REFERENCES

Abayomi-Alli;, O. O., Onashoga;, S. A., Sodiya;, A. S., & Ojo, D. A. 2015. "A Critical Analysis of Existing SMS Spam Filtering Approaches". In International Conference on Applied Information Technology (pp. 211–220).

Abbott, D. 2013. Introduction to Text Mining.

Abdelhaq, M., Alsaqour, R., & Abdelhaq, S. 2015. "Securing Mobile Ad Hoc Networks Using Danger Theory-Based Artificial Immune Algorithm". PLoS ONE, 10(5), 1–9. https://doi.org/10.1371/journal.pone.0120715

Abdelhaq, M., Alsaqour, R., Ismail, M., & Abdelhaq, S. 2015. "Dendritic Cell Fuzzy Logic Algorithm over Mobile Ad Hoc Networks". In International Conference on Intelligent Systems, Modelling and Simulation (pp. 64–69). https://doi.org/10.1109/ISMS.2015.36

Abdulhamid, S. M., Abd Latiff, M. S., Chiroma, H., Osho, O., Abdul-Salaam, G., Abu Bakar, A. I., & Herawan, T. 2017. "A Review on Mobile SMS Spam Filtering Techniques". IEEE Access, 1–21. https://doi.org/10.1109/ACCESS.2017.2666785

Adewole, K. S., Anuar, N. B., & Kamsin, A. 2016. "Ensemble Based Streaming Framework for Spam Detection and Risk Assessment in Microblogging Social Networks". In International Conference on Computer Science and Computational Mathematics (ICCSCM).

Aickelin, U., Bentley, P., Cayzer, S., Jungwon, K., & McLeod, J. 2003. "Danger Theory: The Link Between AIS and IDS?" In International Conference on Artificial Immune Systems (ICARIS) (pp. 147–155). https://doi.org/10.1007/b12020

Aickelin, U., & Greensmith, J. 2007. "Sensing Danger: Innate Immunology for Intrusion Detection". Information Security Technical Report (Vol. 12). https://doi.org/10.1016/j.istr.2007.10.003

Al-Hassan, A. A., & El-Alfy, E.-S. M. 2015. "Dendritic Cell Algorithm for Mobile Phone Spam Filtering". In International Conference on Ambient Systems, Networks and Technologies (ANT) (Vol. 52, pp. 244–251).

Al-Talib, G. A., & Hassan, H. S. 2013. "A Study on Analysis of SMS Classification Using TF-IDF Weighting". International Journal of Computer Networks and Communications Security, 1(5), 189–194. Retrieved from http://www.ijcncs.org/published/volume1/issue5/p3_1-5.pdf

Almeida, T. A., & Hidalgo, J. M. G. 2012. "UCI Machine Learning Repository". Retrieved March 3, 2014, from http://archive.ics.uci.edu/ml/datasets/SMS+Spam+Collection#

Almeida, T. A., Hidalgo, J. M. G., & Silva, T. P. 2012. "Towards SMS Spam Filtering : Results under a New Dataset". International Journal of Information Security Sceince, 2(1), 1–18.

Almeida, T. A., Hidalgo, J. M. G., & Yamakami, A. 2011. "Contributions to the Study of SMS Spam Filtering: New Collection and Results". In Proceedings of the 11th ACM Symposium on Document Engineering - DocEng '11 (pp. 259–262).

Almeida, T. A., Silva, T. P., Santos, I., & Hidalgo, J. M. G. 2016. "Text Normalization and Semantic Indexing to Enhance Instant Messaging and SMS Spam Filtering". Knowledge-Based Systems, 108, 1–32. https://doi.org/10.1016/j.knosys.2016.05.001

Alotaibi, S., Furnell, S., & Clarke, N. 2016. "A Novel Taxonomy for Mobile Applications Data". International Journal of Cyber-Security and Digital Forensics (IJCSDF), 5(3), 115–121.

Anandita, S., Rosmansyah, Y., Dabarsyah, B., & Choi, J. U. 2015. "Implementation of Dendritic Cell Algorithm as an Anomaly Detection Method for Port Scanning Attack". In International Conference on Information Technology Systems and Innovation (ICITSI) (pp. 1–6). https://doi.org/10.1109/ICITSI.2015.7437688

Anwar, S., Zain, J. M., Zolkipli, M. F., Inayat, Z., Khan, S., Anthony, B., & Chang, V. 2017. "From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions". Algorithms, 10(2), 1–24. https://doi.org/10.3390/a10020039

Arago, M. V. C., Frigieri, E. P., Ynoguti, C. A., & Paiva, A. P. 2016. "Factorial Design Analysis Applied to The Performance of SMS Anti-Spam Filtering Systems". Expert Systems with Applications, 64(August), 589–604. https://doi.org/10.1016/j.eswa.2016.08.038

Atila, E., & Jones, J. C. 2014. "The Engineering Design Process". Retrieved February 21, 2017, from http://www.sciencebuddies.org/engineering-design-process/engineering-design-process-steps.shtml#theengineeringdesignprocess

Bali, M., & Gore, D. 2015. "A Survey on Text Classification with Different Types of Classification Methods". International Journal of Innovative Research in Computer and Communication Engineering, 3(5), 4888–4894. https://doi.org/10.15680/ijircce.2015.0305174

Balubaid, M. A., Manzoor, U., Zafar, B., Qureshi, A., & Ghani, N. 2015. "Ontology Based SMS Controller for Smart Phones". International Journal of Advanced Computer Science and Applications (IJACSA), 6(1), 133–139.

Belém, D., & Duarte-Figuriredo, F. 2011. "Content Filtering for SMS Systems Based on Bayesian Classifier and Word Grouping". IEEE, 1–7.

Blank, R. M., & Gallagher, P. D. 2012. "Guide for Conducting Risk Assessments". National Institute of Standards and Technology (NIST).

Brownlee, J. 2011. "Dendritic Cell Algorithm". In Clever Algorithms: Nature Inspired Programming Recipes (pp. 312–318). Creative Commons.

Brownlee, J. 2013. "A Tour of Machine Learning Algorithms". Retrieved December 29, 2014, from http://machinelearningmastery.com/a-tour-of-machine-learning-algorithms/

Bujang, Y., & Hussin, H. 2012. "Investigating Email Users Behavior against Spam: A Proposed Theoretical Framework". Journal of Internet and E-Business Studies, 1–53. https://doi.org/10.5171/2012.936368

Canada, G. of. 2012. "Worried It's Spam? 5 Things to Look For". Canada's Law on Spam and Other Electronis Threats. Retrieved from http://spectrumdirect.ic.gc.ca/eic/site/030.nsf/vwapj/infographicen.pdf/$file/infographicen.pdf

Cao, L., Nie, G., & Liu, P. 2011. "Ontology-based Spam Detection Filtering System". In International Conference on Business Management and Electronic Information (BMEI) (pp. 282–284). https://doi.org/10.1109/ICBMEI.2011.5920449

Chelly, Z., & Elouedi, Z. 2015. "A Survey of The Dendritic Cell Algorithm". Knowledge and Information Systems. https://doi.org/10.1007/s10115-015-0891-y

Chen, T., & Kan, M. Y. 2013. "Creating a Live, Public Short Message Service Corpus: The NUS SMS Corpus". Language Resources and Evaluation, 47(2), 299–335. https://doi.org/10.1007/s10579-012-9197-9

Choudhary, N., & Jain, A. K. 2017. "Towards Filtering of SMS Spam Messages Using Machine Learning Based Technique". In International Conference on Advanced Informatics for Computing Research (ICAICR) (Vol. 712, pp. 18–30). https://doi.org/10.1007/978-981-10-5780-9

Cloudmark. 2011. "SMS Spam and Mobile Messaging Attacks- Introduction, Trends and Examples". Retrieved from www.gsmworls.com/spamreportingservice
Cloudmark. 2013. 2013 Global Messaging Threat Report.

Colwill, C. 2009. "Human Factors in Information Security: The Insider Threat - Who Can You Trust These Days?" Information Security Technical Report, 14(4), 186–196. https://doi.org/10.1016/j.istr.2010.04.004

ConstantContact. 2010. "Understanding Your Spam Risk". Retrieved from www.constantcontact.com

Cormack, G. V, Hidalgo, J. M. G., & Sánz, E. P. 2007. "Feature Engineering for Mobile (SMS) Spam Filtering". In SIGIR (pp. 1–2).

Danziger, M., & de Lima Neto, F. B. 2011. "A Hybrid Approach for IEEE 802.11 Intrusion Detection based on AIS, MAS and Naïve Bayes". International Journal of Computer Information Systems and Industrial Management Applications, 3, 193–201. https://doi.org/10.1109/HIS.2010.5600083

David Emm. 2010. "Patching Human Vulnerabilities". Retrieved December 11, 2014, from http://securelist.com/analysis/publications/36287/patching-human-vulnerabilities/%0A

Delany, S. J., Buckley, M., & Greene, D. 2012. "SMS Spam Filtering: Methods and Data". Expert Systems with Applications, 01(10), 9899–9908.

Ding, L., Yu, F., & Yang, Z. 2013. "Survey of DCA for Abnormal Detection". Journal of Software, 8(8), 2087–2094. https://doi.org/10.4304/jsw.8.8.2087-2094

Eshmawi, A. 2015. "The Roving Proxy for SMS Spam and Phishing Detection". Southern Methodist University.

Ezpeleta, E., Garitano, I., Zurutuza, U., & Hidalgo, J. M. G. 2017. "Short Messages Spam Filtering Combining Personality Recognition and Sentiment Analysis". International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 25(December), 175–189. https://doi.org/10.1145/2934732.2934742

Fallows, D. 2011. Internet Users and Spam : What the Attitudes and Behavior of Internet Users can Tell Us About Fighting Spam.

Farrell, N. 2014. "China Arrests Mobile Spammers". Retrieved April 4, 2014, from http://fudzilla.com/news/34343-china-arrests-mobile-spammers

Fernandes, D. A. B., Freire, M. M., Fazendeiro, P. A. P., & Inácio, P. R. M. 2017. "Applications of Artificial Immune Systems to Computer Security: A survey". Journal of Information Security and Applications, 35, 138–159. https://doi.org/10.1016/j.jisa.2017.06.007

Figueredo, G. P., Siebers, P.-O., Aickelin, U., & Foan, S. 2012. "A Beginner's Guide to Systems Simulation in Immunology". In International Conference on Artificial Immune Systems (ICARIS) (pp. 57–71). https://doi.org/10.1007/978-3-642-33757-4

G.C.Tjhai, & S.M.Furnell. 2006. "Strengthening the Human Firewall". In P. S. Dowland & S. M. Furnell (Eds.), Advances in Networks, Computing and Communications 4 (pp. 222–230). Retrieved from https://www.secureworks.com/blog/bg-strengthening-the-human-firewall

Gabrielli, N., & Rigodanzo, M. 2011. An Artificial Immune System for Network Intrusion Detection on a Web Server: First Results.

Gansterer, W. N., & David, P. 2009. E-Mail Classification for Phishing Defense.

