**Important Research Papers’ List**

| Citation No. | Important Papers | Assigned Member Names for Important Papers |
| --- | --- | --- |
| 1 | X. Zheng, Z. Zeng, Z. Chen, Y. Yu, and C. Rong, “Detecting spammers on social networks,” Neurocomputing, vol. 159, pp. 27–34, Jul. 2015, doi: 10.1016/j.neucom.2015.02.047. | [Rahul Nayak](mailto:rrnayak@asu.edu) |
| 2 | S. Gheewala and R. Patel, "Machine Learning Based Twitter Spam Account Detection: A Review," 2018 Second International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2018, pp. 79-84, doi: 10.1109/ICCMC.2018.8487992. | [Rahul Nayak](mailto:rrnayak@asu.edu) |
| 3 | S. Shinde and S. B. Mane, "Malicious Profile Detection on Social Media: A Survey Paper," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2021, pp. 1-5, doi: 10.1109/ICRITO51393.2021.9596322. | [Rahul Nayak](mailto:rrnayak@asu.edu) |
| 4 | M. Jiang, P. Cui and C. Faloutsos, "Suspicious Behavior Detection: Current Trends and Future Directions," in IEEE Intelligent Systems, vol. 31, no. 1, pp. 31-39, Jan.-Feb. 2016, doi: 10.1109/MIS.2016.5. | [Rahul Nayak](mailto:rrnayak@asu.edu) |
| 5 | X. Qi and M. Zong, “An overview of privacy preserving data mining,” Procedia Environmental Sciences, vol. 12, pp. 1341–1347, Jan. 2012, doi: 10.1016/j.proenv.2012.01.432. | [Gautham Vijayaraj](mailto:gvijaya6@asu.edu) |
| 6 | M. Binjubeir, A. A. Ahmed, M. A. B. Ismail, A. S. Sadiq and M. Khurram Khan, "Comprehensive Survey on Big Data Privacy Protection," in IEEE Access, vol. 8, pp. 20067-20079, 2020, doi: 10.1109/ACCESS.2019.2962368. | [Gautham Vijayaraj](mailto:gvijaya6@asu.edu) |
| 7 | J. Vaidya and C. Clifton, "Privacy-preserving data mining: why, how, and when," in IEEE Security & Privacy, vol. 2, no. 6, pp. 19-27, Nov.-Dec. 2004, doi: 10.1109/MSP.2004.108. | [Gautham Vijayaraj](mailto:gvijaya6@asu.edu) |
| 8 | M. S. Sudha, K. A. Priya, A. K. Lakshmi, A. Kruthika, D. L. Priya and K. Valarmathi, "Data Mining Approach for Anomaly Detection in Social Network Analysis," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 2018, pp. 1862-1866, doi: 10.1109/ICICCT.2018.8472985. | [Gautham Vijayaraj](mailto:gvijaya6@asu.edu) |
| 9 | A. P. Jain and V. D. Katkar, "Sentiments analysis of Twitter data using data mining," 2015 International Conference on Information Processing (ICIP), Pune, India, 2015, pp. 807-810, doi: 10.1109/INFOP.2015.7489492. | [Gautham Vijayaraj](mailto:gvijaya6@asu.edu) |
| 10 | S. Gharge and M. K. Chavan, “An integrated approach for malicious tweets detection using NLP,” International Conference on Inventive Communication and Computational Technologies, Mar. 2017, doi: 10.1109/icicct.2017.7975235. | [Krupaben Kothadia](mailto:kkothadi@asu.edu) |
| 11 | A. Kumar and S. Singh, “Detection of User Cluster with Suspicious Activity in Online Social Networking Sites,” 2013 Second International Conference on Advanced Computing, Networking and Security, Dec. 2013, doi: 10.1109/adcons.2013.17. | [Krupaben Kothadia](mailto:kkothadi@asu.edu) |
| 12 | M. S. Al-Ghamdi and M. A. Khan, “Intelligent analysis of Arabic tweets for detection of suspicious messages,” Arabian Journal for Science and Engineering, vol. 45, no. 8, pp. 6021–6032, Mar. 2020, doi: 10.1007/s13369-020-04447-0. | [Krupaben Kothadia](mailto:kkothadi@asu.edu) |
| 13 | M. P. Selvan and R. Selvaraj, “Mining user Message Pattern for Suspicious Behavior on Terrorism using NLP in Social Networks with Single Sign-On,” Indian Journal of Science and Technology, Apr. 2017, doi: 10.17485/ijst/2017/v10i14/111364. | [Krupaben Kothadia](mailto:kkothadi@asu.edu) |
| 14 | S. A. Mansoori, A. Almansoori, M. Alshamsi, S. A. Salloum, and K. Shaalan, “Suspicious Activity Detection of Twitter and Facebook using Sentimental Analysis,” TEM Journal, pp. 1313–1319, Nov. 2020, doi: 10.18421/tem94-01. | [Krupaben Kothadia](mailto:kkothadi@asu.edu) |
