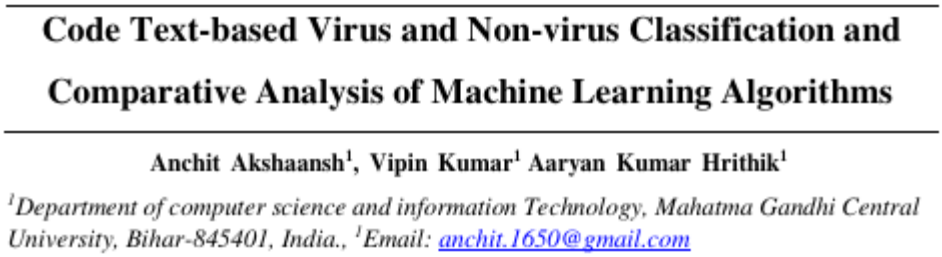
Erratum

Article Information
Original Paper Title: Code Text-based Virus and Non-virus Classification and Comparative Analysis of Machine Learning Algorithms,
Book/Proceedings Title: International Conference on Recent and Future Trends in Smart Electronics System and Manufacturing - (SESMIC 2022)
Series Title: River Publishers Series in Proceedings
Authors: Anchit Akshaansh[1], Vipin Kumar[1] Aaryan Kumar Hrithik[1]
DOI: 10.13052/rp-9788770229852
e-ISBN: 9788770229852

Correction 1: Author Details
Original Text and Image:

Anchit Akshaansh[1], Vipin Kumar[1] Aaryan Kumar Hrithik[1]
[1]Department of computer science and information Technology, Mahatma Gandhi Central University, Bihar-845401, India.
[1]Email: anchit.1650@gmail.com



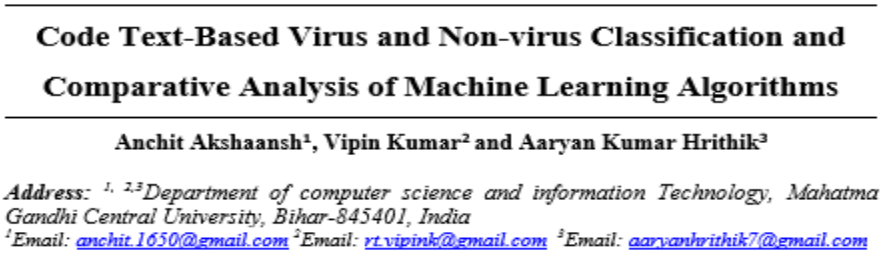
Code Text-based Virus and Non-virus Classification and Comparative Analysis of Machine Learning Algorithms

Anchit Akshaansh[1], Vipin Kumar[1] Aaryan Kumar Hrithik[1]

[1]Department of computer science and information Technology, Mahatma Gandhi Central University, Bihar-845401, India., [1]Email: anchit.1650@gmail.com

Corrected Text and Image:

Anchit Akshaansh[1], Vipin Kumar[2] and Aaryan Kumar Hrithik[3]
Address: [1], [2], [3]Department of Computer Science and Information Technology, Mahatma Gandhi Central University, Bihar-845401, India
[1]Email: anchit.1650@gmail.com | [2]Email: rt.vipink@gmail.com | [3]Email: aaryanhrithik7@gmail.com



Code Text-Based Virus and Non-virus Classification and Comparative Analysis of Machine Learning Algorithms

Anchit Akshaansh[1], Vipin Kumar[2] and Aaryan Kumar Hrithik[3]

Address: [1, 2,3]*Department of computer science and information Technology, Mahatma Gandhi Central University, Bihar-845401, India*
[1]*Email: anchit.1650@gmail.com* [2]*Email: rt.vipink@gmail.com* [3]*Email: aaryanhrithik7@gmail.com*

Correction 2: Biographies
Original Text and Image:
Biographies



Anchit Akshaansh is currently working as Assistant Professor in the Department of Computer Science and Engineering, Meerut Institute of Technology, Meerut, UP India. Author has completed his B.Tech (2017) in Computer Science and Engineering form Biju Patnaik University of Technology, Rourkela, Odisha and Received M.Tech (2022) in Computer Science and Engineering from Mahatma Gandhi Central University,Motihari Bihar. He is focused in CyberSecurity, Machine Learning, Deep Learning Text Mining, Image Processing etc. Author Aim is to Develop Machine and Deep Learning Techniques for Cybersecurity and has in field of Image Processing. Author is looking further for PhD in his interest field.