Garrido, J. M. 2012. Introduction to Elementary Computational Modeling-Essential Concepts, Principles and Problem Solving. CRC Press-Taylor & Francis Group.

Gasanova, T., Sergienko, R., Akhmedova, S., Semenkin, E., & Minker, W. 2014. "Opinion Mining and Topic Categorization with Novel Term Weighting". In Workshop on Computational Approaches to Subjectivity, Sentiment and Social Media Analysis (pp. 84–89). https://doi.org/10.3115/v1/W14-2615

Ge, Y., Liang, H., Chen, L., & Zhang, Q. 2015. "The Designation of Bio-Inspired Intrusion Detection System Model in Cloud Computing Based on Machine Learning". In International Conference on Automation, Mechanical Control and Computational Engineering (AMCCE) (pp. 1932–1937).

Goel, D., & Jain, A. K. 2017. "Mobile Phishing Attacks and Defence Mechanisms: State of Art and Open Research Challenges". Computers & Security, 1–44. https://doi.org/10.1016/j.cose.2017.12.006

Gonçalves, T., & Quaresma, P. 2005. "Evaluating Preprocessing Techniques in a Text Classification Problem". In Congresso da Sociedade Brasileira de Computacao (pp. 841–850). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.131.1271&rep=rep1&type=pdf

Greensmith, J. 2007. "The Dendritic Cell Algorithm". Thesis for the Degree of Doctor of Philosophy. University of Nottingham. Retrieved from http://ima.ac.uk/papers/greensmith_thesis.pdf

Greensmith, J., & Aickelin, U. 2008. The Deterministic Dendritic Cell Algorithm.

Greensmith, J., & Aickelin, U. 2009. "Artificial Dendritic Cells: Multi-faceted Perspectives". In Human-Centric Information Processing Through Granular Modelling (Vol. 182, pp. 375–395). https://doi.org/10.1007/978-3-540-92916-1_16

Greensmith, J., Aickelin, U., & Cayzer, S. 2010. Detecting Danger : The Dendritic Cell Algorithm.

Greensmith, J., Aickelin, U., & Tedesco, G. 2010. "Information Fusion for Anomaly Detection with The Dendritic Cell Algorithm". Information Fusion, 11(1), 21–34. https://doi.org/10.1016/j.inffus.2009.04.006

Greensmith, J., Aickelin, U., & Twycross, J. 2009. Articulation and Clarification of the Dendritic Cell Algorithm.

Greensmith, J., Whitbrook, A., & Aickelin, U. 2010a. "Artificial Immune Systems". Immunology, 1–29. Retrieved from http://arxiv.org/abs/1006.4949

Greensmith, J., Whitbrook, A., & Aickelin, U. 2010b. "Artificial Immune Systems". Immunology, 1–29.

Griesel, M., & Fourie, W. 2012. "Choosing the Best Classifier for The Job: Mobile Filtering for The South African Context". Computational Linguistics in the Netherlands Journal, 2(12), 23–33.

Gu, F., Greensmith, J., & Aickelin, U. 2008. "Further Exploration of the Dendritic Cell Algorithm: Antigen Multiplier and Time Windows". In International Conference on Artificial Immune Systems (pp. 142–153).

Gu, F., Greensmith, J., & Aicklein, U. 2011. "Biologically Inspired Networking and Sensing: Algorithms and Architectures. The Dendritic Cell Algorithm for Intrusion Detection". Bio-Inspired Communications and Networking, IGI Global, (January), 84–102. Retrieved from https://ssrn.com/abstract=2824971

Gu, F., Greensmith, J., Oates, R., & Aickelin, U. 2010. PCA 4 DCA : The Application of Principal Component Analysis to The Dendritic Cell Algorithm.

Haritha, K. H., Kumar, R. S., & Krishnan, M. S. 2017. "An Analytical Exploration on SMS Spam & User Retort". International Journal of Pure and Applied Mathematics, 114(11), 147–156. Retrieved from http://www.ijpam.eu

Hidalgo, J. M. G., Bringas, G. C., & Sánz, E. P. 2003. Content Based SMS Spam Filtering.

Hofmeyr, S. A., & Forrest, S. 2000. "Architecture for an Artificial Immune System". Journal of Evolutionary Computation, 8(4), 443–473. https://doi.org/10.1162/106365600568257
Humphreys, E. 2010. "Information Security Risk Management Handbook for ISO/IEC 27001". https://doi.org/10.3403/9780580607455

Imenda, S. 2014. "Is There a Conceptual Difference Between Theoretical and Conceptual Frameworks?" Journal of Social Sciences, 38(2), 185–195. https://doi.org/10.1111/j.1471-0528.2006.00853.x

Iyer, K. B. P., & Shanthi, V. 2013. "Privacy Preferences for Geo-Calendar Based SMS Using Intelligent Text Configurator". International Journal of Computer and Communication Engineering, 2(1), 82–85.

Jain, A. K., & Gupta, B. B. 2018. "Rule-based Framework for Detection of Smishing Messages in Mobile Environment". In International Conference on Smart Computing and Communications (ICSCC) (Vol. 125, pp. 617–623). Elsevier B.V. https://doi.org/10.1016/j.procs.2017.12.079

Japkowicz, N., & Shah, M. 2011. "Evaluating Learning Algorithms: A Classification Perspective". Cambridge University Press. https://doi.org/10.1017/CBO9780511921803

Jayakumar, N. K., & Phippen, A. D. 2006. "Evaluating the Perceptions of People towards Online Security". In P. S. Dowland & S. M. Furnell (Eds.), Advances in Networks, Computing and Communications 4 (pp. 199–204).

Johnson, M. E., & Moag, J. 2011. "Human Behavior and Security Culture: Managing Information Risk through a Better Understanding of Human Culture". CISO Information Security Workshop.

Junaid, M. B., & Farooq, M. 2011. "Using Evolutionary Learning Classifiers to Do Mobile Spam (SMS) Filtering". In Genetic and Evolutionary Computation Conference (GECCO) (pp. 1795–1801).

Karami, A., & Zhou, L. 2014a. "Exploiting Latent Content-based Features for the Detection of Static SMS Spams". In Proceedings of the American Society for Information Science and Technology (pp. 1–4). https://doi.org/10.1002/meet.2014.14505101157

Karami, A., & Zhou, L. 2014b. "Improving Static SMS Spam Detection by Using New Content-based Features". In Americas Conference on Information Systems (pp. 1–9).

Khemapatapan, C. 2010. "Thai-English Spam SMS Filtering". In Asia Pacific Conference on Communications (APCC) (pp. 226–230).

Kim, J., Bentley, P. J., Aickelin, U., Greensmith, J., Tedesco, G., & Twycross, J. 2007. "Immune System Approaches to Intrusion Detection - A Review". Natural Computing, 6(4), 413–466. https://doi.org/10.1007/s11047-006-9026-4

Kim, J., Bentley, P., Wallenta, C., Ahmed, M., & Hailes, S. 2006. "Danger is Ubiquitous: Detecting Malicious Activities in Sensor Networks Using the Dendritic Cell Algorithm". In International Conference on Artificial Immune Systems (ICARIS) (Vol. 4163, pp. 390–403). https://doi.org/10.1007/11823940_30

Kim, J., Greensmith, J., Twycross, J., & Aickelin, U. 2010. "Malicious Code Execution Detection and Response Immune System Inspired by The Danger Theory". Retrieved from http://arxiv.org/ abs/1003.4142

Kim, S.-E., Jo, J.-T., & Choi, S.-H. 2015. "SMS Spam Filterinig using Keyword Frequency Ratio". International Journal of Security and Its Applications, 9(1), 329–336. https://doi.org/10.14257/ijsia.2015.9.1.31

Knipe, L. 2017. "Bulk SMS – The Superhero Without a Cape". Retrieved February 27, 2017, from http://thehub.smsglobal.com/bulk-sms-the-superhero-without-a-cape

Kontostathis, A., Edwards, L., & Leatherman, A. 2010. "Text Mining and Cyber Crime". In Text Mining-Applicatrons and Theory (pp. 149–162). John Wiley & Sons. https://doi.org/10.1002/9780470689646

Kumar, K. 2015. "Biological Comparative Analysis of Dendritic Cell Algorithm and Immune Networks Algorithm in Neural Network". International Journal of Computer Science and Engineering, (4), 62–65.

Ladjana, J. 2018. Duit tabung 28 tahun "hangus." Harian Metro, pp. 1–2.

Lark, J. 2015. "ISO 31000 Risk Management". https://doi.org/10.1093/rpd/ncr142

Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I., & Zhang, J. 2012. "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing". In Conference on Ubiquitous Computing (UbiComp) (pp. 1–10). https://doi.org/10.1145/2370216.2370290

Lintean, M., Moldovan, C., Rus, V., & McNamara, D. 2010. "The Role of Local and Global Weighting in Assessing the Semantic Similarity of Texts Using Latent Semantic Analysis". In International Florida Artificial Intelligence Research Society Conference (FLAIRS) (pp. 235–240). Retrieved from http://www.aaai.org/ocs/index.php/FLAIRS/2010/paper/viewFile/1310/1746

Lokesh, M. R., & Kumaraswamy, Y. S. 2015. "State AwarenessTtowards Resiliency in Cyber-Physical System: A Modified Danger Theory Based Deterministic Dendritic Cell Algorithm Approach". In International Conference on Computer Graphics, Vision and Information Security (CGVIS) (pp. 201–208). https://doi.org/10.1109/CGVIS.2015.7449922

Lota, L. N., & Hossain, B. M. M. 2017. "A Systematic Literature Review on SMS Spam Detection Techniques". International Journal of Information Technology and Computer Science, 9(7), 42–50. https://doi.org/10.5815/ijitcs.2017.07.05

Luko, S. N. 2013. "Reviews of Standards and Related Material-Risk Management Terminology". Quality Engineering, 25(4), 451–454. https://doi.org/10.1080/08982112.2013.814508

M.El-Alfy, E.-S., & Al-Hasan, A. A. 2014. "A Novel Bio-Inspired Predictive Model for Spam Filtering Based on Dendritic Cell Algorithm". IEEE.

M.El-Alfy, E.-S., & Alhasan, A. A. 2016. "Spam Filtering Framework for Multimodal Mobile Communication Based on Dendritic Cell Algorithm". In Future Generation Computer Systems (pp. 1–40). Elsevier B.V. https://doi.org/10.1016/j.future.2016.02.018

M, A. C., Uma, S., & Kumar, M. M. 2014. "Detaining and Avoiding Mobile Virus Propagation by Considering Human Behavior". International Journal of Advanced Computer Technology, 3(3), 619–623.

Mahmoud, T. M., El Nashar, A. I., Abd-El-Hafeez, T., & Khairy, M. 2014. "An Efficient Three-phase Email Spam Filtering Technique". British Journal of Mathematics & Computer Science, 4(9), 1184–1201.

Mahmoud, T. M., & Mahfouz, A. M. 2012a. "SMS Spam Filtering Technique Based on Artificial Immune System". International Journal of Computer Science Issues (IJCSI), 9(2), 589–597.

Mahmoud, T. M., & Mahfouz, A. M. 2012b. "SMS Spam Filtering Technique Based on Artificial Immune System". International Journal of Computer Science Issues (IJCSI), 9(2), 589–597.

