REFERENCES

[1] C. Yang, R. Harkreader and G. Gu, "Empirical evaluation and new design for fighting evolving twitter spammers," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 8, AUGUST 2013,* vol. 8, p. 14, 2013.

[2] C. Chen, J. Zhang, Y. Xiang and W. Zhou, "Spammers Are Becoming ‘Smarter’ on Twitter," *https://ieeexplore.ieee.org/document/7436683,* vol. 18, no. 2, pp. 66 - 70, 2016.

[3] H. Shen and X. Liu, "Detecting Spammers on Twitter Based on Content and Social Interaction," *2015 International Conference on Network and Information Systems for Computers,* vol. V, p. 5, 2015.

[4] N. eshraqi, M. Jalali and M. H. Moattar, "Detecting Spam Tweets In Twitter Using a Data Stream Clustering Algorithm," *Second International Congress on Technology, Communication and Knowledge (ICTCK 2015) November, 11-12, 201,* p. 5, 2015.

[5] S. J. Soman, "A survey on behaviors exhibited by spammers in popular social media networks," *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT),* 2016.

[6] M. Mateen, M. A. Iqbal, M. Aleem and M. A. Islam, "A hybrid approach for spam detection for Twitter," *14th International Bhurban Conference on Applied Sciences and Technology (IBCAST),* pp. 466-471, 2017.

[7] K. Lee, J. Caverlee and S. Webb, "Uncovering Social Spammers: Social Honeypots +Machine Learning," *ACM SIGIR Conference (SIGIR),* p. 8, 2010.

[8] G. Stringhini, S. Barbara, C. Kruegel and a. G. Vigna, "Detecting Spammers On Social Networks," *Annual Computer Security Applications Conference (ACSAC’10),* 2010.

[9] "Twitter Policies," Twitter, [Online]. Available: https://help.twitter.com/en/using-twitter/twitter-follow-limit.

[10] A. H. Wang, "Don't follow me: Spam detection in twitter. in Security and Cryptography (SECRYPT)," *Proceedings of the 2010 International Conference on. 2010. IEEE,* 2010.

[11] C. Yang, R. Harkreader, J. Zhang, S. Shin and G. Gu, "Analyzing Spammers’ Social Networks for Fun and Profit," *ACM New York, NY, USA ©2012,* pp. 71-80, 2012.

[12] "Local Clustering Coefficient.," [Online]. Available: http://wikipedia.org/wiki/Clustering_ coefficient#Local_clustering_coefficienty.

[13] "Betweenness Centrality," [Online]. Available: http://en.wikipedia.org/wiki/Centrality.

[14] F. Benevenuto, G. Magno, T. Rodrigues and V. Almeida, "Detecting Spammers on Twitter," *Electronic messaging, Anti-Abuse and Spam Confference (CEAS),* 2010.

[15] E. Lozano, J. Cedeño, G. Castillo, F. Layedra, H. Lasso and C. Vaca, "Requiem for online harassers: Identifying racism from political tweets," *2017 Fourth International Conference on eDemocracy & eGovernment (ICEDEG),* 2017.

[16] B. Alghamdi, J. Watson and Y. Xu, "Toward Detecting Malicious Links in Online Social Networks through User Behavior," *2016 IEEE/WIC/ACM International Conference on Web Intelligence Workshops (WIW),* 2016.

[17] I.-A. Bara, C. J. Fung and T. Dinh, "Enhancing Twitter spam accounts discovery using cross-account pattern mining," *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM),* 2015.

[18] A. M. Ghate and L. G. Malik, "Survey on designing framework for analyzing twitter spammers using forensic method," *2015 International Conference on Pervasive Computing (ICPC),* 2015.

[19] F. Fathaliani and M. Bouguessa, "A model-based approach for identifying spammers in social networks," *2015 IEEE International Conference on Data Science and Advanced Analytics (DSAA),* 2015.

[20] C. Chen, J. Zhang, X. Chen, Y. Xiang and W. Zhou, "6 million spam tweets: A large ground truth for timely Twitter spam detection," *2015 IEEE International Conference on Communications (ICC),* 2015.

[21] J. Oliver, P. Pajares, C. Ke, C. Chen and Y. Xiang, "An In-Depth Analysis of Abuse on Twitter," 2014.

[22] M.-W. C. K. L. K. T. Jacob Devlin, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," 2019.

[23] Chi Sun, Xipeng Qiu∗, Yige Xu, Xuanjing Huang, "How to Fine-Tune BERT for Text Classification?"

