %								
Incorrectly Classified Instances 1 0.2577 %								
Kappa statistic 0.9461								
Mean absolute error 0.0034								
Root mean squared error 0.0508								
Relative absolute error 6.2271 %								
Root relative squared error 32.027 %								
Total Number of Instances 388								
TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
1.000	0.100	0.997	1.000	0.999	0.947	0.903	0.995	0
0.900	0.000	1.000	0.900	0.947	0.947	0.903	0.903	1
0.997	0.097	0.997	0.997	0.997	0.947	0.903	0.993	Weighted Averege
=== Confusion Matrix ===								
a b <-- classified as								
378 0 | a = 0								
1 9 | b = 1								

Table 6: Trust Score Evaluation

User	Friends	Transactions	Incoming Transactions	Outgoing Transactons	Sp/ Sn/ So	Credibility	Credibilty (boolean)	Trust Score	Reliability
Peer 1	742	40	25	15	Sp	35	0	0.375	0
Peer 2	1,585	65	62	3	Sp	31.81818	0	0.046154	0
Peer 3	1,487	10	2	8	Sn	63.63636	0.5	0.8	0
Peer 4	548	9	2	7	Sn	93.33333	1	0.777778	0
Peer 5	2,044	25	3	22	Sn	73.68421	1	0.88	0
Peer 6	360	19	15	4	Sp	56	0.5	0.210526	0
Peer 7	271	20	15	5	Sp	46.66667	0	0.25	0
Peer 8	793	26	18	8	Sp	41.17647	0	0.307692	0
Peer 9	1,333	44	22	22	So	63.63636	0.5	0.5	1
Peer 10	330	99	22	77	Sn	73.68421	1	0.777778	1
Peer 11	520	52	40	12	Sp	56	0.5	0.230769	1
Peer 12	772	28	10	18	Sn	87.5	1	0.642857	1
Peer 13	218	50	36	14	Sp	70	1	0.28	1
Peer 14	292	46	22	24	Sn	77.77778	1	0.521739	1
Peer 15	441	24	14	10	Sp	56	0.5	0.416667	1
Peer 16	1,051	39	19	20	Sn	43.75	0	0.512821	1
Peer 17	1,111	25	15	10	Sp	29.16667	0	0.4	1
Peer 18	1,201	55	25	30	Sn	40	0	0.545455	1

6. Conclusion

This work discusses a framework(Safe SoNet) that analyses risks in social network associated with sharing of posts with peers. The first part of the framework analyses user behaviours using machine learning algorithms and the second part aims at quantifying the risk which paves way for users to make an efficient decision regarding with whom the post can be shared. In short the scheme provides an efficient and effective mitigation technique that significantly includes the security of social network users. The proposed framework undoubtedly can act as a foundation stone over which additional changes can be implemented to cope up with the ever growing privacy and security threats in social networks.

Future work is conducted in identifying suitable deep learning algorithms and trust models that could be integrated in the framework for improved behaviour assessment for eliminating linguistic barriers and addressing sarcasm in user comments.

References

[1] Ho, Ai, AbdouMaiga, and EsmaAïmeur. "Privacy protection issues in social networking sites." Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on. IEEE, 2009.

[2] Yang, Li, et al. "Research of Security Relationship Based on Social Networks." International Conference on Trustworthy Computing and Services. Springer, Berlin, Heidelberg, 2012.

[3] Liu, Huiqing, Jinyan Li, and Limsoon Wong. "A comparative study on feature selec-tion and classication methods using gene expression pro les and proteomic patterns." Genome informatics 13, 51-60, (2002).

[4] Huang, Lung-Cheng, Sen-Yen Hsu, and Eugene Lin. "A comparison of classification methods for predicting Chronic Fatigue Syndrome based on genetic data." Journal of Translational Medicine 7.1 (2009): 81.

[5] Huang, Jin, Jingjing Lu, and Charles X. Ling. "Comparing naive Bayes, decision trees, and SVM with AUC and accuracy." Data Mining, 2003. ICDM 2003. Third IEEE Inter-national Conference on. IEEE, (2003)

[6] Zhang, Chi, et al. "Privacy and security for online social networks: challenges and op-portunities." IEEE Network 24.4 (2010).

[7] Omanakuttan, Saumya, and MadhumitaChatterjee. "Experimental Analysis on Access Control Using Trust Parameter for Social Network." International Conference on Security in Computer Networks and Distributed Systems. Springer, Berlin, Heidelberg, (2014).
[8] Neethu,Harini."Securing image posts in Social networking sites",International Conference On Computational Vision and Bio Inspired Computing",Proceedings of Springer - Lecture Notes in Computational Vision and Biomechanics.,(2017)
[9] Bengio, Yoshua. "Deep learning of representations for unsupervised and transfer learn-ing." Proceedings of ICML Workshop on Unsupervised and Transfer Learning. (2012).
[10] Harini, Narasimhan, and Tattamangalam R. Padmanabhan. "3c-auth: A new scheme for enhancing security." International Journal of Network Security 18.1, 143-150, (2016).
[11] Harini, N. "A System to Screen Posts that Minimize user Frustration." International Journal of Applied Engineering Research 11.6, 3944-3949, (2016).