Malcolm, R. 2016. "Mobile Messaging Report 2016". Retrieved from www.mobileecosystemforum.com

Marzuki, E. 2013. "Linguistic Features in SMS Apologies by Malay Native Speakers". Journal of Language Studies, 13(3), 179–192.

Mathew, K., & Issac, B. 2011. "Intelligent Spam Classification for Mobile Text Message". In International Conference on Computer Science and Network Technology (pp. 101–105).

Matzinger, P. 1994. "Tolerance, Danger and The Extended Family". Annual Reviews Immunology, 12, 991–1045.

Matzinger, P. 1998. An Innate Sense of Danger. Immunology, 10, 399–415.

Matzinger, P. 2002, April 12. "The Danger Model: A Renewed Sense of Self". Science (New York, N.Y.), 296(5566), 301–305. https://doi.org/10.1126/science.1071059

Matzinger, P. 2007. "Friendly and Dangerous Signals: Is The Tissue in Control?" Nature Immunology, 8(1), 11–13. https://doi.org/10.1038/ni0107-11

Mihai-Gabriel, E. I., & Patriciu, V.-V. 2014. "Biologically Inspired Risk Assessment in Cyber Security Using Neural Networks". In International Conference on Communications (COMM) (pp. 1–4). https://doi.org/10.1109/ICComm.2014.6866746

Mitnick, K. D., & Simon, W. L. 2003. "The Art of Deception: Controlling the Human Element of Security. Kineticstomp". https://doi.org/0471237124

Mohamad Mohsin, M. F., Hamdan, A. R., & Bakar, A. A. 2015. "An Evaluation of Feature Selection Technique for Dendrite Cell Algorithm". In International Conference on IT Convergence and Security (ICITCS) (pp. 1–5). https://doi.org/10.1109/ICITCS.2014.7021732

Mohd Foozy, C. F., Ahmad, R., & Abdollah, M. A. F. 2014. "A Framework for SMS Spam and Phishing Detection in Malay Language: A Case Study". International Review on Computers and Software (IRECOS), 9(7), 1248–1254.

Mohsin Mohamad, M. F., Bakar, A. A., & Hamdan, A. R. 2017. "An Adaptive Anomaly Threshold in Artificial Dendrite Cell Algorithm". In International Conference of Computing and Informatics (ICOCI) (pp. 250–255).

Monte F. Hancock, J. 2012. "Practical Data Mining (1st ed.)". Taylor & Francis Group. Retrieved from http://www.celestech.com/PracticalDataMining

Mosquera, A., Aouad, L., Grzonkowski, S., & Morss, D. 2014. "On Detecting Messaging Abuse in Short Text Messages Using Linguistic and Behavioral Patterns". Social Media Intelligence, 1–10. Retrieved from http://arxiv.org/abs/1408.3934

Mujtaba, G., & Yasin, M. 2014. "SMS Spam Detection Using Simple Message Content Features". Journal of Basic Applied Scientific Research, 4(4), 275–279.

Musselle, C. J. 2010. "Insights Into The Antigen Sampling Component of The Dendritic Cell Algorithm". In International Conference on Artificial Immune Systems (ICARIS) (pp. 88–101). https://doi.org/10.1007/978-3-642-14547-6_8

n.a. 2012a. "Combating Spam: Policy, Technical and Industry Approaches. Internet Society 20 Years". Retrieved from http://www.internetsociety.org/doc/combating-spam-policy-technical-and-industry-approaches

n.a. 2012b. "Differences Between In Vitro, In Vivo, and In Silico Studies". https://doi.org/10.1371/journal.pcbi.1000423

n.a. 2012c. "Introducing PDCA". Retrieved March 9, 2017, from http://www.17799central.com/pdca.htm

n.a. 2013. "SMS spam more dangerous than email spam". Retrieved September 12, 2017, from https://www.cstl.com/Newsletter/October-2013/sms-spam.htm

n.a. 2014a. "The History of Spam". Retrieved from http://www.internetsociety.org/doc/history-spam

n.a. 2014b. "What is spam?" Retrieved from http://www.internetsociety.org/doc/what-spam

n.a. 2015. "MCMC Takes Legal Action Against Errant Content Providers". Retrieved November 16, 2015, from http://www.nst.com.my/news/2015/11/mcmc-takes-legal-action-against-errant-content-providers

n.a. 2016. "Muslihat Soalan Perangkap". Harian Metro.

n.a. 2017. "Penipuan Dalam Talian Meningkat". Bernama. Retrieved from http://www.hmetro.com.my/node/203993

Narayan, A., & Saxena, P. 2013. "The Curse of 140 Characters: Evaluating the Efficacy of SMS Spam Detection on Android". In Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM) (pp. 1–9). https://doi.org/10.1145/2516760.2516772

Natris, W. de. 2014. "Best Practice Forum on Regulation and Mitigation of Unsolicited Communications". Retrieved from https://www.intgovforum.org/cms/documents/best-practice-forums/regulation-and-mitigation-of-unwanted-communications/411-bpf-2014-outcome-document-regulation-and-mitigation-of-unsolicited-communications-spam/file

Nayak, A. S., Kanive, A. P., Chandavekar, N., & R, B. 2016. "Survey on Pre-Processing Techniques for Text Mining". International Journal Of Engineering And Computer Science, 5(6), 16875–16879. https://doi.org/10.18535/ijecs/v5i6.25

Nuruzzaman, M. T., Lee, C., & Choi, D. 2011. "Independent and Personal SMS Spam Filtering". In International Conference on Computer and Information Technology (pp. 429–435). https://doi.org/10.1109/CIT.2011.23

Oates, R., Kendall, G., & Garibaldi, J. M. 2008a. "Frequency Analysis for Dendritic Cell Population Tuning". Evolutionary Intelligence, 1(123), 145–157. https://doi.org/10.1007/s12065-008-0011-y

Oates, R., Kendall, G., & Garibaldi, J. M. 2008b. "The Limitations of Frequency Analysis for Dendritic Cell Population Modelling". Evolutionary Intelligence, 1(2), 145–157. https://doi.org/10.1007/s12065-008-0011-y

Oda, T. 2005. "A Spam-Detecting Artificial Immune System". Carleton University Ottawa, Canada.

Onanuga, P. 2017. "Language Use in Nigerian Spam SMSs: A Linguistic Stylistic Analysis". Language Matters-Studies in the Languages of Africa, 48(2), 91–116. https://doi.org/10.1080/10228195.2017.1337805

Ozarkar, P., & Patwardhan, M. 2013. "Efficient Spam Classification by Appropriate Feature Selection". Global Journal of Computer Science and Technology Software & Data Engineering, 13(5), 1–11.

Parimala, R., & Nallaswamy, R. 2012. "A Study on Analysis of SMS Classification Using Document Frequency Thresold". International Journal of Information Engineering and Electronic Business, 4(1), 44–50. https://doi.org/10.5815/ijieeb.2012.01.06

Patra, A., & Singh, D. 2013. "A Survey Report on Text Classification with Different Term Weighting Methods and Comparison Between Classification Algorithms". International Journal of Computer Applications, 75(7), 14–18.

Pelnekar, C. 2011. "Planning for and Implementing ISO 27001". ISACA Journal, 4(70), 1–8. Retrieved from http://www.isaca.org/Journal/Past-Issues/2011/Volume-4/Documents/jpdf11v4-Planning-for-and.pdf

Peng, L., & Ruchuan, W. 2015. "Research on Network Malicious Code Immune Based on Imbalanced Support Vector Machines". Chinese Journal of Electronics, 24(1), 181–186.

Pereira, G. 2011. Artificial Immune System Algorithm Based on Danger Theory.

PortioResearch. 2015. "SMS: The Language of 6 Billion People". Mobile Messaging Futures 2014-2018. Retrieved from http://www.portioresearch.com/en/messaging-reports/mobile-messaging-research/ mobile-messaging- futures-2014-2018.aspx

Rafique, M. Z., & Abulaish, M. 2012. "Graph-Based Learning Model for Detection of SMS Spam on Smart Phones". In International Wireless Communications and Mobile Computing Conference (IWCMC) (Vol. 53, pp. 1689–1699). https://doi.org/10.1017/CBO9781107415324.004

Rafique, M. Z., & Farooq, M. 2010. "SMS Spam Detection by Operating on Byte-Level Distributions Using Hidden Markov Models (HMMS)". In Virus Bulletin Conference (pp. 1–7).

Rahman, N. H. A., Abdullah, N. A., A. Hamid, I. R., Chai Wen, C., & Mohd Jelani, M. S. R. 2017. "A CCTV System with SMS Alert (CMDSA): An Implementation of Pixel Processing Algorithm for Motion Detection". In International Conference on Applied Science and Technology (ICAST) (Vol. 1891, pp. 1–6). https://doi.org/10.1063/1.5005346

Rauscher, K. F., & Yonglin, Z. 2011. Fighting Spam to Build Trust.

Ricknas, M. 2014. "UK Mobile Operators Join Forces to Combat Text Spam". Retrieved April 1, 2014, from http://www.networkworld.com/article/2175359/network-security/uk-mobile-operators-join-forces-to-combat-text-spam.html

Roshidi, A. S. 2018. "More fall for 'Macau Scam' in Malacca". New Straits Times, pp. 1–2.

S.Kannan, & Gurusamy, V. 2015. "Preprocessing Techniques for Text Mining". International Journal of Computer Science & Communication Networks, 5(1), 7–16. Retrieved from http://www.ijcscn.com/Documents/Volumes/vol5issue1/ijcscn2015050102.pdf

Samsudin, N., Hamda, A. R., Puteh, M., & Nazri, M. Z. A. 2013. "Mining Opinion in Online Messages". International Journal of Advanced Computer Science and Applications (IJACSA), 4(8), 19–24. Retrieved from http://ijacsa.thesai.org/

Samsudin, N., Puteh, M., Hamdan, A. R., & Ahmad Nazri, M. Z. 2012. "Normalization of Common NoisyTerms in Malaysian Online Media". In Knowledge Management International Conference (KMICe) (pp. 515–520). Retrieved from http://www.kmice.cms.net.my/ProcKMICe /KMICe2012/PDF/CR204.pdf

Scott, J., & Spaniel, D. 2016. "The ICIT Ransomware Report. Institute for Critical Infrastructure Technology". Retrieved from http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report.pdf

Sethi, G., & Bhootna, V. 2014. "SMS Spam Filtering Application Using Android". International Journal of Computer Science and Information Technologies (IJCSIT), 5(3), 4624–4626.

Shamshirband, S., Anuar, N. B., Kiah, M. L. M., Rohani, V. A., Petkovic, D., Misra, S., & Khan, A. N. 2014. "Co-FAIS : Cooperative Fuzzy Artificial Immune System for Detecting Intrusion in Wireless Sensor Networks". Journal of Network and Computer Applications, 42, 102–117. https://doi.org/10.1016/j.jnca.2014.03.012

Shirali-Shahreza, M. H., & Shirali-Shahreza, M. 2008. "An Anti-SMS-Spam Using CAPTCHA". In International Colloquium on Computing, Communication, Control and Management (pp. 318–321). https://doi.org/10.1109/CCCM.2008.247

SIG, R. A. S. I. G. 2012. "PCI Data Security Standard Risk Assessment Guidelines". Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf

Singh, D., & Bedi, S. S. 2015. "Novel Intrusion Detection in MANETs Based on Trust". International Journal of Computer Science and Information Technologies (IJCSIT), 6(4), 3556–3560.