Dr. Vipin Kumar is currently working as an Assistant Professor in the Department of Computer Science and Information Technology, Mahatma Gandhi Central University, Bihar India. Author has Completed B.Tech (2009) in Computer Science and Engineering from National Institute of Technology Allahabad (NITA), UP, India. In addition, he has received M.Tech (2012) and PhD (2015) in Computer Science from JNU.New Delhi, India. Teaching and Research areas are Machine Learning, Data Science, Data Mining, Deep Learning and Big Analytics. Seven (7) Years of Teaching Experience for UG, PG and PhD. He teaches Machine Learning, Data Mining, Data Science Soft Computing, Text Mining, Sentiment Analysis, Data Base Management Systems, Data Structure, Python Programming, C Programming, Combinatorial Optimization, etc. His associated and reputed journals are Information Science, Information Fusion, etc. and review several research papers. He is focused on research to Develop Machine Learning Techniques for a High-Dimensional Dataset for Classification Tasks, Image processing Using Machine Learning and Deep Learning for Seeds & Leaf Detection in Agriculture Fields and Semi-Supervised Learning Tasks for Remote Sensing, Developing Algorithms for Multi-View Learning for the Classification Task.



Aaryan Kumar Hrithik has completed his B.Tech (2019) in Computer Science and Engineering from I. K Gujral Punjab Technical University, Jalandhar and Received M.Tech (2022) in Computer Science and Engineering from Mahatma Gandhi Central University, Motihari Bihar. He is focused in CyberSecurity, Machine Learning, Deep Learning, Text Mining and Image Processing etc. Author has Presented and Published 3 Paper in Machine and Deep Learning



Anchit Akshaansh is currently working as Assistant Professor in the Department of Computer Science and Engineering, Meerut Institute of Technology, Meerut, UP India. Author has completed his B. Tech (2017) in Computer Science and Engineering form Biju Patnaik University of Technology, Rourkela, Odisha and Received M. Tech (2022) in Computer Science and Engineering from Mahatma Gandhi Central University, Motihari Bihar.



Vipin Kumar is currently working as an Assistant Professor in the Department of Computer Science and Information Technology, Mahatma Gandhi Central University, Bihar India. Author has Completed B. Tech (2009) in Computer Science and Engineering from National Institute of Technology Allahabad (NITA), UP, India. In addition, he has received M. Tech (2012) and PhD (2015) in Computer Science from JNU New Delhi, India. Teaching and Research areas are Machine Learning, Data Science, Data Mining, Deep Learning and Big Analytics.



Aaryan Kumar Hrithik has completed his B. Tech (2019) in Computer Science and Engineering from I. K Gujral Punjab Technical University, Jalandhar and Received M. Tech (2022) in Computer Science and Engineering from Mahatma Gandhi Central University, Motihari Bihar. He is focused in CyberSecurity, Machine Learning, Deep Learning, Text Mining and Image Processing etc. Author has Presented and Published 3 Paper in Machine and Deep Learning.

Corrected Text and Image:

Biographies



Anchit Akshaansh is currently working as Assistant Professor in the Department of Computer Science and Engineering, Meerut Institute of Technology, Meerut, UP India. Author has completed his B.Tech (2017) in Computer Science and Engineering form Biju Patnaik University of Technology, Rourkela, Odisha and Received M.Tech (2022) in Computer Science and Engineering from Mahatma Gandhi Central University,Motihari Bihar. He is focused in CyberSecurity, Machine Learning, Deep Learning Text Mining, Image Processing etc. Author Aim is to Develop Machine and Deep Learning Techniques for Cybersecurity and has in field of Image Processing. Author is looking further for PhD in his interest field.



