# A RELIABLE FRIENDSHIP MECHANISM FOR ONLINE SOCIAL NETWORK EXPLOITING PRE AND POST-FILTERING APPROACH

S M NAZMUS SADAT

DOCTOR OF PHILOSOPHY

UNIVERSITI MALAYSIA PAHANG

**SUPERVISOR'S DECLARATION**

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Doctor of Philosophy.

Md. Arafatur Rahman

(Supervisor's Signature)
Name of Supervisor: Dr. Md Arafatur Rahman
Position: Associate Professor
Date: October 12, 2022

**STUDENTS'S DECLARATION**

I hereby declare that the work in this thesis/project is my own for quotations and summaries which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

(Student's Signature)
Name: S M Nazmus Sadat
ID number: PCC17008
Date: October 12, 2022

# A RELIABLE FRIENDSHIP MECHANISM FOR ONLINE SOCIAL NETWORK EXPLOITING PRE AND POST-FILTERING APPROACH

S M NAZMUS SADAT

Thesis submitted in fulfilment of the requirements
for the award of the degree of
Doctor of Philosophy

Faculty of Computing
UNIVERSITI MALAYSIA PAHANG

OCTOBER 12, 2022

## ACKNOWLEDGEMENTS

Al-hamdu lillah, first of all, I wish to express my gratitude to Almighty Allah, for all the strength and blessing to complete the thesis. I would like to express my sincere gratitude and indebtedness to my supervisor Dr. Md. Arafatur Rahman for his supervision, guidance, and encouragement throughout this study. His invaluable suggestions and constructive criticism from time to time during the preparation of this thesis enabled me to present the thesis in this form. My sincere gratitude is also due to my co-supervisor Professor TS. Dr. Ruzaini Abdullah Arshah for his supervision and valuable suggestions throughout this study. Regards to Dr. A. Taufiq Asyhari, because his contribution is undeniable for the development of my research skills. It is a pleasure working with them. I also like to express my sincere gratitude to University Malaysia Pahang (UMP) for providing consistent support and help. It is a wonderful place to work, and the staff are very dedicated and helpful. I have gained so much knowledge and experience from UMP. I would also like to thank the academic, management, and technical staff of the Faculty of Computing (FKoM) and the staff of the Institute of Postgraduate Studies (IPS). Next, I would also like to express tremendous appreciation to my family, especially my sister, Nadia Refat for their generous support in every way, which has always been a source of energy and inspiration. Thanks to all my friends, colleagues, and all Malaysians for their openness, friendship, and hospitality. Finally, I would like to thank the Malaysian Government for providing consistent services and security that helped to create a comfortable environment to study.

# ABSTRAK

Rangkaian sosial dalam talian menjadi semakin popular dan penggunaannya semakin meningkat dari hari ke hari. Ia adalah bahagian penting dalam kehidupan seharian kita dan medium yang tiada tandingan untuk berkomunikasi dengan keluarga, rakan dan profesional demi kepentingan tujuan peribadi dan profesional. Disebabkan ciri-ciri ini, rangkaian sosial dalam talian mengandungi banyak maklumat yang boleh dikongsi oleh individu antara satu sama lain. Oleh itu, maklumat peribadi mudah didedahkan dalam talian dan disalahgunakan oleh rakan atau rakan yang tidak boleh dipercayai tanpa kesedaran pengguna. Malangnya, isu fungsi tertentu belum ditangani berkenaan pendekatan penapisan automatik dalam memulakan persahabatan dan interaksi pengguna dengan rakan sekutu dalam talian mereka. Tambahan pula, pengguna tidak boleh meneliti dengan betul tingkah laku anomali pengguna lain sepanjang masa, yang boleh melibatkan mereka dalam penyelewengan dengan jelas. Untuk menangani isu ini, kajian yang dicadangkan membangunkan mekanisme persahabatan yang boleh dipercayai untuk rangkaian sosial dalam talian dengan menggunakan pendekatan penapisan dua fasa automatik (pra dan pasca) untuk menentukan rakan yang boleh dipercayai dan memantau aktiviti tingkah laku mereka. Dalam pendekatan pra-penapisan, pengguna boleh memilih rakan menggunakan mekanisme yang boleh dipercayai, yang terdiri daripada dua pilihan: berasaskan atribut dan berasaskan model. Pendekatan pasca penapisan didayakan pembelajaran mesin (ML) direka untuk menentukan aktiviti tingkah laku yang mencurigakan dan tidak diingini. Akhir sekali, mekanisme yang dicadangkan itu menggabungkan pendekatan pra dan pasca penapisan, menghasilkan pendekatan hibrid baru yang boleh mencapai tujuan kajian. Analisis empirikal menunjukkan beberapa data perbandingan yang signifikan terhadap pendekatan hibrid (selepas menggabungkan pendekatan pra dan pasca penapisan), di mana persepsi pengguna terhadap pendekatan yang dicadangkan melebihi pendekatan bersaing yang lain dengan ketara. Seperti yang ditunjukkan dalam nilai min berkadar, pendekatan hibrid yang dicadangkan mencapai nisbah tertinggi sebanyak 90.64%, dengan pra-penapisan menyumbang 69.76% dan selepas penapisan berjumlah 70.56%. Dan pendekatan sedia ada mempunyai nilai min berkadar terendah pada 47.60%. Hasil kajian ini diharapkan dapat membantu penyedia OSN, komuniti penyelidikan, dan pihak berkuasa ICT dalam menyediakan penyelesaian standard untuk memilih rakan yang boleh dipercayai dan mengelakkan penyelewengan mereka dalam OSN.