Singhal, K., Arora, G., Kumari, S., & Majumder, P. 2013. "SMS Normalization for FAQ Retrieval". Forum for Information Retrieval Evaluation (FIRE), 7536, 163–174. https://doi.org/10.1007/978-3-642-40087-2_16

Song, G., Ye, Y., Du, X., Huang, X., & Bie, S. 2014. "Short Text Classification: A Survey". Journal of Multimedia, 9(5), 635–643. https://doi.org/10.4304/jmm.9.5.635-643

Sonowal, G., & Kuppusamy, K. S. 2018. "SmiDCA: An Anti-Smishing Model with Machine Learning Approach". The British Computer Society 2018, (June), 1–15. https://doi.org/10.1093/comjnl/bxy039/4985552

Srividhya, V., & Anitha, R. 2010. "Evaluating Preprocessing Techniques in Text Categorization". International Journal of Computer Science and Application, 49–51. Retrieved from http://www.sinhgad.edu/IJCSA-2012/pdfpapers/1_11.pdf

Stepney, S., Smith, R. E., Timmis, J., Tyrell, A. M., J.Neal, M., & N.W.Hone, A. 2005. "Conceptual Frameworks for Artificial Immune Systems". Retrieved from http://download.adamas.ai/dlbase/ebooks/AX_related/Conceptual Frameworks for Artificial Immune Systems.pdf

Stoneburner, G., Goguen, A., & Feringa, A. 2002. "Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology". NIST Special Publication 800-30. https://doi.org/10.1111/j.1745-6622.2008.00202.x

Sulaiman, N. F., & Jali, M. Z. 2014. "Integrated Mobile Spam Model Using Artificial Immune System Algorithms". In Knowledge Management International Conference (KMICe) (pp. 1–5). Retrieved from http:www.kmice.cms.net.my

Sulaiman, N. F., & Jali, M. Z. 2015. "A New SMS Spam Detection Method Using Both Content-Based and Non Content-Based Features". In Advanced Computer and Communication Engineering Technology (pp. 505–514).

Suleiman, D., & Al-Naymat, G. 2017. "SMS Spam Detection using H2O Framework". In International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN) (Vol. 113, pp. 154–161). Elsevier B.V. https://doi.org/10.1016/j.procs.2017.08.335

Sun, F. 2011. "Danger Theory Based Model for Network Security Risk Assessment". Advanced Materials Research, 187(2), 148–154. https://doi.org/10.4028/www.scientific.net/AMR.187.148

Tan, H., Goharian, N., & Sherr, M. 2012. "$100,000 Prize Jackpot. Call Now! Identifying the Pertinent Features of SMS Spam". In Special Interest Group on Information Retrieval (SIGIR) (pp. 1175–1176).

Telecom, G. 2017. "Globe Block More Than 165M Spam/Scam Messages in 2016". Retrieved February 3, 2017, from http://newsroom.globe.com.ph/press-release/consumer/2017-01/globe-blocks-more-than-165.html

The Institute of Risk Management (IRM). 2010. "A Structured Approach to Enterprise Risk Management (ERM) and The Requirements of ISO 31000". The Public Risk Management Association. https://doi.org/10.1016/j.solmat.2010.12.013

Theoharidou, M., Mylonas, A., & Gritzalis, D. 2012. "A Risk Assessment Method for Smartphones". In International Information Security Conference (pp. 443-456).

Trivedi, S. K., & Dey, S. 2016. "A Comparative Study of Various Supervised Feature Selection Methods for Spam Classification". In International Conference on Information and Communication Technology for Competitive Strategies (ICTCS) (pp. 1–6). https://doi.org/10.1145/2905055.2905122

Twycross, J., & Aickelin, U. 2006. "Experimenting with Innate Immunity". Retrieved from http://arxiv.org/abs/1004.2854

Twycross, J., & Aickelin, U. 2010. Libtissue-Implementing Innate Immunity.

Twycross, J. P. 2007. "Integrated Innate and Adaptive Artificial Immune Systems Applied to Process Anomaly Detection". Ph.D. Thesis, The University of Nottingham. University of Nottingham.

Tziortzis, S. 2013. Sentiment Analysis by Emoticons and Unsupervised Comment Summarization in Greek e-Government Data.

Unucheck, R. 2017. "Mobile Malware Evolution 2016". Retrieved from https://securelist.com/analysis/kaspersky-security-bulletin/77681/mobile-malware-evolution-2016/

Uysal, A. K., & Gunal, S. 2014. "The Impact of Preprocessing on Text Classification". Information Processing and Management, 50(1), 104–112. https://doi.org/10.1016/j.ipm.2013.08.006

Uysal, A. K., Gunal, S., Ergin, S., & Gunal, E. S. 2012. "A Novel Framework for SMS Spam Filtering". In International Symposium on Innovations in Intelligent Systems and Applications (INISTA) (pp. 1–4). https://doi.org/10.1109/INISTA.2012.6246947

Uysal, A. K., Gunal, S., Ergin, S., & Gunal, E. S. 2013. "The Impact of Feature Extraction and Selection on SMS Spam Filtering". Elektronika Ir Electrotechnika, 19(5), 67–72. https://doi.org/10.5755/j01.eee.19.5.1829

Vijayarani, S., Ilamathi, J., & Nithya, M. 2015. "Preprocessing Techniques for Text Mining-An Overview". International Journal of Computer Science & Communication Networks, 5(1), 7–16. Retrieved from http://www.ijcscn.com/Documents/Volumes/vol5issue1/ijcscn2015050102.pdf

Vural, I., & Venter, H. S. 2012. "Combating Mobile Spam Through Botnet Detection Using Artificial Immune Systems". Journal of Universal Computer Science, 18(6), 750–774.

Waheeb, W., & Ghazali, R. 2017. "Content-based SMS Classification: Statistical Analysis for the Relationship between Number of Features and Classification Performance". Computacion y Sistemas, 21(4), 771–785. https://doi.org/10.13053/CyS-21-4-2593

Wang, A. H. 2012. "Machine Learning for the Detection of Spam in Twitter Networks". In International Joint Conference on e-Business and Telecommunications (ICETE) (pp. 319–333).

Warade, S. J., A.Tijare, P., & N.Sawalkar, S. 2016. "Implementation of SMS Spam Detection System". International Journal of Research in Advent Technology, 4(5), 46–52.

Warade, S. J., Tijare, P. A., & Sawalkar, S. N. 2014. "An Approach for SMS Spam Detection". International Journal of Research in Advent Technology, 2(12), 8–11.

Wasilewska, A., Vijaykumar, S., & Sonawane, P. 2014. "Text Mining: Overview, Applications and Issues".

Wieder, E. 2003. "Dendritic Cells: A Basic Review". International Society for Cellular Therapy, (May), 1–6. Retrieved from www.celltherapysociety.org

Witten, I. H. 2011. "Text Mining". International Journal of Computational Biology and Drug Design, 4(3), 239–244. https://doi.org/10.1504/IJCBDD.2011.041412

Xia, H., Fu, Y., & Zhou, J. 2013. "Intelligent Spam Filtering for Massive Short Message Stream". International Journal for Computation and Mathematics in Electrical and Electronic Engineering, 32(2), 586–596. https://doi.org/10.1108/03321641311296963

Xu, Q., Xiang, E. W., Yang, Q., Du, J., & Zhong, J. 2012. "SMS Spam Detection Using Noncontent Features". IEEE Intelligent Systems, 44–51.

Yadav, K., Kumaraguru, P., Goyal, A., Gupta, A., & Naik, V. 2011. "SMSAssassin: Crowdsourcing Driven Mobile-based System for SMS Spam Filtering". In Workshop on Mobile Computing Systems and Applications (pp. 1–6). https://doi.org/10.1145/2184489.2184491

Yadav, K., Saha, S. K., Kumaraguru, P., & Kumra, R. 2012. "Take Control of Your SMSes: Designing an Usable Spam SMS Filtering System". In International Conference on Mobile Data Management (pp. 352–355). https://doi.org/10.1109/MDM.2012.54

Yan, G., Eidenbenz, S., & Galli, E. 2009. "SMS-Watchdog: Profiling Social Behaviors of SMS Users for Anomaly Detection". Recent Advances in Intrusion Detection (RAID), 5758, 202–223. https://doi.org/10.1007/978-3-642-04342-0_11

Yeboah-Boateng, E. O., & Amanor, P. M. 2014. "Phishing, SMiShing & Vishing: An Assessment of Threats Against Mobile Devices". Journal of Emerging Trends in Computing and Information Sciences, 5(4), 297–307.

Yoon, J. W., Kim, H., & Huh, J. H. 2010. "Hybrid Spam Filtering for Mobile Communication". Computers and Security, 29(4), 446–459. https://doi.org/10.1016/j.cose.2009.11.003

Zainal, K., & Jali, M. Z. 2017. "The Significant Effect of Feature Selection Methods in Spam Risk Assessment using Dendritic Cell Algorithm". In International Conference on Information and Communication Technology (ICoICT 2017) (pp. 277–284).

Zainal, K., Sulaiman, N. F., & Jali, M. Z. 2015. "An Analysis of Various Algorithms For Text Spam Classification and Clustering Using RapidMiner and Weka". International Journal of Computer Science and Information Security (IJCSIS), 13(3), 66–74. Retrieved from http://sites.google.com/site/ijcsis/

Zalpuri, N., & Arora, M. 2015. "An Efficient Model for S.M.S Security and SPAM Detection: A Review". International Journal of Computer Sciences and Engineering (IJCSE), 3(12), 1–6.

Zaman, M., & Toth, I. 2013. "Immunostimulation by Synthetic Lipopeptide-based Vaccine Candidates: Structure-activity Relationships". Frontiers in Immunology, 4(OCT), 1–12. https://doi.org/10.3389 /fimmu.2013.00318

Zareapoor, M., & Seeja, K. . 2015. "Feature Extraction or Feature Selection for Text Classification: A Case Study on Phishing Email Detection". International Journal Information Engineering and Electronic Business, 2(March), 60–65. https://doi.org/10.5815/ijieeb.2015.02.08

Zekri, M., Souici, L., & Meslati, 2014. "Immunological Approach for Intrusion Detection". ARIMA Journal, 17, 221–240.

Zhang, H., & Wang, W. 2009. "Application of Bayesian Method to Spam SMS Filtering". In International Conference on Information Engineering and Computer Science (ICIECS) (pp. 1–3).