Dr. Vipin Kumar is currently working as an Assistant Professor in the Department of Computer Science and Information Technology, Mahatma Gandhi Central University, Bihar India. Author has Completed B.Tech (2009) in Computer Science and Engineering from National Institute of Technology Allahabad (NITA), UP, India. In addition, he has received M.Tech (2012) and PhD (2015) in Computer Science from JNU.New Delhi, India. Teaching and Research areas are Machine Learning, Data Science, Data Mining, Deep Learning and Big Analytics. Seven (7) Years of Teaching Experience for UG, PG and PhD. He teaches Machine Learning, Data Mining, Data Science Soft Computing, Text Mining, Sentiment Analysis, Data Base Management Systems, Data Structure, Python Programming, C Programming, Combinatorial Optimization, etc. His associated and reputed journals are Information Science, Information Fusion, etc. and review several research papers. He is focused on research to Develop Machine Learning Techniques for a High-Dimensional Dataset for Classification Tasks, Image processing Using Machine Learning and Deep Learning for Seeds & Leaf Detection in Agriculture Fields and Semi-Supervised Learning Tasks for Remote Sensing, Developing Algorithms for Multi-View Learning for the Classification Task.



Aaryan Kumar Hrithik has completed his B.Tech (2019) in Computer Science and Engineering from I. K Gujral Punjab Technical University, Jalandhar and Received M.Tech (2022) in Computer Science and Engineering from Mahatma Gandhi Central University, Motihari Bihar. He is focused in CyberSecurity, Machine Learning, Deep Learning, Text Mining and Image Processing etc. Author has Presented and Published 3 Paper in Machine and Deep Learning

Biographies



Aashit Akshansh is currently working as Assistant Professor in the Department of Computer Science and Engineering, Meerut Institute of Technology, Meerut, UP India. Author has completed his B.Tech (2017) in Computer Science and Engineering form Biju Patnaik University of Technology, Rourkela, Odisha and Received M.Tech (2022) in Computer Science and Engineering from Mahatma Gandhi Central University,Motihari Bihar. He is focused in CyberSecurity, Machine Learning, Deep Learning Text Mining, Image Processing etc. Author Aim is to Develop Machine and Deep Learning Techniques for Cybersecurity and has in field of Image Processing. Author is looking further for PhD in his interest field.



Dr. Vipin Kumar is currently working as an Assistant Professor in the Department of Computer Science and Information Technology, Mahatma Gandhi Central University, Bihar India. Author has Completed B.Tech (2009) in Computer Science and Engineering from National Institute of Technology Allahabad (NITA), UP, India. In addition, he has received M.Tech (2012) and PhD (2015) in Computer Science from JNU New Delhi, India. Teaching and Research areas are Machine Learning, Data Science, Data Mining, Deep Learning and Big Analytics. Seven (7) Years of Teaching Experience for UG, PG and PhD. He teaches Machine Learning, Data Mining, Data Science Soft Computing, Text Mining, Sentiment Analysis, Data Base Management Systems, Data Structure, Python Programming, C Programming, Combinatorial Optimization, etc. His associated and reputed journals are Information Science, Information Fusion, etc. and review several research papers. He is focused on research to Develop Machine Learning Techniques for a High-Dimensional Dataset for Classification Tasks, Image processing Using Machine Learning and Deep Learning for Seeds & Leaf Detection in Agriculture Fields and Semi-Supervised Learning Tasks for Remote Sensing, Developing Algorithms for Multi-View Learning for the Classification Task.



Aaryan Kumar Rithik has completed his B.Tech (2019) in Computer Science and Engineering from I. K. Gujral Punjab Technical University, Jalandhar and Received M.Tech (2022) in Computer Science and Engineering from Mahatma Gandhi Central University, Motihari Bihar. He is focused in CyberSecurity, Machine Learning, Deep Learning, Text Mining and Image Processing etc. Author has Presented and Published 3 Paper in Machine and Deep Learning

Correction 3: References

Original Text:

D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," Technology Innovation Management Review, vol. 4, no. 10, 2014.

R. Anderson and T. Moore, "The economics of information security," Science (1979), vol. 314, no. 5799, pp. 610–613, 2006.

N. Idika and A. P. Mathur, "A survey of malware detection techniques," Purdue University, vol. 48, no. 2, pp. 32–46, 2007.