| 15 | S. Ghosal, A. Jain and D. K. Tayal, "An approach to detect abusive content incorporating Word2Vec and Multilayer Perceptron," 2022 IEEE Bombay Section Signature Conference (IBSSC), Mumbai, India, 2022, pp. 1-5, doi: 10.1109/IBSSC56953.2022.10037274. | [Avani Mundra](mailto:amudra@asu.edu) |
| 16 | S. Alami and O. Elbeqqali, “Cybercrime profiling: Text mining techniques to detect and predict criminal activities in microblog posts,” International Conference on Intelligent Systems: Theories and Applications (SITA), Oct. 2015, doi: 10.1109/sita.2015.7358435. | [Avani Mundra](mailto:amudra@asu.edu) |
| 17 | S. Mitra, T. Tasnim, M. A. R. Islam, N. I. Khan and M. S. Majib, "A Framework to Detect and Prevent Cyberbullying from Social Media by Exploring Machine Learning Algorithms," 2021 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2), Rajshahi, Bangladesh, 2021, pp. 1-4, doi: 10.1109/IC4ME253898.2021.9768450. | [Avani Mundra](mailto:amudra@asu.edu) |
| 18 | S. Garg, K. Kaur, N. Kumar and J. J. P. C. Rodrigues, "Hybrid Deep-Learning-Based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective," in IEEE Transactions on Multimedia, vol. 21, no. 3, pp. 566-578, March 2019, doi: 10.1109/TMM.2019.2893549. | [Yeshwanth Reddy Chennur](mailto:ychennur@asu.edu) |
| 19 | S. Mittal, P. K. Das, V. Mulwad, A. Joshi and T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), San Francisco, CA, USA, 2016, pp. 860-867, doi: 10.1109/ASONAM.2016.7752338. | [Anuranjan Dubey](mailto:adubey37@asu.edu) |
| 20 | A. Ritter, E. Wright, W. Casey, and T. Mitchell, “Weakly supervised extraction of computer security events from twitter,” Florence, Italy: International World Wide Web Conferences Steering Committee, 2015, pp. 896–905. doi: https://doi.org/10.1145/2736277.2741083. | [Anuranjan Dubey](mailto:adubey37@asu.edu) |
| 21 | S. W. Liew, N. F. M. Sani, M. T. Abdullah, R. Yaakob, and M. Y. Sharum, “An effective security alert mechanism for real-time phishing tweet detection on Twitter,” Computers & Security, vol. 83, pp. 201–207, Jun. 2019, doi: 10.1016/j.cose.2019.02.004. | [Anuranjan Dubey](mailto:adubey37@asu.edu) |
| 22 | N. Dionísio, F. Alves, P. M. Ferreira and A. Bessani, "Cyberthreat Detection from Twitter using Deep Neural Networks," 2019 International Joint Conference on Neural Networks (IJCNN), Budapest, Hungary, 2019, pp. 1-8, doi: 10.1109/IJCNN.2019.8852475. | [Anuranjan Dubey](mailto:adubey37@asu.edu) |
| 23 | G. Rathee, S. Garg, G. Kaddoum, D. N. K. Jayakody, M. J. Piran and G. Muhammad, "A Trusted Social Network Using Hypothetical Mathematical Model and Decision- Based Scheme," in IEEE Access, vol. 9, pp. 4223-4232, 2021, doi: 10.1109/ACCESS.2020.3048077. | [Yeshwanth Reddy Chennur](mailto:ychennur@asu.edu) |
| 24 | Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu and V. C. M. Leung, "A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View," in IEEE Access, vol. 6, pp. 12103-12117, 2018, doi: 10.1109/ACCESS.2018.2805680. | [Yeshwanth Reddy Chennur](mailto:ychennur@asu.edu) |
| 25 | S. Jain, V. Sharma and R. Kaushal, "Towards automated real-time detection of misinformation on Twitter," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 2016, pp. 2015-2020, doi: 10.1109/ICACCI.2016.7732347. | [Yeshwanth Reddy Chennur](mailto:ychennur@asu.edu) |
| 26 | E. Osa and O. E. Oghenevbaire, “Comparative Analysis of Machine Learning Models in Computer Network Intrusion Detection”, In 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development, Lagos, Nigeria, 2022, pp. 1-5, doi: 10.1109/NIGERCON54645.2022.9803175 | [Justin Young](mailto:jtyoun15@asu.edu) |
| 27 | Z. Chkirbene, R. Camila, A. Erbad, S. Kiranyaz, N. Al-Emadi and M. Hamdi, “Cooperative Machine Learning Techniques for Cloud Intrusion Detection”, In 2021 International Wireless Communications and Mobile Computing, Harbin City, China pp. 837-842, doi: 10.1109/IWCMC51323.2021.9498809 | [Justin Young](mailto:jtyoun15@asu.edu) |