Zhang, L., Zhu, J., & Yao, T. 2004. "An Evaluation of Statistical Spam Filtering Techniques". ACM Transactions on Asian Language Information Processing (TALIP), 3(4), 243–269. https://doi.org/10.1.1.109.7685

Zhang, P., & Tan, Y. 2014. "Immune Cooperation Mechanism Based Learning Framework". Neurocomputing, 1–9. https://doi.org/10.1016/j.neucom.2012.08.076

Zhang, Y., Xiao, Y., Ghaboosi, K., Zhang, J., & Deng, H. 2012. "A Survey of Cyber Crimes". Security and Communication Networks, 5, 422–437. https://doi.org/10.1002/sec.331

Zhao, Y., Zhang, Z., Wang, Y., & Liu, J. 2012. "Robust Mobile Spamming Detection via Graph Patterns". In International Conference on Pattern Recognition (ICPR) (pp. 983–986).

APPENDIX A
List of Published Papers

No	Title	Name of Journal / Conference	Publication Year	Indexed In
1	An Analysis of Various Algorithms For Text Spam Classification and Clustering Using RapidMiner and Weka	*International Journal of Computer Science and Information Security (IJCSIS)*	2015	Google Scholar
2	A Perception Model of Spam Risk Assessment Inspired by Danger Theory of Artificial Immune Systems	*International Conference on Computer Science and Computational Intelligence (ICCSCI)*	2015	Scopus
3	A Review of Feature Extraction Optimization in SMS Spam Messages Classification	*International Conference on Soft Computing in Data Science (SCDS)*	2016	Scopus / ISI Proceedings
4	The Design and Development of Spam Risk Assessment Prototype: In Silico of Danger Theory Variants	*International Journal of Advanced Computer Science and Applications (IJACSA)*	2017	Thomson Reuters Emerging Sources Citation Index
5	The Significant Effect of Feature Selection Methods in Spam Risk Assessment Using Dendritic Cell Algorithm	*International Conference on Information and Communication Technology (ICoICT)*	2017	Scopus
6	Comparative Analysis of Danger Theory Variants in Measuring Risk Level for Text Spam Messages	*International Symposium on Data Mining Applications (SDMA)*	2018	Scopus / ISI Proceedings
7	An Immunological-based Simulation: A Case Study of Risk Concentration for Mobile Spam Context Assessment	*International Journal of Advanced Science, Engineering and Information Technology (IJASEIT)*	2018	Scopus

APPENDIX B

Research Operational Template (ROT)

RESEARCH GAP

Spam management consists phases of classification, clustering and determination of spam severity level (as integrated with common standard of Risk Management). Numerous works have been found for the spam classification and clustering, but only small number of research available for the final phase, risk assessment. This missing piece is needed to be filled in order to assist users to decipher the spam's risk and help them respond accordingly against spam.

WORKING TITLE

Risk Concentration for Context Assessment (RiCCA) of SMS Messages Using Danger Theory

THEORITICAL MODEL

Danger Theory by Matzinger (1994)
Dendritic Cell Algorithm (DCA) by Greensmith (2007)
Deterministic Dendritic Cell Algorithm (dDCA) by Greensmith (2010)

PROBLEM STATEMENT

Unknowing of a risk level of the received spam would lead to serious adverse impact, since human is the weakest link in security chain and due to lacking of awareness and knowledge, users tend to response inappropriately. Hence, there is a critical need to develop an intelligent decision support system in aiding users to make decision wisely in reminding the potential risk and responding against spam.

RESEARCH QUESTIONS

i. How text spam messages can be assessed for its risk value?
ii. What is the possible mechanism to apply Danger Theory in risk assessment of text spam messages?
iii. How can the proposed risk assessment model for text spam messages identified as a reliable solution?

OBJECTIVES

i. to study and evaluate the Danger Theory of AIS for application in risk identification and assessment on text spam messages;
ii. to propose and develop a model that is related to the assessment of spam risk level using an integration of the Danger Theory, text mining and risk assessment methodology; and
iii. to evaluate the accuracy of the proposed model with the aim of more than 90% accuracy rate.

INSTRUMENT

i. Immunological-based simulation cycle
ii. Prototype designed and developed that is inspired from Danger Theory of AIS

ANALYSIS

Performance Metrics: Accuracy in spam categorizing according to 3 distinguished severity levels (high, medium and low)

RESEARCH DESIGN

Mixed methods: qualitative and quantitative

SAMPLING FRAME / TECHNIQUE

Datasets SMS collected from the public shared corpus and self-collected data.

CONTRIBUTION TO THE BODY OF KNOWLEDGE

i. Danger Theory of AIS is recognized as one of the applied alternative in assessing risk.
ii. The findings of this works can be extended in determination of severity level for other form of spam message such as email spamming, instant messaging or chat media such as WhatsApp and other's Internet spamming such in social media and blog website.
iii. The automated mechanism that has been developed could enhance the research work in text mining, specifically in computational linguistics and information retrieval.

APPENDIX C
Research Milestone

APPENDIX C -
Research Milestone

WBS	Tasks	Start	End	Duration (Days)
1.0	**Draft the Research Proposal**	13-Feb-14	14-Jul-14	152
1.1	Attending Research Methodology and Data Analysis class (compulsory)	13-Feb-14		
1.2	Do Literature Review as background study			
1.3	Formulate the research gap and objectives			
1.4	Identify research methodology and approach			
1.5	Thesis writing - Chapter 1			
1.6	Design the proposed framework			
1.7	Plan for data collection, processing and analysis			
1.8	Thesis writing - Chapter 2		14-Jul-14	
2.0	**Presenting and Submission of Research Proposal**	15-Jul-14	31-Mar-15	260
2.1	Prepare research proposal	15-Jul-14		
2.2	Present (and defence) the research proposol in Qualifying Test (QT) session	21-Jan-15	21-Jan-15	
2.3	Making correction or amendment of the proposal document			
2.4	Submission of edited version of the proposal	30-Mar-15	30-Mar-15	
2.5	Accepted paper for journal publication (Paper #1)		31-Mar-15	
3.0	**Designation of the Proposed Framework**	01-Apr-15	30-Sep-16	549
3.1	Designation of algorithm and framework	01-Apr-15		
3.2	Accepted paper for proceeding (Paper #2)	24-Aug-15	26-Aug-15	
3.3	Data collection			
3.4	Initial data analysis			
3.5	Accepted paper for proceeding (Paper #3)	21-Sep-16	22-Sep-16	
3.6	Thesis writing - Chapter 3		30-Sep-16	
4.0	**Algorithm Testing as Initial Evaluation**	01-Oct-16	31-May-17	231
4.1	Evaluation of the initial algorithm design and re-design as necessary	01-Oct-16		
4.2	Execute testing to identify algorithm feasibility			
4.3	Accepted paper for journal publication (Paper #4)	30-Apr-17	30-Apr-17	
4.4	Accepted paper for proceeding (Paper #5)	17-May-17	19-May-17	
4.5	Development of prototype		31-May-17	
5.0	**Development of the Prototype and Final Testing**	01-Jun-17	30-Nov-17	183
5.1	Development of prototype (continued)	01-Jun-17		
5.2	Thesis writing - Chapter 4			
5.3	Additional data collection			
5.4	Final testing and data analysis			
5.5	Thesis writing - Chapter 5 and Chapter 6		30-Nov-17	
6.0	**Thesis Submission For Viva-voce**	01-Dec-17	31-Mar-18	121
6.1	Submission for proofreading	01-Dec-17		
6.2	Final editing of the thesis			
6.3	Softbound submission (via iPPS portal)	11-Mar-18	11-Mar-18	
6.4	Accepted paper for proceeding (Paper #6)	21-Mar-18	22-Mar-18	
6.5	Thesis submission for viva session	19-Mar-18	31-Mar-18	
7.0	**Viva-voce and Thesis Final Submission**	01-Apr-18	30-Aug-18	152
7.1	Accepted paper for journal publication (Paper #7)	02-May-18	02-May-18	
7.2	Viva-voce session	25-May-18	25-May-18	