M. Kaeo, Designing network security. Cisco Press, 2004.

A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," Wiley Interdiscip Rev Data Min Knowl Discov, vol. 9, no. 4, p. e1306, 2019.

A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," Wiley Interdiscip Rev Data Min Knowl Discov, vol. 9, no. 4, p. e1306, 2019.

J.-Y. Wu, “Learning analytics on structured and unstructured heterogeneous data sources: Perspectives from procrastination, help-seeking, and machine-learning defined cognitive engagement,” Comput Educ, vol. 163, p. 104066, 2021.

I. F. Kilincer, F. Ertam, and A. Sengur, “Machine learning methods for cyber security intrusion detection: Datasets and comparative study,” Computer Networks, vol. 188, p. 107840, 2021.

S. Ismail and H. Reza, “Evaluation of Na\"\ive Bayesian Algorithms for Cyber- Attacks Detection in Wireless Sensor Networks,” in 2022 IEEE World AI IoT Congress (AIIoT), 2022, pp. 283–289.
G. Wang, D. Tse, Y. Cui, and H. Jiang, “An Exploratory Study on Sustaining Cyber Security Protection through SETA Implementation,” Sustainability, vol. 14, no. 14, p. 8319, 2022.

S. Ismail and H. Reza, “Evaluation of Na\"\ive Bayesian Algorithms for Cyber- Attacks Detection in Wireless Sensor Networks,” in 2022 IEEE World AI IoT Congress (AIIoT), 2022, pp. 283–289.

H. Berry, M. A. Abdel-Malek, and A. S. Ibrahim, “A Machine Learning Approach for Combating Cyber Attacks in Self-Driving Vehicles,” in SoutheastCon 2021, 2021, pp. 1–3.

M. Choubisa, R. Doshi, N. Khatri, and K. K. Hiran, “A Simple and Robust Approach of Random Forest for Intrusion Detection System in Cyber Security,” in 2022 International Conference on IoT and Blockchain Technology (ICIBT), 2022, pp. 1– 5.

S. S. A. Krishnan, A. N. Sabu, P. P. Sajan, and A. L. Sreedeep, “SQL Injection Detection Using Machine Learning,” REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS, vol. 11, no. 3, pp. 300–310, 2021.

S. H. Majidi, S. Hadayeghparast, and H. Karimipour, “FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid,” International Journal of Critical Infrastructure Protection, vol. 37, p. 100508, 2022.

C. Florackis, C. Louca, R. Michaely, and M. Weber, “Cybersecurity risk,” 2020.
S. Skryl et al., “Assessing the response timeliness to threats as an important element of cybersecurity: Theoretical foundations and research model,” in Conference on Creativity in Intelligent Technologies and Data Science, 2019, pp. 258–269.

P. P. Kaur and S. Singh, “Classification of Herbal Plant and Comparative Analysis of SVM and KNN Classifier Models on the Leaf Features Using Machine Learning,” pp. 227–239, 2021, doi: 10.1007/978-98116-1048-6_17.

E. Burnaev and D. Smolyakov, “One-class SVM with privileged information and its application to malware detection,” in 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW), 2016, pp. 273–280.

[1] J. L. Leevy, J. Hancock, R. Zuech, and T. M. Khoshgoftaar, “Detecting cybersecurity attacks across different network features and learners,” *J Big Data*, vol. 8, no. 1, pp. 1–29, 2021.

[2] T. T. Teoh, G. Chiew, E. J. Franco, P. C. Ng, M. P. Benjamin, and Y. J. Goh, “Anomaly detection in cyber security attacks on networks using MLP deep learning,” in *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2018, pp. 1–5.

[3] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, “Autoencoder-based feature learning for cyber security applications,” in *2017 International joint conference on neural networks (IJCNN)*, 2017, pp. 3854–3861.

[4] A. Mitra, Digital security: cyber terror and cyber security. Infobase Publishing, 2010.

[5] P. Szor, The Art of Computer Virus Research and Defense: ART COMP VIRUS RES DEFENSE _p1. Pearson Education, 2005.

[6] M. T. Signes-Pont, A. Cortés-Castillo, H. Mora-Mora, and J. Szymanski, “Modelling the malware propagation in mobile computer devices,” *Comput Secur*, vol. 79, pp. 80–93, 2018.