| 28 | S. Vanjire and M. Lakshmi, “Behavior-Based Malware Detection System Approach For Mobile Security Using Machine Learning, in 2021 International Conference on Artificial Intelligence and Machine Vision, Gandhinagar, India, pp. 1-4, doi: 10.1109/AIMV53313.2021.9671009 | [Justin Young](mailto:jtyoun15@asu.edu) |
| 29 | C. Chen, J Zhong and W. Chen, “Machine Learning-based web security intrusion detection system”, in 2021 3rd International Academic Exchange Conference on Science and Technology Innovation, Guangzhou, China, pp. 173-177, doi: 10.1109/IAECST54258.2021.9695557 | [Justin Young](mailto:jtyoun15@asu.edu) |
| 30 | Y. Xiao and J. Qiu, "Exploring and Detecting Opinion Spam on Social Media," 2020 Chinese Automation Congress (CAC), Shanghai, China, 2020, pp. 7570-7573, doi: 10.1109/CAC51589.2020.9327093. | [Sangeeth Santhosh](mailto:ssantho9@asu.edu) |
| 31 | H. Afzal and K. Mehmood, "Spam filtering of bi-lingual tweets using machine learning," 2016 18th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea (South), 2016, pp. 710-714, doi: 10.1109/ICACT.2016.7423530. | [Sangeeth Santhosh](mailto:ssantho9@asu.edu) |
| 32 | P. Sinha, O. Maini, G. Malik and R. Kaushal, "Ecosystem of spamming on Twitter: Analysis of spam reporters and spam reportees," 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 2016, pp. 1705-1710, doi: 10.1109/ICACCI.2016.7732293. | [Sangeeth Santhosh](mailto:ssantho9@asu.edu) |
| 33 | N. A. Ghanem and H. M. Habeeb, "Classifying Suspicious Content on Social Media Networks," 2021 International Conference on Advanced Computer Applications (ACA), Maysan, Iraq, 2021, pp. 171-175, doi: 10.1109/ACA52198.2021.9626788. | [Sangeeth Santhosh](mailto:ssantho9@asu.edu) |
| 34 | K. A. Djaballah, K. Boukhalfa, Z. Ghalem and O. Boukerma, "A new approach for the detection and analysis of phishing in social networks: the case of Twitter," 2020 Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS), Paris, France, 2020, pp. 1-8, doi: 10.1109/SNAMS52053.2020.9336572. | [Sangeeth Santhosh](mailto:ssantho9@asu.edu) |
| 35 | C. Prashanth, D. Chandrasekaran, B. Pandian, K. Duraipandian, T. Chen and M. Sathiyanarayanan, "Reveal: Online Fake Job Advert Detection Application using Machine Learning," 2022 IEEE Delhi Section Conference (DELCON), New Delhi, India, 2022, pp. 1-6, doi: 10.1109/DELCON54057.2022.9752784. | [Yeshwanth Reddy Chennur](mailto:ychennur@asu.edu) |
| 36 | J. Kaubiyal and A. K. Jain, “A feature based approach to detect fake profiles in twitter,” Melbourn, VIC, Australia: Association for Computing Machinery, 2019, pp. 135–139. doi: https://doi.org/10.1145/3361758.3361784. Available: https://doi.org/10.1145/3361758.3361784 | [Anuranjan Dubey](mailto:adubey37@asu.edu) |
| 37 | G. Sreelatha, A. Vinaya Babu, D. Midhunchakkarvarthy, “Ensure Anomaly-Aware Security Model for Dynamic Cloud Environment using Transfer Learning”, in “2020 5th International Conference on Communication and Electronics Systems (ICCES)”, 2020, pp. 666-670. doi: https://doi.org/10.1109/ICCES48766.2020.9138009 | [Justin Young](mailto:jtyoun15@asu.edu) |
| 38 | E. Mouhssine and C. Khalid, "Social Big Data Mining Framework for Extremist Content Detection in Social Networks," 2018 International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Rabat, Morocco, 2018, pp. 1-5, doi: 10.1109/ISAECT.2018.8618726. | [Avani Mundra](mailto:amudra@asu.edu) |
| 39 | S. G, D. Chandrasekaran, M. D. Sre and M. Sathiyanarayanan, "Predicting Abnormal User Behaviour Patterns in Social Media Platforms based on Process Mining," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 204-209, doi: 10.1109/IITCEE57236.2023.10091025. | [Avani Mundra](mailto:amudra@asu.edu) |
| 40 | K. J. Reza, Z. Islam, and V. Estivill‐Castro, “Privacy Preservation of Social Network Users Against Attribute Inference Attacks via Malicious Data Mining,” 5th International Conference on Information Systems Security and Privacy, Jan. 2019, doi: 10.5220/0007390404120420. | [Gautham Vijayaraj](mailto:gvijaya6@asu.edu) |