## ABSTRACT

Online social networks are becoming increasingly popular, and their uses are growing day by day. It is an integral part of our daily lives and an incomparable medium to communicate with family, friends, and professionals in the interest of personal and professional purposes. Because of these features, the online social network contains a great deal of information that individuals can share with one another. Therefore, personal information is easily disclosed online and is misused by unreliable friends or associates without the users' awareness. Unfortunately, certain functional issues have not been addressed regarding the automatic filtering approach in initiating friendships and users' interactions with their online associates. Furthermore, a user cannot properly scrutinize the anomalous behavior of other users over the time variant, which can clearly engage them in malpractices. In order to address these issues, the proposed study develops a reliable friendship mechanism for online social networks by utilizing automated two-phased (pre and post) filtering approaches to determine reliable friends and monitor their behavioral activities. In the pre-filtering approach, a user can select a friend using a reliable mechanism, which consists of two choices: attribute-based and model-based. A machine learning (ML) enabled post-filtering approach is designed to determine suspicious and unwanted behavioral activities. Finally, the proposed mechanism incorporates pre and post-filtering approaches, resulting in a novel hybrid approach that can accomplish the purpose of the study. The empirical analysis shows some significant comparison data towards the hybrid approach (after incorporating pre and post-filtering approaches), where the users' perceptions of the proposed approach exceed the other competing approaches significantly. As shown in the proportionate mean values, the proposed hybrid approach achieved the highest ratio of 90.64%, with pre-filtering accounting for 69.76% and post-filtering standing for 70.56%, while the existing approach had the lowest proportionate mean value at 47.60%. The outcomes of this study are expected to assist OSN providers, research communities, and ICT authorities in providing a standard solution for selecting reliable friends and avoiding their malpractices in OSN.

## TABLE OF CONTENT

**DECLARATION**

**TITLE PAGE**

**ACKNOWLEDGEMENTS** ii

**ABSTRAK** iii

**ABSTRACT** iv

**TABLE OF CONTENT** v

**LIST OF TABLES** viii

**LIST OF FIGURES** ix

**LIST OF SYMBOLS** xi

**LIST OF ABBREVIATIONS** xii

**LIST OF APPENDICES** xiii

**CHAPTER 1 INTRODUCTION** 1

1.1 Background & Motivation 1

1.2 Problem Statement 4

1.3 Research Questions 7

1.4 Research Objectives 7

1.5 Research Contribution 9

1.6 Research Scope 10

1.7 Research Methodology 11

1.7.1 Phase 1: Designing a Reliable Friendship Mechanism 11

1.7.2 Phase 2: Filtering Approaches for Reliable Friendship in OSN 12

1.7.3 Phase 3: Validation of the Research 12
1.7.4 Phase 4: Result and Summary 13
1.8 Outline of the Thesis 13

**CHAPTER 2 LITERATURE REVIEW 15**
2.1 Introduction 15
2.2 Research Background 16
2.3 Discussion on Previous Studies 18
2.3.1 Filtering Approaches for Reliable Friendship in OSN 18
2.4 The Novelty of the Proposed Study: 38
2.5 Online Social Networks 40
2.5.1 The Classification of Online Social Network 40
2.5.2 Reliable Friendship in OSN 43
2.6 Malicious Activities 43
2.6.1 Issues of Malicious Activities 44
2.6.2 Malicious Activities in OSN 47
2.7 Summary 50

**CHAPTER 3 METHODOLOGY 51**
3.1 Introduction 51
3.2 Phase 1: Design a Reliable Friendship Mechanism 52
3.2.1 Mechanism for Reliable Friend Selection 53
3.2.2 Mechanism for user's Friend Behavior Analysis 56
3.2.3 Reliable Friendship Mechanism in OSN Platform 59
3.3 Phase 2: Filtering Approaches for Reliable Friendship Mechanism 61
3.3.1 Pre-filtering Approach for Reliable Friend Selection 62
3.3.2 Post-filtering Approach for Behavioral Analysis 78
3.3.3 Development of the approach and its implementation 85
3.4 Phase 3: Validation of the Research 93
3.4.1 Validation of Pre-filtering Approach 93
3.4.2 Validation of Post-filtering Approach 95

