Sources Acquired so far:

1. "A basic introduction to neural networks,". [Online]. Available: <http://pages.cs.wisc.edu/~bolo/shipyard/neural/local.html> . Accessed: Nov. 8, 2016.
2. A. L. Blum and P. Langley, "Selection of relevant features and examples in machine learning," *Artificial Intelligence*, vol. 97, no. 1-2, pp. 245–271, 1997. [Online]. Available: <http://ac.els-cdn.com/S0004370297000635/1-s2.0-S0004370297000635-main.pdf?_tid=73adbcce-9e09-11e6-b4bf-00000aab0f01&acdnat=1477767591_ae57e9d5edfa313dd20eae51311b5337> . Accessed: Oct. 29, 2016.
3. A. M. Sasse, "Computer security: Anatomy of a usability disaster, and a plan for recovery,". [Online]. Available: <http://discovery.ucl.ac.uk/20347/2/hcisec-workshop-sasse.pdf> . Accessed: Nov. 8, 2016.
4. B. Selman, R. Brooks, T. Dean, E. Horvitz, T. Mitchel, and N. Nilsso, "Challenge problems for artificial intelligence," in Microsoft Research, 1996. [Online]. Available: <http://research.microsoft.com/en-us/um/people/horvitz/seltext.htm> . Accessed: Nov. 8, 2016.
5. C. Landwehr "Cybersecurity and artificial intelligence,". [Online]. Available: <https://www.researchgate.net/profile/Carl_Landwehr/publication/220496586_Cybersecurity_and_Artificial_Intelligence_From_Fixing_the_Plumbing_to_Smart_Water/links/559abc4108ae99aa62ce2288.pdf> . Accessed: Oct. 29, 2016.
6. D. E. Goldberg and J. H. Holland, "GUEST EDITORIAL - Genetic Algorithms and Machine Learning," *Machine Learning*, vol. 3, no. 2/3, pp. 95–99, 1988.
7. D. Martin, O. Vanni, and A. E. Weaver, "Rapid7 aims to stop IoT devices from becoming pawns in future Cyber attacks," BostInno, 2016. [Online]. Available: <http://bostinno.streetwise.co/2016/11/01/rapid7-announces-new-practice-to-secure-the-internet-of-things/> . Accessed: Nov. 8, 2016.
8. E. Hodo *et al.*, "Threat analysis of IoT networks using artificial neural network intrusion detection system," 2016. [Online]. Available: <https://pure.strath.ac.uk/portal/files/53939530/Hodo_etal_ISNCC_2016_Threat_analysis_of_IoT_networks_using_artificial_neural.pdf> . Accessed: Nov. 8, 2016.
9. F. Xia, L. T. Yang, L. Wang, and A. Vinel, "Internet of things," *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1101–1102, 2012. [Online]. Available: <https://www.homeworkmarket.com/sites/default/files/q5/04/07/danainfo.acppwiszgmk2n0u279qu76contentserver.pdf> . Accessed: Nov. 8, 2016.
10. G. K. Tak and T. Shashikala, "Query based approach towards Spam attacks using artificial neural network," *International Journal of Artificial Intelligence & Applications*, vol. 1, no. 4, pp. 82–99, 2010. [Online]. Available: <http://s3.amazonaws.com/academia.edu.documents/37881663/1010ijaia07.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1477773392&Signature=92BrYqGhec3w1Bvm6m6UnvGhNXU%3D&response-content-disposition=inline%3B%20filename%3DQuery_Based_Approach_Towards_Spam_Attack.pdf>. Accessed: Oct. 29, 2016.
11. Gartner, "Gartner Press Release - IoT," 2015. [Online]. Available: <http://www.gartner.com/newsroom/id/3165317>. Accessed: Nov. 8, 2016
12. H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013. [Online]. Available: <http://dl-maghaleh.ir/wp-content/uploads/2016/03/order-z-1426675381-750.pdf>. Accessed: Nov. 8, 2016.
13. I. Goodfellow, Y. Bengio, and A. Courville, "Deep learning," GoodFellow, 2016. [Online]. Available: <http://www.deeplearningbook.org/front_matter.pdf>. Accessed: Oct. 29, 2016.