APPENDIX D

Source Code For The RiCCA Prototype

DCA Calculation

```
import java.util.Map;

public class CalculatorDca {
        public static boolean calculate(ProcessInput procInput, ProcessResult procResult,
Map<String, Double> schemes) {

                // Level of input signals
                for (String x : procResult.words) {
                        // TODO: ?
                        // if (x.equals("ok")) {
                        // continue;
                        // }

                        if (schemes.containsKey(x)) {
                                if (procResult.listOfTerm1.containsKey(x)) {
                                        ListOfTerm lot = procResult.listOfTerm1.get(x);
                                        lot.n++;
                                } else {
                                        Double v = schemes.get(x);
                                        ListOfTerm lot = new ListOfTerm();
                                        lot.word = x;
                                        lot.value = v.doubleValue();
                                        lot.n = 1;

                                        if (lot.value <= procInput.dcaPamp1 && lot.value >=
procInput.dcaPamp2)
                                                lot.level = AppConst.LEVEL_PAMP;
                                        else if (lot.value < procInput.dcaPamp2 && lot.value
>= procInput.dcaDanger2)
                                                lot.level = AppConst.LEVEL_DANGER;
                                        else if (lot.value < procInput.dcaDanger2 && lot.value
>= procInput.dcaSafe2)
                                                lot.level = AppConst.LEVEL_SAFE;

                                        procResult.listOfTerm1.put(x, lot);
                                }
                        }
                }

                // Calculate (max, min, average) value of terms
                ListOfTerm maxPamp = null;
                ListOfTerm maxDanger = null;
                ListOfTerm maxSafe = null;

                ListOfTerm minPamp = null;
                ListOfTerm minDanger = null;
                ListOfTerm minSafe = null;

                double totalPamp = 0.0;
                double totalDanger = 0.0;
                double totalSafe = 0.0;
```

```
int nPamp = 0;
int nDanger = 0;
int nSafe = 0;

for (String key : procResult.listOfTerm1.keySet()) {
        ListOfTerm lot = procResult.listOfTerm1.get(key);
        // System.out.println(lot.word + ", " + lot.value + ", " + lot.n + ", " +
        // AppConst.getLevelName(lot.level));

        if (lot.level == AppConst.LEVEL_PAMP) {
                if (maxPamp == null || maxPamp.value < lot.value)
                        maxPamp = lot;

                if (minPamp == null || minPamp.value > lot.value)
                        minPamp = lot;

                totalPamp += (lot.value * lot.n);
                nPamp += lot.n;
        } else if (lot.level == AppConst.LEVEL_DANGER) {
                if (maxDanger == null || maxDanger.value < lot.value)
                        maxDanger = lot;

                if (minDanger == null || minDanger.value > lot.value)
                        minDanger = lot;

                totalDanger += (lot.value * lot.n);
                nDanger += lot.n;
        } else if (lot.level == AppConst.LEVEL_SAFE) {
                if (maxSafe == null || maxSafe.value < lot.value)
                        maxSafe = lot;

                if (minSafe == null || minSafe.value > lot.value)
                        minSafe = lot;

                totalSafe += (lot.value * lot.n);
                nSafe += lot.n;
        }
}

procResult.maxPamp = maxPamp == null ? 0 : maxPamp.value;
procResult.maxDanger = maxDanger == null ? 0 : maxDanger.value;
procResult.maxSafe = maxSafe == null ? 0 : maxSafe.value;
procResult.minPamp = minPamp == null ? 0 : minPamp.value;
procResult.minDanger = minDanger == null ? 0 : minDanger.value;
procResult.minSafe = minSafe == null ? 0 : minSafe.value;
procResult.avgPamp = nPamp > 0 ? (totalPamp / nPamp) : 0;
procResult.avgDanger = nDanger > 0 ? (totalDanger / nDanger) : 0;
procResult.avgSafe = nSafe > 0 ? (totalSafe / nSafe) : 0;

// System.out.println("Max-> " + procResult.maxPamp + " : " +
// procResult.maxDanger + " : " + procResult.maxSafe);
// System.out.println("Min-> " + procResult.minPamp + " : " +
// procResult.minDanger + " : " + procResult.minSafe);
// System.out.println("Avg-> " + procResult.avgPamp + " : " +
// procResult.avgDanger + " : " + procResult.avgSafe);

// Calculate output signals - Cycle 1
```

```
                procResult.outputCsm1 = (procInput.dcaCsm1 * procResult.maxPamp) +
(procInput.dcaCsm2 * procResult.maxDanger)
                        + (procInput.dcaCsm3 * procResult.maxSafe);

                // System.out.println(String.format("CSM1 = (%f * %f) + (%f * %f) + (%f * %f)
=>
                // %f", procInput.dcaCsm1,
                // procResult.maxPamp, procInput.dcaCsm2, procResult.maxDanger,
                // procInput.dcaCsm3, procResult.maxSafe,
                // procResult.outputCsm1));

                procResult.outputSmdc1 = (procInput.dcaSmdc1 * procResult.maxPamp) +
(procInput.dcaSmdc2 * procResult.maxDanger)
                        + (procInput.dcaSmdc3 * procResult.maxSafe);

                // System.out.println(String.format("smDC1 = (%f * %f) + (%f * %f) + (%f *
%f)
                // => %f", procInput.dcaSmdc1,
                // procResult.maxPamp, procInput.dcaSmdc2, procResult.maxDanger,
                // procInput.dcaSmdc3, procResult.maxSafe,
                // procResult.outputSmdc1));

                procResult.outputMdc1 = (procInput.dcaMdc1 * procResult.maxPamp) +
(procInput.dcaMdc2 * procResult.maxDanger)
                        - (procInput.dcaMdc3 * procResult.maxSafe);

                // System.out.println(String.format("mDC1 = (%f * %f) + (%f * %f) + (%f * %f)
=>
                // %f", procInput.dcaMdc1,
                // procResult.maxPamp, procInput.dcaMdc2, procResult.maxDanger,
                // procInput.dcaMdc3, procResult.maxSafe,
                // procResult.outputMdc1));

                // Calculate output signals - Cycle 2
                procResult.outputCsm2 = (procInput.dcaCsm1 * procResult.minPamp) +
(procInput.dcaCsm2 * procResult.minDanger)
                        + (procInput.dcaCsm3 * procResult.minSafe);
                procResult.outputSmdc2 = (procInput.dcaSmdc1 * procResult.minPamp) +
(procInput.dcaSmdc2 * procResult.minDanger)
                        + (procInput.dcaSmdc3 * procResult.minSafe);
                procResult.outputMdc2 = (procInput.dcaMdc1 * procResult.minPamp) +
(procInput.dcaMdc2 * procResult.minDanger)
                        - (procInput.dcaMdc3 * procResult.minSafe);

                // Calculate output signals - Cycle 3
                procResult.outputCsm3 = (procInput.dcaCsm1 * procResult.avgPamp) +
(procInput.dcaCsm2 * procResult.avgDanger)
                        + (procInput.dcaCsm3 * procResult.avgSafe);
                procResult.outputSmdc3 = (procInput.dcaSmdc1 * procResult.avgPamp) +
(procInput.dcaSmdc2 * procResult.avgDanger)
                        + (procInput.dcaSmdc3 * procResult.avgSafe);
                procResult.outputMdc3 = (procInput.dcaMdc1 * procResult.avgPamp) +
(procInput.dcaMdc2 * procResult.avgDanger)
                        - (procInput.dcaMdc3 * procResult.avgSafe);

                // System.out.println("procResult.outputCsm1: " + procResult.outputCsm1);
                // System.out.println("procResult.outputSmdc1: " + procResult.outputSmdc1);
```

```
                // System.out.println("procResult.outputMdc1: " + procResult.outputMdc1 +
"\n");

                // System.out.println("procResult.outputCsm2: " + procResult.outputCsm2);
                // System.out.println("procResult.outputSmdc2: " + procResult.outputSmdc2);
                // System.out.println("procResult.outputMdc2: " + procResult.outputMdc2 +
"\n");

                // System.out.println("procResult.outputCsm3: " + procResult.outputCsm3);
                // System.out.println("procResult.outputSmdc3: " + procResult.outputSmdc3);
                // System.out.println("procResult.outputMdc3: " + procResult.outputMdc3 +
"\n");

                // Compare value mDC and smDC
                procResult.mdc = 0;
                procResult.smDc = 0;

                if (procResult.outputMdc1 > procResult.outputSmdc1)
                        procResult.mdc++;

                if (procResult.outputMdc2 > procResult.outputSmdc2)
                        procResult.mdc++;

                if (procResult.outputMdc3 > procResult.outputSmdc3)
                        procResult.mdc++;

                if (procResult.outputMdc1 < procResult.outputSmdc1)
                        procResult.smDc++;

                if (procResult.outputMdc2 < procResult.outputSmdc2)
                        procResult.smDc++;

                if (procResult.outputMdc3 < procResult.outputSmdc3)
                        procResult.smDc++;

                // procResult.mdcGreaterThanSmdc = 0;
                // procResult.mdcGreaterThanSmdc += (procResult.outputMdc1 >
                // procResult.outputSmdc1) ? 1 : 0;
                // procResult.mdcGreaterThanSmdc += (procResult.outputMdc2 >
                // procResult.outputSmdc2) ? 1 : 0;
                // procResult.mdcGreaterThanSmdc += (procResult.outputMdc3 >
                // procResult.outputSmdc3) ? 1 : 0;

                // Identify terms with High, Medium & Low
                for (String x : procResult.words) {
                        if (schemes.containsKey(x)) {
                                if (procResult.listOfTerm2.containsKey(x)) {
                                        ListOfTerm lot = procResult.listOfTerm2.get(x);
                                        lot.n++;
                                } else {
                                        Double v = schemes.get(x);
                                        ListOfTerm lot = new ListOfTerm();
                                        lot.word = x;
                                        lot.value = v.doubleValue();
                                        lot.n = 1;

                                        if (lot.value <= procInput.dcaPamp1 && lot.value >=
procInput.dcaPamp2)
```

```
                                        lot.level = AppConst.LEVEL_HIGH;
                                    else if (lot.value < procInput.dcaPamp2 && lot.value
>= procInput.dcaDanger2)
                                        lot.level = AppConst.LEVEL_MEDIUM;
                                    else if (lot.value < procInput.dcaDanger2 && lot.value
>= procInput.dcaSafe2)
                                        lot.level = AppConst.LEVEL_LOW;

                                    procResult.listOfTerm2.put(x, lot);
                                }
                            }
                        }

                        // Calculate MCAV
                        procResult.totalHighMedium = 0;
                        procResult.totalAll = 0;

                        for (String key : procResult.listOfTerm2.keySet()) {
                            ListOfTerm lot = procResult.listOfTerm2.get(key);

                            if (lot.level == AppConst.LEVEL_HIGH || lot.level ==
AppConst.LEVEL_MEDIUM) {
                                procResult.totalHighMedium += lot.n;
                            }

                            procResult.totalAll += lot.n;
                        }

                        procResult.mcav = ((double) procResult.totalHighMedium) / ((double)
procResult.totalAll);

                        if (procResult.mdc > procResult.smDc && procResult.mcav > procInput.dcaTm)
{
                            procResult.mcavResultLevel = getResultHighMedium(procInput,
procResult.mcav);
                        } else if (procResult.mdc < procResult.smDc && procResult.mcav <
procInput.dcaTm) {
                            procResult.mcavResultLevel = getResultLow(procInput,
procResult.mcav);
                        } else if (procResult.mdc == procResult.smDc && procResult.mcav >
procInput.dcaTm) {
                            procResult.mcavResultLevel = getResultHighMedium(procInput,
procResult.mcav);
                        } else if (procResult.mdc == procResult.smDc && procResult.mcav <
procInput.dcaTm) {
                            procResult.mcavResultLevel = getResultLow(procInput,
procResult.mcav);
                        } else if (procResult.mdc > procResult.smDc && procResult.mcav ==
procInput.dcaTm) {
                            procResult.mcavResultLevel = getResultHighMedium(procInput,
procResult.mcav);
                        } else if (procResult.mdc < procResult.smDc && procResult.mcav ==
procInput.dcaTm) {
                            procResult.mcavResultLevel = getResultLow(procInput,
procResult.mcav);
                        } else if (procResult.mdc > procResult.smDc && procResult.mcav <
procInput.dcaTm) {
```

```
                    procResult.mcavResultLevel =
AppConst.LEVEL_CONDITION_MISMATCH;
                } else if (procResult.mdc < procResult.smDc && procResult.mcav >
procInput.dcaTm) {
                    procResult.mcavResultLevel =
AppConst.LEVEL_CONDITION_MISMATCH;
                }

                return true;
        }

        private static int getResultHighMedium(ProcessInput procInput, double mcav) {
                if (mcav <= procInput.dcaPamp1 && mcav >= procInput.dcaPamp2)
                        return AppConst.LEVEL_HIGH;
                else if (mcav < procInput.dcaPamp2 && mcav >= procInput.dcaDanger2)
                        return AppConst.LEVEL_MEDIUM;
                else if (mcav < procInput.dcaDanger2 && mcav >= procInput.dcaSafe2)
                        return AppConst.LEVEL_VALUE_MISMATCH;
                return 0;
        }

        private static int getResultLow(ProcessInput procInput, double mcav) {
                if (mcav <= procInput.dcaPamp1 && mcav >= procInput.dcaPamp2)
                        return AppConst.LEVEL_VALUE_MISMATCH;
                else if (mcav < procInput.dcaPamp2 && mcav >= procInput.dcaDanger2)
                        return AppConst.LEVEL_VALUE_MISMATCH;
                else if (mcav < procInput.dcaDanger2 && mcav >= procInput.dcaSafe2)
                        return AppConst.LEVEL_LOW;
                return 0;
        }
}
```