[7] T. B. Slayton, “Ransomware: The virus attacking the healthcare industry,” *Journal of Legal Medicine*, vol. 38, no. 2, pp. 287–311, 2018.

[8] A. Riyana, B. Santoso, and R. Hartono, “Trojan malware analysis using reverse engineering method in Windows 7,” *Technium Soc. Sci. J.*, vol. 30, p. 775, 2022.

[9] R. Rawat, V. Mahor, S. Chirgaiya, R. N. Shaw, and A. Ghosh, “Analysis of darknet traffic for criminal activities detection using TF-IDF and light gradient boosted machine learning algorithm,” in *Innovations in electrical and electronic engineering*, Springer, 2021, pp. 671–681.

7. REFERENCES

D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," Technology Innovation Management Review, vol. 4, no. 10, 2014.

R. Anderson and T. Moore, "The economics of information security," Science (1979), vol. 314, no. 5799, pp. 610–613, 2006.

N. Idika and A. P. Mathur, "A survey of malware detection techniques," Purdue University, vol. 48, no. 2, pp. 32–46, 2007.

M. Kaeo, Designing network security. Cisco Press, 2004.

A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," Wiley Interdiscip Rev Data Min Knowl Discov, vol. 9, no. 4, p. e1306, 2019.

A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," Wiley Interdiscip Rev Data Min Knowl Discov, vol. 9, no. 4, p. e1306, 2019.

J.-Y. Wu, "Learning analytics on structured and unstructured heterogeneous data sources: Perspectives from procrastination, help-seeking, and machine-learning defined cognitive engagement," Comput Educ, vol. 163, p. 104066, 2021.

I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," Computer Networks, vol. 188, p. 107840, 2021.

S. Ismail and H. Reza, "Evaluation of Na\"ive Bayesian Algorithms for Cyber- Attacks Detection in Wireless Sensor Networks," in 2022 IEEE World AI IoT Congress (AIIoT), 2022, pp. 283–289.

G. Wang, D. Tse, Y. Cui, and H. Jiang, "An Exploratory Study on Sustaining Cyber Security Protection through SETA Implementation," Sustainability, vol. 14, no. 14, p. 8319, 2022.

S. Ismail and H. Reza, "Evaluation of Na\"ive Bayesian Algorithms for Cyber- Attacks Detection in Wireless Sensor Networks," in 2022 IEEE World AI IoT Congress (AIIoT), 2022, pp. 283–289.

H. Berry, M. A. Abdel-Malek, and A. S. Ibrahim, "A Machine Learning Approach for Combating Cyber Attacks in Self-Driving Vehicles," in SoutheastCon 2021, 2021, pp. 1–3.

M. Choubisa, R. Doshi, N. Khatri, and K. K. Hiran, "A Simple and Robust Approach of Random Forest for Intrusion Detection System in Cyber Security," in 2022 International Conference on IoT and Blockchain Technology (ICIBT), 2022, pp. 1– 5.

S. S. A. Krishnan, A. N. Sabu, P. P. Sajan, and A. L. Sreedeep, "SQL Injection Detection Using Machine Learning," REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS, vol. 11, no. 3, pp. 300–310, 2021.

S. H. Majidi, S. Hadayeghparast, and H. Karimipour, "FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid," International Journal of Critical Infrastructure Protection, vol. 37, p. 100508, 2022.

C. Florackis, C. Louca, R. Michaely, and M. Weber, "Cybersecurity risk," 2020.

S. Skryl et al., "Assessing the response timeliness to threats as an important element of cybersecurity: Theoretical foundations and research model," in Conference on Creativity in Intelligent Technologies and Data Science, 2019, pp. 258–269.

P. P. Kaur and S. Singh, "Classification of Herbal Plant and Comparative Analysis of SVM and KNN Classifier Models on the Leaf Features Using Machine Learning," pp. 227–239, 2021, doi: 10.1007/978-981-16-1048-6_17.

E. Burnaev and D. Smolyakov, "One-class SVM with privileged information and its application to malware detection," in 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW), 2016, pp. 273–280.