3.4.3 Validation of Hybrid Approach 95
3.5 Summary 96

**CHAPTER 4 RESULTS AND DISCUSSIONS 97**
4.1 Introduction 97
4.2 Discussion and Validation of Pre-filtering Approach 98
4.2.1 Effectiveness & Validation of Attribute-based 98
4.2.2 Discussion & Validation of Model-based Approach 104
4.3 Discussion and Validation of Post-filtering Approach 115
4.3.1 Experiments and Performance Evaluation 115
4.4 Discussion and Validation of Reliable Friendship Mechanism 129
4.4.1 The Feasibility of the Hybrid Approach 130
4.5 Summary 136

**CHAPTER 5 CONCLUSIONS 137**
5.1 Introduction 137
5.2 Research Contribution 138
5.3 Limitations of the Study 140
5.4 Directions of Future Work 141

**REFERENCES 142**

**APPENDICES 154**

## LIST OF TABLES


Table 1.1 Research Questions and Research Objective Mapping 9

Table 2.1 Comparison between the proposed mechanism and several previous works (Part:1) 35

Table 2.2 Comparison between the proposed mechanism and several previous works (Part:2) 36

Table 3.1 Sample of application for the evaluation of prospect to become a friend 69

Table 3.2 A Sample of the model of a friend-to-be 74

Table 3.3 Sample of evaluation 75

Table 4.1 T-test Analysis 104

Table 4.2 Observed predicted values of the likelihood of a friend request acceptance 107

Table 4.3 Likelihood intervals to compare the observed (empirical) with the expected (theoretical) distribution 109

Table 4.4 Hypothesis Testing 110

Table 4.5 T-test Analysis 113

Table 4.6 Performance Evaluation on Different Measures in Training Phase 119

Table 4.7 Performance Evaluation on Different Measures in Training Phase with Feature Engineering (FE) 126

Table 4.8 Performance Evaluation on Test Dataset 127

Table 4.9 Performance Evaluation on Test Dataset (FE) 128

Table 4.10 T-test Analysis 135

## LIST OF FIGURES


Figure 1.1 Most Popular Online Social Networks worldwide as of January 2022 2

Figure 1.2 Research process in this thesis 12

Figure 2.1 Harassment Experience on Online social Networks 17

Figure 2.2 Classification of Reviews for filtering approaches in OSN. 19

Figure 2.3 OSN Matrix. 41

Figure 3.1 Structural phases of the thesis 52

Figure 3.2 Generic Mechanism for Pre-filtering Approach 54

Figure 3.3 Proposed Post-filtering Generic Mechanism for OSN Platform 56

Figure 3.4 Proposed Reliable Friendship Mechanism of OSN Platform 60

Figure 3.5 Pre-filtering Approach for Reliable Friend Selection 63

Figure 3.6 Proposed functionality of the SPY-Bot 80

Figure 3.7 Data Retrieval Technique 81

Figure 3.8 Methodology in designing a machine learning-enabled post-filtering approach for OSN. 85

Figure 4.1 Overview of results validation steps of the proposed friendship mechanism 98

Figure 4.2 Users' evaluation of Reliable Friend Selection by Security for different FRA approaches on OSNs 100

Figure 4.3 Users' evaluation of Reliable Friend Selection by flexibility for different FRA approaches on OSNs 101

Figure 4.4 Users' evaluation of Reliable Friend Selection by effectiveness for different FRA approaches on OSNs 102

Figure 4.5 Users' evaluation of Reliable Friend Selection by satisfaction for different FRA approaches on OSNs 103

Figure 4.6 User endorsement towards reliable friend selection, subject to 'flexibility', 'security', 'effectiveness' & 'satisfaction' 111
Figure 4.7 Class Distribution 117
Figure 4.8 Accuracy 120
Figure 4.9 AUC-ROC Comparison between basic SVM and tuned SVM. 121
Figure 4.10 AUC-ROC Comparison between basic SVM and tuned SVM after Feature Engineering. 121
Figure 4.11 AUC-ROC Comparison between basic Logistic Regression and tuned Logistic Regression. 122
Figure 4.12 AUC-ROC Comparison between basic Logistic Regression and tuned Logistic Regression after Feature Engineering. 122
Figure 4.13 AUC-ROC curve for test dataset 123
Figure 4.14 AUC-ROC curve for test dataset after Feature Engineering 124
Figure 4.15 User perceptions in terms of security, reliability, behavioral analysis and offensive activities for a reliable friendship 131
Figure 4.16 User consent regarding Preference for a Reliable Friendship in OSN 134

# REFERENCES


Adamic, L., & Adar, E. (2005). How to search a social network. *Social networks*, *27*(3), 187–203.

Adamkani, J., & Nirmala, K. (2015). A content filtering scheme in social sites. *Indian Journal of Science and Technology*, *8*(33).

Adams, R. (2019). *Social media urged to take 'moment to reflect' after girl's death.*

Adewole, K. S., Anuar, N. B., Kamsin, A., & Sangaiah, A. K. (2017). Smsad: a framework for spam message and spam account detection. *Multimedia Tools and Applications*, 1–36.