dDCA Calculation

```
import java.util.Map;

public class CalculatorDdca {

	public static boolean calculate(ProcessInput procInput, ProcessResult procResult,
Map<String, Double> schemes) {

		// Level of input signals
		for (String x : procResult.words) {
			if (schemes.containsKey(x)) {
				if (procResult.listOfTerm1.containsKey(x)) {
					ListOfTerm lot = procResult.listOfTerm1.get(x);
					lot.n++;
				} else {
					Double v = schemes.get(x);
					ListOfTerm lot = new ListOfTerm();
					lot.word = x;
					lot.value = v.doubleValue();
					lot.n = 1;

					if (lot.value <= procInput.ddcaInputA1 && lot.value
>= procInput.ddcaInputA2)
						lot.level = AppConst.LEVEL_DANGER;
					else if (lot.value < procInput.ddcaInputA2 && lot.value
>= procInput.ddcaInputB2)
						lot.level = AppConst.LEVEL_DANGER;
					else if (lot.value < procInput.ddcaInputB2 && lot.value
>= procInput.ddcaInputC2)
						lot.level = AppConst.LEVEL_SAFE;

					procResult.listOfTerm1.put(x, lot);
				}
			}
		}

		procResult.totalDanger = 0.0;
		procResult.totalSafe = 0.0;
		procResult.numOfTerms = 0;

		for (String key : procResult.listOfTerm1.keySet()) {
			ListOfTerm lot = procResult.listOfTerm1.get(key);
			// System.out.println(lot.word + ", " + lot.value + ", " + lot.n + ", " +
			// AppConst.getLevelName(lot.level));

			if (lot.level == AppConst.LEVEL_DANGER)
				procResult.totalDanger += (lot.value * lot.n);
			else if (lot.level == AppConst.LEVEL_SAFE)
				procResult.totalSafe += (lot.value * lot.n);

			procResult.numOfTerms += lot.n;
		}

		procResult.sk = procResult.totalDanger - (2 * procResult.totalSafe);
		procResult.k = procResult.sk / procResult.numOfTerms;

		if (procResult.k > 0 && procResult.k > procInput.ddcaTk) {
```

```
                        procResult.outputResultLevel = getResultHighMedium(procInput,
procResult.k);
                } else if (procResult.k < 0 && procResult.k < procInput.ddcaTk) {
                        procResult.outputResultLevel = getResultLow(procInput,
procResult.k);
                } else if (procResult.k == 0 && procResult.k > procInput.ddcaTk) {
                        procResult.outputResultLevel = getResultHighMedium(procInput,
procResult.k);
                } else if (procResult.k == 0 && procResult.k < procInput.ddcaTk) {
                        procResult.outputResultLevel = getResultLow(procInput,
procResult.k);
                } else if (procResult.k > 0 && procResult.k == procInput.ddcaTk) {
                        procResult.outputResultLevel = getResultHighMedium(procInput,
procResult.k);
                } else if (procResult.k < 0 && procResult.k == procInput.ddcaTk) {
                        procResult.outputResultLevel = getResultLow(procInput,
procResult.k);
                } else if (procResult.k > 0 && procResult.k < procInput.ddcaTk) {
                        procResult.outputResultLevel =
AppConst.LEVEL_CONDITION_MISMATCH;
                } else if (procResult.k < 0 && procResult.k > procInput.ddcaTk) {
                        procResult.outputResultLevel =
AppConst.LEVEL_CONDITION_MISMATCH;
                }
                return true;
        }

        private static int getResultHighMedium(ProcessInput procInput, double k) {
                if (k <= procInput.ddcaOutputA1 && k >= procInput.ddcaOutputA2)
                        return AppConst.LEVEL_HIGH;
                else if (k < procInput.ddcaOutputA2 && k >= procInput.ddcaOutputB2)
                        return AppConst.LEVEL_MEDIUM;
                else if (k < 0)
                        return AppConst.LEVEL_VALUE_MISMATCH;
                return 0;
        }

        private static int getResultLow(ProcessInput procInput, double k) {
                if (k <= procInput.ddcaOutputA1 && k >= procInput.ddcaOutputA2)
                        return AppConst.LEVEL_VALUE_MISMATCH;
                else if (k < procInput.ddcaOutputA2 && k >= procInput.ddcaOutputB2)
                        return AppConst.LEVEL_VALUE_MISMATCH;
                else if (k < 0)
                        return AppConst.LEVEL_LOW;
                return 0;
        }
}
```

APPENDIX E

Questionnaire: Implicit Risk Of Spam Messages

UNIVERSITI SAINS ISLAM MALAYSIA
جَامِعَة العُلوم الإسْلامِيَة المَالِيزِيَة
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

QUESTIONNAIRE (4 pages)

"IMPLICIT RISK OF SPAM MESSAGES"

Researcher's General Information: Kamahazira Zainal is a Ph.D. student from Faculty of Science and Technology of Universiti Sains Islam Malaysia (USIM). Her research that is interest-based on information security focuses on assessing the potential risk of spam messages. An immunology theory that is known as Artificial Immune Systems (AIS) is applied in her research to verify its capability and reliability in measuring the severity concentration of spam content. The researcher can be contacted via arizah78@yahoo.com or +6012-9802629 for any further query.

Objective: This questionnaire is conducted with the purpose to verify the understanding of users and their abilities in identifying the risk and impact loss that may cause by spam messages. The result from this questionnaire will be considered as an **expert judgment resource** and will be compared to the risk-level calculated from the proposed solution, **RiCCA**. This automated version known as **Risk Concentration for Context Assessment** is developed and implemented in this research. This survey is divided into two (2) Sections; General information of respondent and their perspectives on spam's risk level.

Section A: Respondent's General Information

Please tick your answer.

1.	Age	☐ 21-30 years old	☐ 31-40 years old	☐ Over 41 years old
2.	Profession	☐ Government	☐ Private	☐ Other
3.	Are you using a **smartphone** for mobile communication?	☐ Yes	☐ No	
4.	Do you have **experience receiving spam** messages via SMS?	☐ Yes	☐ No	
5.	Have you ever **reply to the received SMS spam** messages? (please respond if answered *Yes* to question no.4)	☐ Yes, all the time	☐ Sometime	☐ Never

Based on your prior experience (if any) and common sense, please rate the following SMS spam messages for its possible risk level. The different risk levels are defined and distinguished as the following:

i. **HIGH RISK**: the spam message may cause SEVERE IMPACT if the user is responding accordingly as requested such as **clicking on a given URL link**. This action literally could activate phishing activity and scam/fraud action by the perpetrators. These may cause users to lose money and lead to identity theft.

ii. **MEDIUM RISK**: the spam message may cause SERIOUS IMPACT but lesser than high risk. This may happen if user responding to the message such as **return call or text back** to given unknown numbers. This action may impose some unnecessary/hidden cost to users or in worse case scenario; social-engineering technique may be applied for the perpetrator stealing confidential information such as bank card number and identification number.

iii. **LOW RISK**: the spam message basically only contains **information or notification** of something without requesting the user to reply or take any further action. This type of spam messages may have a NEGLIGIBLE RISK OR NONE at all. For certain circumstances, the very low risk for spam messages may validate as non-spam messages.

Section B: Respondent's Perspectives

Please tick your answer according to a reasonable risk level from your point of view (with the assistance of defined risk stated in the previous paragraph). This questionnaire has **20 samples** of SMS messages to be tagged for its possible risk level. These samples are adapted from the real-world case scenario.

No	SMS messages	Possible risk level		
1	Happy Birthday from TM Rewards! Get 96pcs 4R prints for RM9.90 (worth RM57.60)+FREE 1 box frame+2.5% Cashback www.shopback.my/tmb Valid till 31/3/17. T&;C apply	☐ High	☐ Medium	☐ Low
2	RM0 Guess the number of shuttlecocks & win! RM100K on Big Win now! Go2 www.bigwin.com.my & guess as many times you want! SincerelyCelcom.Info:1111	☐ High	☐ Medium	☐ Low
3	RM0 Have you heard CHARLIE PUTH's new hit single? Get WE DON'T TALK ANYMORE as your CallMeTones now! Dial *888*269129#.FREE 7days! SincrelyCelcom. info1111	☐ High	☐ Medium	☐ Low
4	You hv a missed call fr 067613333
5.3.2015 at 11:50 am)	☐ High	☐ Medium	☐ Low
5	Kindly note yr bill amounting to RM85.1 is now overdue. Pls remit pymt within 20 days to avoid call barring. Bill info: dial *111#.TQ	☐ High	☐ Medium	☐ Low
6	LAZADA: Your order 364244777 is being shipped. Please check your email for more info on the shipment.	☐ High	☐ Medium	☐ Low
7	RM0 BNM alert! Beware of phone calls or emails you receive. BNM/bank/PDRM will never require you to disclose your PIN or transfer your money to another	☐ High	☐ Medium	☐ Low

No	SMS messages	Possible risk level		
	account.			
8	RM0 Thank you for your payment of RM108.00. Stay connected with Celcom!	☐ High	☐ Medium	☐ Low
9	RM0 You've utilized 70% of your 4.00GB Internet. Thank you.	☐ High	☐ Medium	☐ Low
10	RM0.00 M2U: Your TAC No. is 933417. TRANSFER TO MAYBANK A/C ***0787/AMAN PALES for RM150.00 on 23 Dec 2016 17:43:31. Did not request? Call: 03-58914744	☐ High	☐ Medium	☐ Low
11	RM0 Your pay-per-use data roam charges have reached RMX. To continue using the service sends YESDATA to 28882. Thank you.	☐ High	☐ Medium	☐ Low
12	RM0.00 JQKclub.com; Live Casino, Slot Games Sportsbook & 4D; Register Now for 100% Welcome Bonus!; 0167909996	☐ High	☐ Medium	☐ Low
13	RM0.00 Maybank Cards: Spend & stand to buy Samsung Galaxy S6 at only RM188! SMS; space; New NRIC No; space; B2 to 66628 by 31/8/15. T&C: www.maybank.com.my	☐ High	☐ Medium	☐ Low
14	RM0.00 Win Cash Prize with Maybank EzyCash, EzyPay Plus or Balance Transfer from now till 21/08/16. Find out more http://mybk.co/wuis. T&C apply.	☐ High	☐ Medium	☐ Low
15	You have an important customer service announcement from PREMIER.	☐ High	☐ Medium	☐ Low
16	Hi - this is your Mailbox Messaging SMS alert. You have 4 messages. You have 21 matches. Please call back on 09056242159 to retrieve your messages and matches	☐ High	☐ Medium	☐ Low
17	Your unique user ID is 1172. For removal send STOP to 87239 customer services 08708034412	☐ High	☐ Medium	☐ Low
18	Check Out Choose Your Babe Videos @ sms.shsex.netUN fgkslpoPW fgkslpo	☐ High	☐ Medium	☐ Low
19	Congrats! 1-year special cinema pass for 2 is yours. call 09061209465 now! C Suprman V, Matrix3, StarWars3, etc all 4 FREE! bx420-ip4-5we. 150pm. Dont miss out!	☐ High	☐ Medium	☐ Low
20	URGENT! You have won a 1-week FREE membership in our RM100,000 Prize Jackpot! Txt the word: CLAIM to No: 81010 T&C www.dbuk.net LCCLTD POBOX 4403LDNW1A7RW18	☐ High	☐ Medium	☐ Low

Please state your **suggestion** if the definition of the stated risk level should be different (disagree) from the aforementioned paragraph (on page 2). Kindly please justify your suggestion.

Thank you for your co-operation.

Date: .....