| 41 | J. R. Sánchez et al., “Uncovering Cybercrimes in Social Media through Natural Language Processing,” Complexity, vol. 2021, pp. 1–15, Dec. 2021, doi: 10.1155/2021/7955637. | [Krupaben Kothadia](mailto:kkothadi@asu.edu) |
| 42 | J. Martínez-Romo and L. Araujo, “Detecting malicious tweets in trending topics using a statistical analysis of language,” Expert Systems With Applications, vol. 40, no. 8, pp. 2992–3000, June 2013, doi: 10.1016/j.eswa.2012.12.015. | [Krupaben Kothadia](mailto:kkothadi@asu.edu) |
| 43 | N. Z. Gong, M. Frank and P. Mittal, "SybilBelief: A Semi-Supervised Learning Approach for Structure-Based Sybil Detection," in IEEE Transactions on Information Forensics and Security, vol. 9, no. 6, pp. 976-987, June 2014, doi: 10.1109/TIFS.2014.2316975. | [Rahul Nayak](mailto:rrnayak@asu.edu) |
| 44 | S. G. Sutar, "Intelligent data mining technique of social media for improving health care," in International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 1356-1360, June 2017, doi: 10.1109/ICCONS.2017.8250690. | [Gautham Vijayaraj](mailto:gvijaya6@asu.edu) |

**Not so Important Research Papers’ List**

| Citation No. | Not so Important Papers |
| --- | --- |
| 1 | V. U. Gongane, M. V. Munot, and A. Anuse, “Detection and moderation of detrimental content on social media platforms: current status and future directions,” Social Network Analysis and Mining, vol. 12, no. 1, Sep. 2022, doi: 10.1007/s13278-022-00951-3. |
| 2 | S. Aldera, A. Emam, M. Al-Qurishi, M. Alrubaian and A. Alothaim, "Online Extremism Detection in Textual Content: A Systematic Literature Review," in IEEE Access, vol. 9, pp. 42384-42396, 2021, doi: 10.1109/ACCESS.2021.3064178. |
| 3 | A. Geiger, D. Liu, S. Alnegheimish, A. Cuesta-Infante and K. Veeramachaneni, "TadGAN: Time Series Anomaly Detection Using Generative Adversarial Networks," 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 33-43, doi: 10.1109/BigData50022.2020.9378139. |
| 4 | L. Safarnejad, Q. Xu, Y. Ge and S. Chen, "A Multiple Feature Category Data Mining and Machine Learning Approach to Characterize and Detect Health Misinformation on Social Media," in IEEE Internet Computing, vol. 25, no. 5, pp. 43-51, 1 Sept.-Oct. 2021, doi: 10.1109/MIC.2021.3063257. |
| 5 | Anna L. Buczak, Erhan Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153 - 1176, 26 October 2015, doi: 10.1109/COMST.2015.2494502. |
| 6 | N. Cao, C. Shi, S. Lin, J. Lu, Y. Lin, C. Lin, “TargetVue: Visual Analysis of Anomalous User Behaviors in Online Communication Systems”, in IEEE Transactions on Visualization and Computer Graphics, vol. 22, no. 1, pp. 280-289, 11 August 2015, doi: 10.1109/TVCG.2015.2467196 |
| 7 | Ravneet Kaur, Sarbjeet Singh. "A survey of data mining and social network analysis-based anomaly detection techniques." Egyptian Informatics Journal, Volume 17, Issue 2, 2016, Pages 199-216. ISSN 1110-8665. doi: 10.1016/j.eij.2015.11.004. |
| 8 | T.R Soumya, S.Solai Manohar, N.Bala Sundara Ganapathy, Leema Nelson, A. Mohan, M.Thurai Pandian. "Profile Similarity Recognition in Online Social Network using Machine Learning Approach" in International Conference on Inventive Research in Computing Applications (ICIRCA), 29 December 2022, Pages 805-809. ISSN 22473631 doi:10.1109/ICIRCA54612.2022.9985683. |
| 9 | AlAjlan, Shatha AbdulAziz and A. Khader, “Machine learning approach for threat detection on social media posts containing Arabic text,” Evolutionary Intelligence, vol. 14, no. 2, pp. 811–822, 2021, doi: https://doi.org/10.1007/s1206502000458w. |
| 10 | Z. Abbass, Z. Ali, M. Ali, B. Akbar and A. Saleem, "A Framework to Predict Social Crime through Twitter Tweets By Using Machine Learning," 2020 IEEE 14th International Conference on Semantic Computing (ICSC), San Diego, CA, USA, 2020, pp. 363-368, doi: 10.1109/ICSC.2020.00073. |