[24] Priya Dwivedi, "Real vs Fake Tweet Detection using a BERT Transformer Model in few lines of code", https://becominghuman.ai/real-vs-fake-tweet-detection-using-a-bert-transformer-model-in-few-lines-of-code-ccc33ecb1a2

[25] Google-Research, "BERT", https://github.com/google-research/bert

[26] Wikipedia, "Levenshtein Distance", https://en.wikipedia.org/wiki/Levenshtein_distance

[27] Automatically Follow Back. http://autofollowback.com

[28] Calculate Twitter Reputation. http://www.thekirankumar.com/blog/tag/calculate-twitter-reputation/.

[29] Capture HPC. https://projects.honeynet.org/capture-hpc

[30] Google Safe Browsing API. http://code.google.com/apis/safebrowsing/

[31] KOOBFACE: Inside a Crimeware Network. http://www.infowar-monitor.net/reports/iwm-koobface.pdf

[32] Lady Gaga Falls Prey to Rogue Twitter Attack. http://mashable.com/2011/04/28/lady-gaga-twitter-attack/

[33] Purchase Twitter Friends. http://www.purchasetwitterfriends.com/

[34] The Twitter Rules. http://help.twitter.com/entries/18311-the-twitter-rules

[35] Twitter accounts spreading malicious code. http://www.net-security.org/malware_news.php?id=1554

[36] Twitter-based Botnet Command Channel. http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/

[37] Twitter Streaming API. https://dev.twitter.com/docs/streaming-api

[38] Twitter vulnerability allows cyber criminals to spread spam. http://www.one.com/en/web-hosting-news/website/twitter-vulnerability-allows-/cyber-criminals-to-spread-spam-links\$800076628.htm

[39] Twitter’s Following Limits. http://support.twitter.com/groups/32-something-s-not-working/topics/117-following-problems/articles/66885-i-can-t-follow-people-follow-limits

[40] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman. SybilGuard: Defending Against Sybil Attacks via Social Networks. In Proceedings of ACM SIGCOMM Conference, 2006

[41] T. Wang, Y. Chen, Z. Zhang, P. Sun, B. Deng, and X. Li. Unbiased Sampling in Directed Social Graph. In ACM Special Interest Group on Data Communication, (SIGCOMM’10), 2010

[42] F. Benevenuto, T. Rodrigues, V. Almeida, J. Almeida, C. Zhang, and K. Ross. Identifying Video Spammers in Online Social Networks. In Int’l Workshop on Adversarial Information Retrieval on the Web (AirWeb’08), 2008

[43] C. Castillo, M. Mendoza, and B. Poblete. Information Credibility on Twitter. In International World Wide Web Conference, (WWW’11), 2011

[44] D. Pelleg and A. Moore. X-Means: Extending K-means with Efficient Estimation. In International Conference on Machine Learning, 2000

[45] G. Salton and C. Buckley. Term-weighting approaches in automatic text retrieval. In Information Processing & Management, 1998

[46] H. Kwak, C. Lee, H. Park, and S. Moon. What is Twitter, a Social Network or a News Media? In Int’l World Wide Web (WWW ’10), 2010

[47] J. Kleinberg. Authoritative sources in a hyperlinked environment. In Journal of the ACM, Vol.46, No. 5, pp. 604-632, 1999

[48] F. Benevenuto, G. Magno, T. Rodrigues, and V. Almeida. Detecting Spammers on Twitter. In Collaboration, Electronic messaging, Anti-Abuse and Spam Conference (CEAS), 2010

[49] Alexa top 500 global sites. http://www.alexa.com/topsites

[50] Compete site comparison. http://siteanalytics.compete.com/facebook.com+myspace.com+twitter.com/

[51] Harris Interactive Public Relations Research. A study of social networks scams. 2008

[52] S. Webb, J. Caverlee, , and C.Pu. Social honeypots: Making friends with a spammer near you. In Conference on Email and Anti-Spam (CEAS 2008), 2008

[53] Honeypots. http://en.wikipedia.org/wiki/Honeypot_computing

[54] The recaptcha project. http://recaptcha.net/

[55] J. Baltazar, J. Costoya, and R. Flores. Koobface: The largest web 2.0 botnet explained. 2009

[56] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All your contacts are belong to us: Automated identity
theft attacks on social networks. In World Wide Web Conference, 2009

[57] G. Brown, T. Howe, M. Ihbe, A. Prakash, and K. Borders. Social networks and context-aware spam.
In ACM Conference on Supportive Cooperative Work, 2008

[58] T.N. Jagatic, N.A. Johnson, M. Jakobsson, and T.N. Jagatif. Social phishing. Comm. ACM, 50(10):94–100, 2007

[59] Harris Interactive Public Relations Research. A study of social networks scams. 2008

[60] D. Aha, D. Kibler, “Instance-based Learning Algorithms”, Machine Learning, Vol 6, pp 37-66