Agarwal, S., & Sureka, A. (2015). Applying social media intelligence for predicting and identifying on-line radicalization and civil unrest oriented threats. *arXiv preprint arXiv:1511.06858*.

Aghasian, E., Garg, S., Gao, L., Yu, S., & Montgomery, J. (2017). Scoring users' privacy disclosure across multiple online social networks. *IEEE access*, *5*, 13118–13130.

Aiello, L. M., Barrat, A., Schifanella, R., Cattuto, C., Markines, B., & Menczer, F. (2012). Friendship prediction and homophily in social media. *ACM Transactions on the Web (TWEB)*, *6*(2), 1–33.

Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. *Journal of Computational Science*, *25*, 152–160.

Anderson, J., Bresnahan, M., & Musatics, C. (2014). Combating weight-based cyberbullying on facebook with the dissenter effect. *Cyberpsychology, Behavior, and Social Networking*, *17*(5), 281–286.

Armstrong, M. (2020). *16% of all facebook accounts are fake or duplicates.*

Baca, M., Cosic, J., & Cosic, Z. (2013). Forensic analysis of social networks (case study). In *Proceedings of the iti 2013 35th international conference on information technol-*

*ogy interfaces* (pp. 219–223).

Bastiaensens, S., Vandebosch, H., Poels, K., Van Cleemput, K., Desmet, A., & De Bourdeaudhuij, I. (2014). Cyberbullying on social network sites. an experimental study into bystanders' behavioural intentions to help the victim or reinforce the bully. *Computers in Human Behavior*, *31*, 259–271.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, 1017–1041.

Benevenuto, F., Rodrigues, T., Cha, M., & Almeida, V. (2009). Characterizing user behavior in online social networks. In *Proceedings of the 9th acm sigcomm conference on internet measurement* (pp. 49–62).

Benkhelifa, R., & Laallam, F. Z. (2016). Facebook posts text classification to improve information filtering. In *Webist (1)* (pp. 202–207).

Boser, B. E., Guyon, I. M., & Vapnik, V. N. (1992). A training algorithm for optimal margin classifiers. In *Proceedings of the fifth annual workshop on computational learning theory* (pp. 144–152).

Buettner, R. (2017). Predicting user behavior in electronic markets based on personality-mining in large online social networks. *Electronic Markets*, *27*(3), 247–265.

Caramujo, J., & da Silva, A. M. R. (2015). Analyzing privacy policies based on a privacy-aware profile: The facebook and linkedin case studies. In *2015 ieee 17th conference on business informatics* (Vol. 1, pp. 77–84).

Carter, D. (2016). Hustle and brand: The sociotechnical shaping of influence. *Social Media+ Society*, *2*(3), 2056305116666305.

Charfi, I., Miteran, J., Dubois, J., Atri, M., & Tourki, R. (2012). Definition and performance evaluation of a robust svm based fall detection solution. In *2012 eighth international conference on signal image technology and internet based systems* (pp. 218–224).

Chavan, V. S., & Shylaja, S. (2015). Machine learning approach for detection of cyber-aggressive comments by peers on social media network. In *2015 international conference on advances in computing, communications and informatics (icacci)* (pp. 2354–2358).

Chen, C., Wen, S., Zhang, J., Xiang, Y., Oliver, J., Alelaiwi, A., & Hassan, M. M. (2017). Investigating the deceptive information in twitter spam. *Future Generation Com-*

*puter Systems*, *72*, 319–326.

Chen, H., & Jin, H. (2015). Efficient keyword searching in large-scale social network service. *IEEE Transactions on Services Computing*.

Chen, K.-H., & Liang, T. (2013). Friendship prediction on social network users. In *Social computing (socialcom), 2013 international conference on* (pp. 379–384).

Chen, W., & Fong, S. (2010). Social network collaborative filtering framework and online trust factors: A case study on facebook. In *2010 fifth international conference on digital information management (icdim)* (pp. 266–273).

Chen, Y., Zhou, Y., Zhu, S., & Xu, H. (2012). Detecting offensive language in social media to protect adolescent online safety. In *2012 international conference on privacy, security, risk and trust and 2012 international confernece on social computing* (pp. 71–80).

Cho, E., Myers, S. A., & Leskovec, J. (2011). Friendship and mobility: user movement in location-based social networks. In *Proceedings of the 17th acm sigkdd international conference on knowledge discovery and data mining* (pp. 1082–1090).

Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2015). Fame for sale: Efficient detection of fake twitter followers. *Decision Support Systems*, *80*, 56–71.

Das, K., & Sinha, S. K. (2016). A survey on user behaviour analysis in social networks. *International Journal of Computer Science and Information Security*, *14*(11), 895.

Deshpande, V. M., & Nair, M. K. (2017). A novel framework for privacy preserving ad-free social networking. In *2017 2nd international conference for convergence in technology (i2ct)* (pp. 139–145).