-END OF QUESTIONNAIRE-

APPENDIX F

Validation Form: The Influence Of Risk Concentration For Context Assessment (RiCCA) Of SMS Messages In Daily Use

UNIVERSITI SAINS ISLAM MALAYSIA
جَامِعَة العُلُوم الإسْلَامِيَة المَالِيزِيَة
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

VALIDATION FORM

THE INFLUENCE OF RISK CONCENTRATION FOR CONTEXT ASSESSMENT (RiCCA) OF SMS MESSAGES IN DAILY USE

Dear Datuk / Datin / Prof. / Assoc. Prof. / Dr.,

I am a Ph.D. student of Faculty of Science & Technology, Universiti Sains Islam Malaysia (USIM). My research that is interest-based on information security focuses on assessing the potential risk of SMS messages. An immunology theory that is known as Artificial Immune Systems (AIS) is applied in this research to verify its capability and reliability in measuring the severity concentration of spam content.

Due to your reputation in the field of information security, I would like to ask for your opinion in validating the proposed model in this study. I am grateful for your time and effort participating in this questionnaire.

Objective:
This questionnaire is conducted with the purpose to verify the necessity or influence of the proposed model, **R**isk **C**oncentration for **C**ontext Assessment (RiCCA) in assisting users in detecting danger that may cause by spam messages. There are many mobile apps available online for spam filtering, but so far none for anticipating the risk that may occur.

The result from this questionnaire will be considered in the literature review of the thesis.

Research Gap Analysis:
Theoharidou, Mylonas, & Gritzalis (2016) and Yeboah-Boateng & Amanor (2014) proclaimed that SMS spam has been observed as one of the mobile threats due to its malevolent impacts. Since spam is needed to be treated as threat, then it is required to be managed as proposed in most of the risk management standards in order to prevail over it. There are three (3) main processes involved in managing spam which are spam classification, spam clustering, and determination level of spam's severity which also includes the options available to the response against spam.

There are numerous study found for SMS spam filtering (Lota & Hossain, 2017; Choudhary & Jain, 2017; Abdulhamid et al., 2017; M.El-Alfy & Alhasan, 2016; Sulaiman & Jali, 2015; Mosquera et al., 2014) which differentiation of spam and ham (valid) messages. However, so far **there are no study found in assessing the risk of SMS spam messages**. A study done by

Theoharidou et al. (2012) shared a risk that may occurred for many type of threats in a smart phone which this study is more focus for threat assessment. Other than that, author in Adewole, Anuar, & Kamsin (2016) suggested a framework to assess the risk of microblogging comments into six (6) different levels; extremely normal, normal, low risk, medium risk, high risk, extremely harmful. This framework that combined multinomial NB and kNN consist of spam identification and risk assessment. However, this study did not provide proposal for SMS messages risk measurement. Expected as one of the complement safeguard to control the potential loss cause by spam messages, this RiCCA model is proposed as the following.

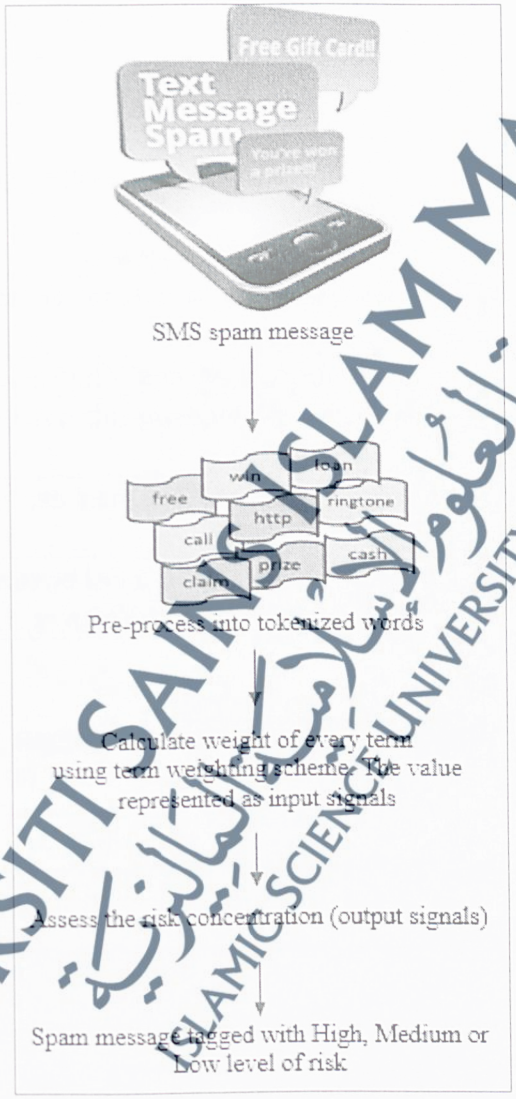


Figure 1: The flow process of functionality for the proposed model, RiCCA

The phase of determination of spam's severity level is divided into three (3) main risk category:

i. High – spam message could be expected to have a **severe or catastrophic** adverse effect;
ii. Medium – spam message could be expected to have a **serious** adverse effect; and
iii. Low – spam message could be expected to have a **limited or negligible** adverse effect.

As in a common risk assessment, the risk level of a threat is measured via the function of impact and likelihood of identified threat that exploiting vulnerabilities. Basically, risk assessment is the critical phase which the evaluation of risk will influence the decision on how to deal with it.

Validation of necessity:

Based on the aforementioned gap analysis and a model proposed (RiCCA) in this study, please circle the numbers corresponding to your degree of agreement to each item with the denoted scale.

1 Strongly disagree
2 Disagree
3 Neutral
4 Agree
5 Strongly agree

No.	Questions	Scale				
1.	The proposed model is reliable in assisting users to detect malicious messages.	1	2	3	4	5
2.	The proposed model is feasible in daily use as life routine.	1	2	3	4	5
3.	It is a good thing to have this proposed model as mobile apps for daily use.	1	2	3	4	5
4.	The proposed model can increase awareness on spam's impact among users.	1	2	3	4	5
5.	It is potentially to expand the usable of this proposed model to other platforms such as email and social media.	1	2	3	4	5

Please state any of your **suggestion** regarding to this matter. Kindly please justify your suggestion.

Thank you for your co-operation.

Date: .....

References:

Abdulhamid, S. M., Abd Latiff, M. S., Chiroma, H., Osho, O., Abdul-Salaam, G., Abu Bakar, A. I., & Herawan, T. (2017). A Review on Mobile SMS Spam Filtering Techniques. *IEEE Access*, 1–21. https://doi.org/10.1109/ACCESS.2017.2666785

Adewole, K. S., Anuar, N. B., & Kamsin, A. (2016). Ensemble Based Streaming Framework for Spam Detection and Risk Assessment in Microblogging Social Networks. In *International Conference on Computer Science and Computational Mathematics (ICCSCM)*.

Choudhary, N., & Jain, A. K. (2017). Towards Filtering of SMS Spam Messages Using Machine Learning Based Technique. In *International Conference on Advanced Informatics for Computing Research (ICAICR)* (Vol. 712, pp. 18–30). https://doi.org/10.1007/978-981-10-5780-9

Lota, L. N., & Hossain, B. M. M. (2017). A Systematic Literature Review on SMS Spam Detection Techniques. *International Journal of Information Technology and Computer Science*, *9*(7), 42–50. https://doi.org/10.5815/ijitcs.2017.07.05

M.El-Alfy, E.-S., & Alhasan, A. A. (2016). Spam Filtering Framework for Multimodal Mobile Communication Based on Dendritic Cell Algorithm. In *Future Generation Computer Systems* (pp. 1–40). Elsevier B.V. https://doi.org/10.1016/j.future.2016.02.018

Mosquera, A., Aouad, L., Grzonkowski, S., & Morss, D. (2014). On Detecting Messaging Abuse in Short Text Messages Using Linguistic and Behavioral Patterns. *Social Media Intelligence*, 1–10. Retrieved from http://arxiv.org/abs/1408.3934

Sulaiman, N. F., & Jali, M. Z. (2015). A New SMS Spam Detection Method Using Both Content-Based and Non Content-Based Features. In *Advanced Computer and Communication Engineering Technology* (pp. 505–514).

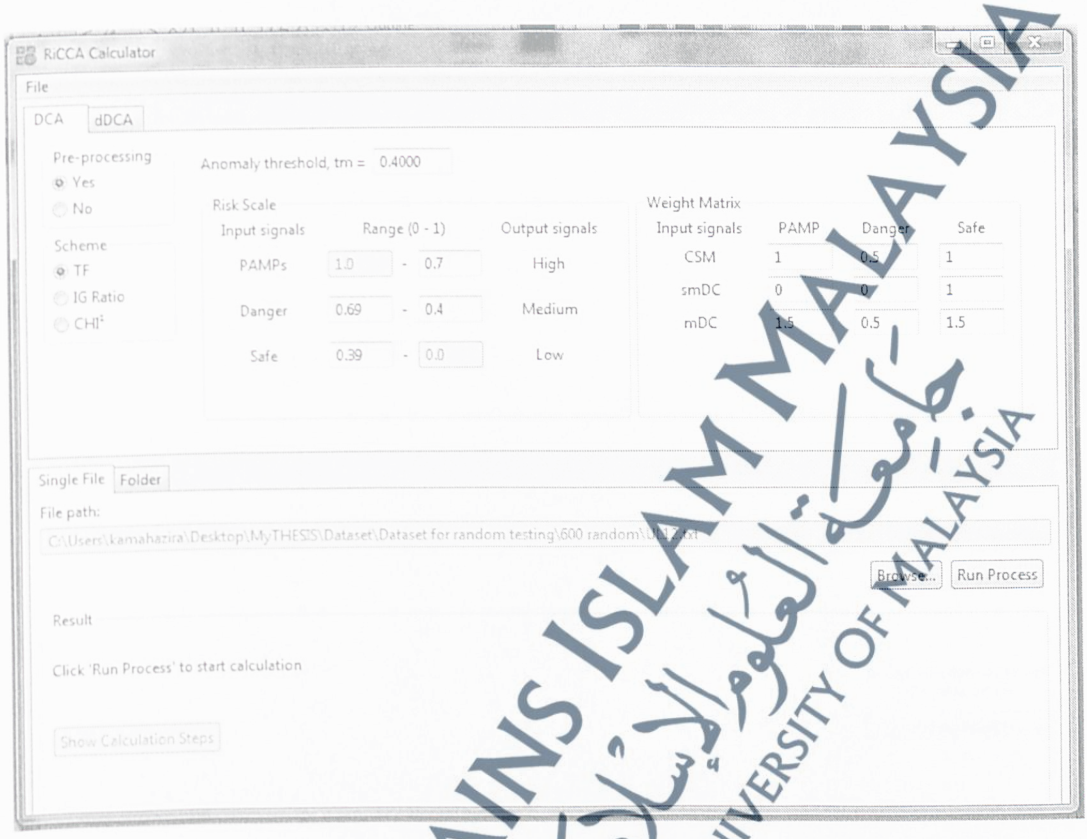
Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A Risk Assessment Method for Smartphones. In *International Information Security Conference* (pp. 443–456).

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: An Assessment of Threats Against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297–307.

-END OF QUESTIONNAIRE-

APPENDIX G
Interface Of RiCCA Prototype

DCA Interface



dDCA Interface