[1] J. L. Leevy, J. Hancock, R. Zuech, and T. M. Khoshgoftaar, "Detecting cybersecurity attacks across different network features and learners," J Big Data, vol. 8, no. 1, pp. 1–29, 2021.

[2] T. T. Teoh, G. Chiew, E. J. Franco, P. C. Ng, M. P. Benjamin, and Y. J. Goh, "Anomaly detection in cyber security attacks on networks using MLP deep learning," in 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2018, pp. 1–5.

[3] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, "Autoencoder- based feature learning for cyber security applications," in 2017 International joint conference on neural networks (IJCNN), 2017, pp. 3854–3861.

[4] A. Mitra, Digital security: cyber terror and cyber security. Infobase Publishing, 2010.

[5] P. Szor, The Art of Computer Virus Research and Defense: ART COMP VIRUS RES DEFENSE _p1. Pearson Education, 2005.

[6] M. T. Signes-Pont, A. Cortés-Castillo, H. Mora-Mora, and J. Szymanski, "Modelling the malware propagation in mobile computer devices," Comput Secur, vol. 79, pp. 80–93, 2018.

[7] T. B. Slayton, "Ransomware: The virus attacking the healthcare industry," Journal of Legal Medicine, vol. 38, no. 2, pp. 287–311, 2018.

[8] A. Riyanto, B. Santoso, and R. Hartono, "Trojan malware analysis using reverse engineering method in Windows 7," Technium Soc. Sci. J., vol. 30, p. 775, 2022.

[9] R. Rawat, V. Mahor, S. Chirgaiya, R. N. Shaw, and A. Ghosh, "Analysis of darknet traffic for criminal activities detection using TF-IDF and light gradient boosted machine learning algorithm," in Innovations in electrical and electronic engineering, Springer, 2021, pp. 671–681.

Corrected Text and Image:

[1] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technology Innovation Management Review*, vol. 4, no. 10, 2014.

[2] R. Anderson and T. Moore, "The economics of information security," *Science (1979)*, vol. 314, no. 5799, pp. 610–613, 2006.

[3] N. Idika and A. P. Mathur, "A survey of malware detection techniques," *Purdue University*, vol. 48, no. 2, pp. 32–46, 2007.

[4] M. Kaeo, *Designing network security*. Cisco Press, 2004.

[5] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *Wiley Interdiscip Rev Data Min Knowl Discov*, vol. 9, no. 4, p. e1306, 2019.

[6] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *Wiley Interdiscip Rev Data Min Knowl Discov*, vol. 9, no. 4, p. e1306, 2019.

[7] J.-Y. Wu, "Learning analytics on structured and unstructured heterogeneous data sources: Perspectives from procrastination, help-seeking, and machine-learning defined cognitive engagement," *Comput Educ*, vol. 163, p. 104066, 2021.

[8] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol. 188, p. 107840, 2021.

[9] S. Ismail and H. Reza, "Evaluation of Na\"\ive Bayesian Algorithms for Cyber-Attacks Detection in Wireless Sensor Networks," in *2022 IEEE World AI IoT Congress (AIIoT)*, 2022, pp. 283–289.

[10] G. Wang, D. Tse, Y. Cui, and H. Jiang, "An Exploratory Study on Sustaining Cyber Security Protection through SETA Implementation," *Sustainability*, vol. 14, no. 14, p. 8319, 2022.

[11] S. Ismail and H. Reza, "Evaluation of Na\"\ive Bayesian Algorithms for Cyber-Attacks Detection in Wireless Sensor Networks," in *2022 IEEE World AI IoT Congress (AIIoT)*, 2022, pp. 283–289.

[12] H. Berry, M. A. Abdel-Malek, and A. S. Ibrahim, "A Machine Learning Approach for Combating Cyber Attacks in Self-Driving Vehicles," in *SoutheastCon 2021*, 2021, pp. 1–3.

[13] M. Choubisa, R. Doshi, N. Khatri, and K. K. Hiran, "A Simple and Robust Approach of Random Forest for Intrusion Detection System in Cyber Security," in *2022 International Conference on IoT and Blockchain Technology (ICIBT)*, 2022, pp. 1–5.