Devineni, P., Koutra, D., Faloutsos, M., & Faloutsos, C. (2017). Facebook wall posts: a model of user behaviors. *Social Network Analysis and Mining*, *7*(1), 6.

Dong, X., Shen, J., Wang, W., Liu, Y., Shao, L., & Porikli, F. (2018). Hyperparameter optimization for tracking with continuous deep q-learning. In *Proceedings of the ieee conference on computer vision and pattern recognition* (pp. 518–527).

Dong, Y. (2016). User modeling in large social networks. In *Proceedings of the ninth acm international conference on web search and data mining* (pp. 713–713).

Elmendili, F., Maqran, N., Idrissi, Y. E. B. E., & Chaoui, H. (2018). A security approach

based on honeypots: Protecting online social network from malicious profiles. *arXiv preprint arXiv:1804.09988*.

Ferri, C., Hernández-Orallo, J., & Modroiu, R. (2009). An experimental comparison of performance measures for classification. *Pattern Recognition Letters*, *30*(1), 27–38.

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*, *16*(4), 2019–2036.

Fong, P. W., Anwar, M., & Zhao, Z. (2009). A privacy preservation model for facebook-style social network systems. In *European symposium on research in computer security* (pp. 303–320).

Fong, S., Zhuang, Y., & He, J. (2012). Not every friend on a social network can be trusted: Classifying imposters using decision trees. In *The first international conference on future generation communication technologies* (pp. 58–63).

Foody, M., Samara, M., El Asam, A., Morsi, H., & Khattab, A. (2017). A review of cyberbullying legislation in qatar: Considerations for policy makers and educators. *International journal of law and psychiatry*, *50*, 45–51.

Foong, Y. J., & Oussalah, M. (2017). Cyberbullying system detection and analysis. In *2017 european intelligence and security informatics conference (eisic)* (pp. 40–46).

Fox, J., & Moreland, J. J. (2015). The dark side of social networking sites: An exploration of the relational and psychological stressors associated with facebook use and affordances. *Computers in human behavior*, *45*, 168–176.

Ganesan, R., Hemalatha, D., & Joseph, J. (2017). Enhanced privacy settings in online content sharing websites using key distribution center (kdc). *International Journal of Civil Engineering and Technology*, *8*(9), 725–732.

Géron, A. (2019). *Hands-on machine learning with scikit-learn, keras, and tensorflow: Concepts, tools, and techniques to build intelligent systems*. O'Reilly Media.

Ghorbani, S., & Ganjali, Y. (2012). Will you be my friend? privacy implications of accepting friendships in online social networks. In *International conference on information society (i-society 2012)* (pp. 340–345).

Gou, L., You, F., Guo, J., Wu, L., & Zhang, X. (2011). Sfviz: interest-based friends exploration and recommendation in social networks. In *Proceedings of the 2011 visual information communication-international symposium* (pp. 1–10).

Gupta, A., Budania, H., Singh, P., & Singh, P. K. (2017). Facebook based choice filtering. In *Advance computing conference (iacc), 2017 ieee 7th international* (pp. 875–879).

Hanani, U., Shapira, B., & Shoval, P. (2001, Aug 01). Information filtering: Overview of issues, research and systems. *User Modeling and User-Adapted Interaction*, *11*(3), 203–259. doi: 10.1023/A:1011196000674

Hasbullah, S. S. (2016). Rule-based agent for social media sentiment detection. In *Agent, multi-agent systems and robotics (isamsr), 2016 2nd international symposium on* (pp. 128–132).

Hattingh, F., Buitendag, A., & Thompson, W. (2014). User willingness to accept friend requests on sns: A facebook experiment. In *2014 ist-africa conference proceedings* (pp. 1–8).

Huang, J., Hu, Z., & Dai, Z. (n.d.). Efficient keyword search over online social network by using stream dynamic bloom filter. In *2017 international conference on dependable systems and their applications (dsa)* (pp. 172–177).

Hunt, S. D., Sparkman Jr, R. D., & Wilcox, J. B. (1982). The pretest in survey research: Issues and preliminary findings. *Journal of marketing research*, *19*(2), 269–273.

Jiang, W., Wu, J., & Wang, G. (2013). RATE: Recommendation-aware trust evaluation in online social networks. In *Proc. 12th ieee international symposium on network computing and applications (nca)* (pp. 149–152).

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research*, *37*(5), 858–873.

Kansara, K. B., & Shekokar, N. M. (2015). A framework for cyberbullying detection in social network. *International Journal of Current Engineering and Technology*, *5*(1), 494–498.

Kaveri, V. V., & Gopal, S. (2015). Notifying and filtering undesirable messages from online social network (osn). In *International confernce on innovation information in computing technologies* (pp. 1–8).

Kiliroor, C. C., & Valliyammai, C. (2017). Trust analysis on social networks for identifying authenticated users. In *Proc. 8th international conference on advanced computing (icoac)* (pp. 37–41).

Kontostathis, A., Reynolds, K., Garron, A., & Edwards, L. (2013). Detecting cyberbully-

ing: query terms and techniques. In *Proceedings of the 5th annual acm web science conference* (pp. 195–204).