14. J. Cannady, "Artificial neural networks for misuse detection," 2005. [Online]. Available: <http://pld.cs.luc.edu/courses/intrusion/fall05/cannady.artificial_neural_networks_for_misuse_detection.pdf> . Accessed: Nov. 8, 2016.
15. J. F. Rank, "Artiicial intelligence and intrusion detection: Current and future directions," Jun. 1994. [Online]. Available: <http://home.eng.iastate.edu/~guan/course/backup/CprE-592-YG-Fall-2002/paper/intrusion/ai-id.pdf>. Accessed: Nov. 8, 2016.
16. L. Atzori, A. Iera, and G. Morabito, "The Internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010. [Online]. Available: <http://www.ghiasian.com/fa/wp-content/uploads/2013/02/IoT-A-survey.pdf>. Accessed: Nov. 8, 2016.
17. M. Botha, V. Solms, K. Perry, E. Loubser, G. Yamoyany, and E. Technikon, "The utilization of artificial intelligence in a hybrid intrusion detection system," 2002. [Online]. Available: <http://neuro.bstu.by/ai/To-dom/My_research/Papers-0/For-research/D-mining/Anomaly-D/Intrusion-detection/20acm.pdf>. Accessed: Oct. 29, 2016.
18. M. Embrechts, A. Bivens, C. Palagiri, R. Smith, and B. Szymanski, "Network-Based Intrusion Detection Using Neural Networks," Dec. 2002. [Online]. Available: <https://www.researchgate.net/profile/Boleslaw_Szymanski/publication/2548475_Network-Based_Intrusion_Detection_Using_Neural/links/00b7d51f958a6b5c18000000.pdf>. Accessed: Nov. 8, 2016.
19. M. Moradi and M. Zulkernine, "A Neural Network Based System for Intrusion Detection and Classification of Attacks," 2004. [Online]. Available: <http://research.cs.queensu.ca/~moradi/148-04-MM-MZ.pdf> . Accessed: Nov. 8, 2016.
20. R. A. Kemmerer and G. Vigna, "Intrusion Detection: A Brief History and Overview," *Security & Privacy*, pp. 27–30, 2002. [Online]. Available: <http://www.ismlab.usf.edu/isec/files/kemmerer2002.pdf> . Accessed: Nov. 8, 2016.
21. S. Mukkamala, G. Janoski, A. Sung “Intrusion Detection: Support Vector Machines and Neural Networks” Feb 2002 [Online]: Available: <https://www.researchgate.net/publication/3950039_Intrusion_detection_using_neural_networks_and_support_vector_machines>. Accessed Nov 8, 2016
22. S. Worldwide, "FREE response time viewer for Wireshark," 2003. [Online]. Available: <http://www.solarwinds.com/free-tools/response-time-viewer-for-wireshark?&CMP=KNC-TAD-GGL-SW_NE_UK_PP_CPC_FT_EN_PROD_DWA-FXNET-X_X_X_X-X&kwid=b08GFXYg&gclid=CICsu6TJmdACFUk8GwodnMsAMQ>. Accessed: Nov. 8, 2016.
23. L.Dhanabal ,Dr. S.P. Shantharajah, “A Study on NSL - KDD Dataset for Intrusion Detection System Based on Classification Algorithms” 2015 [Online]. Available: <http://www.ijarcce.com/upload/2015/june-15/IJARCCE%2096.pdf> Accessed Nov 18 2015.
24. L.Xu “Android Malware Classification using Parallelized Machine Learning Methods” 2016 [Online] Available: <https://docs.google.com/viewer?url=http://udspace.udel.edu/bitstream/handle/19716/19893/2016_XuLifan_PhD.pdf> Accessed
25. A. Silva “Log File Regular Expression Pattern Matching and Capture with GPUS” 2016 [Online] Available: <https://docs.google.com/viewer?url=http://hgpu.org/papers/16842_20161221221507.pdf> Accessed
26. A. Drozdov “Batched Shift Reduce Parsing with Lists of Vectors on CUDA” 2016 [Online] Available: <https://docs.google.com/viewer?url=http://mrdrozdov.com/papers/batched-spinn.pdf> Accessed