[14] S. S. A. Krishnan, A. N. Sabu, P. P. Sajan, and A. L. Sreedeep, "SQL Injection Detection Using Machine Learning," *REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS*, vol. 11, no. 3, pp. 300–310, 2021.

[15] S. H. Majidi, S. Hadayeghparast, and H. Karimipour, "FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid," *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100508, 2022.

[16] C. Florackis, C. Louca, R. Michaely, and M. Weber, "Cybersecurity risk," 2020.

[17] S. Skryl *et al.*, "Assessing the response timeliness to threats as an important element of cybersecurity: Theoretical foundations and research model," in *Conference on Creativity in Intelligent Technologies and Data Science*, 2019, pp. 258–269.

[18] P. P. Kaur and S. Singh, "Classification of Herbal Plant and Comparative Analysis of SVM and KNN Classifier Models on the Leaf Features Using Machine Learning," pp. 227–239, 2021, doi: 10.1007/978-981-16-1048-6_17.

[19] E. Burnaev and D. Smolyakov, "One-class SVM with privileged information and its application to malware detection," in *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, 2016, pp. 273–280.

[20] J. L. Leevy, J. Hancock, R. Zuech, and T. M. Khoshgoftaar, "Detecting cybersecurity attacks across different network features and learners," *J Big Data*, vol. 8, no. 1, pp. 1–29, 2021.

[21] T. T. Teoh, G. Chiew, E. J. Franco, P. C. Ng, M. P. Benjamin, and Y. J. Goh, "Anomaly detection in cyber security attacks on networks using MLP deep learning," in *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2018, pp. 1–5.

[22] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, "Autoencoder-based feature learning for cyber security applications," in *2017 International joint conference on neural networks (IJCNN)*, 2017, pp. 3854–3861.

[23] A. Mitra, Digital security: cyber terror and cyber security. Infobase Publishing, 2010.

[24] P. Szor, The Art of Computer Virus Research and Defense: ART COMP VIRUS RES DEFENSE _p1. Pearson Education, 2005.

[25] M. T. Signes-Pont, A. Cortés-Castillo, H. Mora-Mora, and J. Szymanski, "Modelling the malware propagation in mobile computer devices," *Comput Secur*, vol. 79, pp. 80–93, 2018.

[26] T. B. Slayton, "Ransomware: The virus attacking the healthcare industry," *Journal of Legal Medicine*, vol. 38, no. 2, pp. 287–311, 2018.

[27] A. Riyana, B. Santoso, and R. Hartono, "Trojan malware analysis using reverse engineering method in Windows 7," *Technium Soc. Sci. J.*, vol. 30, p. 775, 2022.

[28] R. Rawat, V. Mahor, S. Chirgaiya, R. N. Shaw, and A. Ghosh, "Analysis of darknet traffic for criminal activities detection using TF-IDF and light gradient boosted machine learning algorithm," in *Innovations in electrical and electronic engineering*, Springer, 2021, pp. 671–681.

7. REFERENCES

[1] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technology Innovation Management Review*, vol. 4, no. 10, 2014.

[2] R. Anderson and T. Moore, "The economics of information security," *Science (1979)*, vol. 314, no. 5799, pp. 610–613, 2006.

[3] N. Idika and A. P. Mathur, "A survey of malware detection techniques," *Purdue University*, vol. 48, no. 2, pp. 32–46, 2007.

[4] M. Kaeo, *Designing network security*. Cisco Press, 2004.

[5] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *Wiley Interdiscip Rev Data Min Knowl Discov*, vol. 9, no. 4, p. e1306, 2019.

[6] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *Wiley Interdiscip Rev Data Min Knowl Discov*, vol. 9, no. 4, p. e1306, 2019.

[7] J.-Y. Wu, "Learning analytics on structured and unstructured heterogeneous data sources: Perspectives from procrastination, help-seeking, and machine-learning defined cognitive engagement," *Comput Educ*, vol. 163, p. 104066, 2021.

[8] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol. 188, p. 107840, 2021.

[9] S. Ismail and H. Reza, "Evaluation of Na\'"\ive Bayesian Algorithms for Cyber-Attacks Detection in Wireless Sensor Networks," in *2022 IEEE World AI IoT Congress (AIIoT)*, 2022, pp. 283–289.