Lakshmi, R. (2016). *This islamic preacher might have influenced one of the dhaka terrorists. now indians want him banned.*

Lampe, C. A., Ellison, N., & Steinfield, C. (2007). A familiar face (book) profile elements as signals in an online social network. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 435–444).

Li, N., & Chen, G. (2009). Multi-layered friendship modeling for location-based mobile social networks. In *2009 6th annual international mobile and ubiquitous systems: Networking & services, mobiquitous* (pp. 1–10).

Liu, B., Xiao, Z., Zhang, T., & Cao, J. (2012). Analysis on the security mechanisms of user data protection in facebook. In *2012 7th international conference on computing and convergence technology (iccct)* (pp. 532–536).

Liu, S. (2018). User modeling for point-of-interest recommendations in location-based social networks: The state of the art. *Mobile Information Systems*, *2018*.

Lo, S., & Lin, C. (2006). Wmr–a graph-based algorithm for friend recommendation. In *2006 ieee/wic/acm international conference on web intelligence (wi 2006 main conference proceedings)(wi'06)* (pp. 121–128).

Luo, H., Guo, B., Wang, Z., Feng, Y., et al. (2013). Friendship prediction based on the fusion of topology and geographical features in lbsn. In *2013 ieee 10th international conference on high performance computing and communications & 2013 ieee international conference on embedded and ubiquitous computing* (pp. 2224–2230).

Ma, J., Xu, H., & Chen, H. (2013). Friendship prediction in recommender system. *Journal of National University of Defense Technology*, *35*(1), 163–168.

Maia, M., Almeida, J., & Almeida, V. (2008). Identifying user behavior in online social networks. In *Proceedings of the 1st workshop on social network systems* (pp. 1–6).

Manoharan, S., & Ge, T. (2013). A demerit point strategy to reduce free-riding in bittorrent. *Computer communications*, *36*(8), 875–880.

Mansoor, T., & Ali, M. M. (2017). Content-based access control in an online community. In *Proc. 8th international conference on information technology (icit)* (pp. 677–684).

Maune, T. (2013). *Family of north tulsa teenage girl devastated by her stabbing death.*

McGibbon, R., Hernández, C., Harrigan, M., Kearnes, S., Sultan, M., Jastrzebski, S., ... Pande, V. (2016). Osprey: Hyperparameter optimization for machine learning. *Journal of Open Source Software*, *1*(5), 34.

Mislove, A., Marcon, M., Gummadi, K. P., Druschel, P., & Bhattacharjee, B. (2007). Measurement and analysis of online social networks. In *Proceedings of the 7th acm sigcomm conference on internet measurement* (pp. 29–42).

Mubarak, H., Darwish, K., & Magdy, W. (2017). Abusive language detection on arabic social media. In *Proceedings of the first workshop on abusive language online* (pp. 52–56).

Nguyen-Son, H.-Q., Tran, M.-T., Yoshiura, H., Noboru, S., & Echizen, I. (2014). A system for anonymizing temporal phrases of message posted in online social networks and for detecting disclosure. In *2014 ninth international conference on availability, reliability and security* (pp. 455–460).

Nidhi, R., & Annappa, B. (2017). Twitter-user recommender system using tweets: A content-based approach. In *2017 international conference on computational intelligence in data science (iccids)* (pp. 1–6).

Niland, P., Lyons, A. C., Goodwin, I., & Hutton, F. (2015). Friendship work on facebook: Young adults' understandings and practices of friendship. *Journal of Community & Applied Social Psychology*, *25*(2), 123–137.

Obar, J. A., & Wildman, S. S. (2015). Social media definition and the governance challenge-an introduction to the special issue. *Obar, JA and Wildman, S.(2015). Social media definition and the governance challenge: An introduction to the special issue. Telecommunications policy*, *39*(9), 745–750.

Okemwa, J. G. (2017). Filtering online social networks based on user content generation. *International Journal*, *7*(3).

OrdinalData. (n.d.). *What is the difference between categorical, ordinal and interval variables.*

Parimi, R., & Caragea, D. (2011). Predicting friendship links in social networks using a topic modeling approach. In *Pacific-asia conference on knowledge discovery and data mining* (pp. 75–86).

People, Y. (n.d.). A childnet international research report.

pewresearch. (2021). *Majority of people who've been harassed online say the most recent experience occurred on social media.*

Prakash, G., Saurav, N., & Kethu, V. R. (2016). An effective undesired content filtration and predictions framework in online social network. *International Journal of Advances in Signal and Image Sciences*, *2*(2), 1–8.

Rahman, M. A., Mezhuyev, V., Bhuiyan, M. Z. A., Sadat, S. N., Zakaria, S. A. B., & Refat, N. (2018). Reliable decision making of accepting friend request on online social networks. *IEEE Access*, *6*, 9484–9491.

Raveendirarasa, V., & Amalraj, C. (2020). Sentiment analysis of tamil-english code-switched text on social media using sub-word level lstm. In *2020 5th international conference on information technology research (icitr)* (pp. 1–5).

Rose, J. A., & Pravin, A. (2014). Machine learning text categorization in osn to filter unwanted messages. *IJCSIT) International Journal of Computer Science and Information Technologies, ISSN*, 0975–9646.

Rudra, K., Sharma, A., Ganguly, N., & Ghosh, S. (2018). Characterizing and countering communal microblogs during disaster events. *IEEE Transactions on Computational Social Systems*, *5*(2), 403–417.

Sahay, K., Khaira, H. S., Kukreja, P., & Shukla, N. (2018). Detecting cyberbullying and aggression in social commentary using nlp and machine learning. *International Journal of Engineering Technology Science and Research*, *5*(1).

Salunkhe, P., Bharne, S., & Padiya, P. (2016). Filtering unwanted messages from OSN walls. In *Proc. international conference on innovation and challenges in cyber security (iciccs-inbush)* (pp. 261–264).

Santosh, P., & Kumar, R. P. (2014). Filtered wall: An automated system to filter unwanted messages from OSN user profiles. *IJRCCT*, *3*(9), 1122–1127.

Sarna, G., & Bhatia, M. (2017). Content based approach to find the credibility of user in social networks: an application of cyberbullying. *International Journal Of Machine Learning and Cybernetics*, *8*(2), 677–689.

Savyan, P., & Bhanu, S. M. S. (2017). Behaviour profiling of reactions in facebook posts for anomaly detection. In *2017 ninth international conference on advanced computing (icoac)* (pp. 220–226).

Schneider, F., Feldmann, A., Krishnamurthy, B., & Willinger, W. (2009). Understanding

online social network usage from a network perspective. In *Proceedings of the 9th acm sigcomm conference on internet measurement* (pp. 35–48).

Shao, W., & Ross, M. (2015). Testing a conceptual model of facebook brand page communities. *Journal of Research in Interactive Marketing*.

Sharma, V., You, I., & Kumar, R. (2017). Isma: Intelligent sensing model for anomalies detection in cross platform osns with a case study on iot. *IEEE Access*, *5*, 3284–3301.

Shen, X., Long, H., & Ma, C. (2015). Incorporating trust relationships in collaborative filtering recommender system. In *Proc. 16th ieee/acis international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (snpd)* (pp. 1–8).

Singer, H. M., Singer, I., & Herrmann, H. J. (2009). Agent-based model for friendship in social networks. *Physical Review E*, *80*(2), 026113.

Srividya, M., & Ahmed, M. I. (2017). A filtering of message in online social network using hybrid classifier. *Cluster Computing*, 1–8.

Statista. (2022). *Most famous social network sites 2012, by active users.*

Stroud, S. R., & Henson, J. A. (2017). Social media, online sharing, and the ethical complexity of consent in revenge porn. In *The dark side of social media* (pp. 37–56). Routledge.

Subramaniyaswamy, V., Logesh, R., Vijayakumar, V., & Indragandhi, V. (2015). Automated message filtering system in online social network. *Procedia Computer Science*, *50*, 466–475.

Sun, D., Zhang, X., Choo, K.-K. R., Hu, L., & Wang, F. (2021). Nlp-based digital forensic investigation platform for online communications. *Computers & Security*, *104*, 102210.

Supe, A., & Phursule, R. (2015). A system to clarify unwanted messages from osn user surface. *International Journal of Scientific Engineering and Research (IJSER)*, *3*(5).

Talekar, S., & Nagori, M. (2015). Classification of messages and content based filtering from osn user walls. *International Journal of Computer Applications*, *115*(10).

Tian, Y., Sun, M., Deng, Z., Luo, J., & Li, Y. (2017). A new fuzzy set and nonkernel svm approach for mislabeled binary classification with applications. *IEEE Transactions*

*on Fuzzy Systems*, *25*(6), 1536–1545.

Tidke, S., & SaritaGangbhoj, A. (n.d.). Unwanted message filtration from online social network (osn).

Turner, C. R., Fuggetta, A., Lavazza, L., & Wolf, A. L. (1999). A conceptual basis for feature engineering. *Journal of Systems and Software*, *49*(1), 3–15.

Ujwala, T., & Vaidya, A. S. (2014). A review paper on filter unwanted messages from osn. *(International Journal of Computer Science and Information Technologies,*.

Uttarwar, M. M., Patil, P., & Bhute, Y. (2014, Aug.). A customizable content based system to filter unwanted messages from OSN user wall. *IJCSMC*, *3*(8), 653–661.

Va, S., Rb, L., Vc, V., & Vd, I. (2015). Automated message filtering system in online social network. *Procedia Computer Science*, *50*, 466–475.

Vairagade, A. S., & Fadnavis, R. A. (2016). Automated content based short text classification for filtering undesired posts on facebook. In *2016 world conference on futuristic trends in research and innovation for social welfare (startup conclave)* (pp. 1–5).