[10] G. Wang, D. Tse, Y. Cui, and H. Jiang, "An Exploratory Study on Sustaining Cyber Security Protection through SETA Implementation," *Sustainability*, vol. 14, no. 14, p. 8319, 2022.

[11] S. Ismail and H. Reza, "Evaluation of Na\'"\ive Bayesian Algorithms for Cyber-Attacks Detection in Wireless Sensor Networks," in *2022 IEEE World AI IoT Congress (AIIoT)*, 2022, pp. 283–289.

[12] H. Berry, M. A. Abdel-Malek, and A. S. Ibrahim, "A Machine Learning Approach for Combating Cyber Attacks in Self-Driving Vehicles," in *SoutheastCon 2021*, 2021, pp. 1–3.

[13] M. Choubisa, R. Doshi, N. Khatri, and K. K. Hiran, "A Simple and Robust Approach of Random Forest for Intrusion Detection System in Cyber Security," in *2022 International Conference on IoT and Blockchain Technology (ICIBT)*, 2022, pp. 1–5.

[14] S. S. A. Krishnan, A. N. Sabu, P. P. Sajan, and A. L. Sreedeep, "SQL Injection Detection Using Machine Learning," *REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS*, vol. 11, no. 3, pp. 300–310, 2021.

[15] S. H. Majidi, S. Hadayeghparast, and H. Karimipour, "FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid," *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100508, 2022.

[16] C. Florackis, C. Louca, R. Michaely, and M. Weber, "Cybersecurity risk," 2020.

[17] S. Skryl *et al.*, "Assessing the response timeliness to threats as an important element of cybersecurity: Theoretical foundations and research model," in *Conference on Creativity in Intelligent Technologies and Data Science*, 2019, pp. 258–269.

[18] P. P. Kaur and S. Singh, "Classification of Herbal Plant and Comparative Analysis of SVM and KNN Classifier Models on the Leaf Features Using Machine Learning," pp. 227–239, 2021, doi: 10.1007/978-981-16-1048-6_17.

[19] E. Burnaev and D. Smolyakov, "One-class SVM with privileged information and its application to malware detection," in *2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW)*, 2016, pp. 273–280.

[20] J. L. Leevy, J. Hancock, R. Zuech, and T. M. Khoshgoftaar, "Detecting cybersecurity attacks across different network features and learners," *J Big Data*, vol. 8, no. 1, pp. 1–29, 2021.

[21] T. T. Teoh, G. Chiew, E. J. Franco, P. C. Ng, M. P. Benjamin, and Y. J. Goh, "Anomaly detection in cyber security attacks on networks using MLP deep learning," in *2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2018, pp. 1–5.

[22] M. Yousefi-Azar, V. Varadharajan, L. Hamey, and U. Tupakula, "Autoencoder-based feature learning for cyber security applications," in *2017 International joint conference on neural networks (IJCNN)*, 2017, pp. 3854–3861.

[23] A. Mitra, Digital security: cyber terror and cyber security. Infobase Publishing, 2010.

[24] P. Szor, The Art of Computer Virus Research and Defense: ART COMP VIRUS RES DEFENSE _p1. Pearson Education, 2005.

[25] M. T. Signes-Pont, A. Cortés-Castillo, H. Mora-Mora, and J. Szymanski, "Modelling the malware propagation in mobile computer devices," *Comput Secur*, vol. 79, pp. 80–93, 2018.

[26] T. B. Slayton, "Ransomware: The virus attacking the healthcare industry," *Journal of Legal Medicine*, vol. 38, no. 2, pp. 287–311, 2018.

[27] A. Riyana, B. Santoso, and R. Hartono, "Trojan malware analysis using reverse engineering method in Windows 7," *Technium Soc. Sci. J.*, vol. 30, p. 775, 2022.

[28] R. Rawat, V. Mahor, S. Chirgaiya, R. N. Shaw, and A. Ghosh, "Analysis of darknet traffic for criminal activities detection using TF-IDF and light gradient boosted machine learning algorithm," in *Innovations in electrical and electronic engineering*, Springer, 2021, pp. 671–681.