Vanetti, M., Binaghi, E., Carminati, B., Carullo, M., & Ferrari, E. (2011). Content-based filtering in on-line social networks. In C. Dimitrakakis, A. Gkoulalas-Divanis, A. Mitrokotsa, V. S. Verykios, & Y. Saygin (Eds.), *Privacy and security issues in data mining and machine learning* (pp. 127–140). Berlin, Heidelberg: Springer Berlin Heidelberg.

Vanetti, M., Binaghi, E., Ferrari, E., Carminati, B., & Carullo, M. (2011). A system to filter unwanted messages from osn user walls. *IEEE Transactions on Knowledge and data Engineering*, *25*(2), 285–297.

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283–297.

Vidhate, D. D., & Thakare, A. P. (2015). An avoid unwanted messages from osn user wall: Content based filtering approach. *International Journal of Computer Science and Network Security (IJCSNS)*, *15*(5), 50.

Vishwanath, A. (2015). Habitual facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, *20*(1), 83–98.

Viswanath, B., Bashir, M. A., Crovella, M., Guha, S., Gummadi, K. P., Krishnamurthy,

B., & Mislove, A. (2014). Towards detecting anomalous user behavior in online social networks. In *23rd {USENIX} security symposium ({USENIX} security 14)* (pp. 223–238).

Waheed, H., Anjum, M., Rehman, M., & Khawaja, A. (2017). Investigation of user behavior on social networking sites. *PloS one*, *12*(2), e0169693.

Wang, C., Bo, T., Zhao, Y. W., Chi, C.-H., Lam, K.-Y., Wang, S., & Shu, M. (2018). Behavior-interior-aware user preference analysis based on social networks. *Complexity*, *2018*.

Wang, Y., & Priestley, J. L. (2017). Binary classification on past due of service accounts using logistic regression and decision tree.

Wisniewski, P., Knijnenburg, B. P., & Lipford, H. R. (2014). Profiling facebook users' privacy behaviors. In *Soups2014 workshop on privacy personas and segmentation.*

Wolpert, D. H. (1996). The lack of a priori distinctions between learning algorithms. *Neural computation*, *8*(7), 1341–1390.

Xie, X. (2010). Potential friend recommendation in online social network. In *2010 ieee/acm int'l conference on green computing and communications & int'l conference on cyber, physical and social computing* (pp. 831–835).

Xu-Rui, G., Li, W., & Wei-Li, W. (2015). An algorithm for friendship prediction on location-based social networks. In *International conference on computational social networks* (pp. 193–204).

Yadav, S. H., & Manwatkar, P. M. (2015). An approach for offensive text detection and prevention in social networks. In *Proc. international conference on innovations in information, embedded and communication systems (iciiecs)* (pp. 1–4).

Yan, Q., Wu, L., & Zheng, L. (2013). Social network based microblog user behavior analysis. *Physica A: Statistical Mechanics and Its Applications*, *392*(7), 1712–1723.

Yang, S.-H., Long, B., Smola, A., Sadagopan, N., Zheng, Z., & Zha, H. (2011). Like like alike: joint friendship and interest propagation in social networks. In *Proceedings of the 20th international conference on world wide web* (pp. 537–546).

Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2017). Comprehensive study of symmetric key and asymmetric key encryption algorithms. In *2017 international conference on engineering and technology (icet)* (pp. 1–7).

Yassein, M. B., Aljawarneh, S., & Wahsheh, Y. A. (2019). Survey of online social networks threats and solutions. In *2019 ieee jordan international joint conference on electrical engineering and information technology (jeeit)* (pp. 375–380).

Yin, H., Cui, B., Chen, L., Hu, Z., & Zhou, X. (2015). Dynamic user modeling in social media systems. *ACM Transactions on Information Systems (TOIS)*, *33*(3), 10.

Yoo, S.-Y., & Jeong, O.-R. (2013). SNS based recommendation algorithm. In *Proc. international conference on information science and applications (icisa)* (pp. 1–3).

Yousukkee, S. (2016). Survey of analysis of user behavior in online social network. In *2016 management and innovation technology international conference (miticon)* (pp. MIT–128).

Yu, D., Chen, N., Jiang, F., Fu, B., & Qin, A. (2017). Constrained nmf-based semi-supervised learning for social media spammer detection. *Knowledge-Based Systems*, *125*, 64–73.

Zhang, H., Zhang, L., & Jiang, Y. (2019). Overfitting and underfitting analysis for deep learning based end-to-end communication systems. In *2019 11th international conference on wireless communications and signal processing (wcsp)* (pp. 1–6).

Zhang, Y., & Pang, J. (2015). Distance and friendship: A distance-based model for link prediction in social networks. In *Asia-pacific web conference* (pp. 55–66).

Zhong, E., Xiang, E. W., Fan, W., Liu, N. N., & Yang, Q. (2014). Friendship prediction in composite social networks. *arXiv preprint arXiv:1402.4033*.