National College of Ireland

Configuration Manual

MSc Research Project
Programme Name: - MSC in Artificial intelligence

Shaik Junaid
Student ID: x23354631

School of Computing
National College of Ireland

Supervisor: Lavish Thomas

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Shaik Junaid

Student ID: x23354631

Programme: MSC in Artificial intelligence **Year:** 2025

Module: Practicum 2

Lecturer:

Submission Due Date: 15/09/2025

Project Title: Intelligent Anomaly Detection in Network Traffic Using Advanced Machine Learning Techniques

Word Count: 6113 **Page Count:** 19

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: SHAIK JUNAID

Date: 15/09/2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	

Date:	
Penalty Applied (if applicable):	

Configuration Manual

Shaik Junaid
Student ID: x23354631

1. Introduction

The section provides the target of the research, which is to improve network anomaly detection using machine learning, and addresses the critical issues, including class imbalance, supporting resources, and adaptation requirements.

2. Literature Review

This section provides a review of existing literature on ML-based anomaly detection in terms of techniques, scalability, adaptability, and real-world applicability challenges.

3. Methodology

In this part, the philosophy, approach, design, method of collecting, and analyzing data toward evaluating ML model accuracy in detecting anomalies are discussed.

4. Data Analysis

In this section, the results of the data preparation, preprocessing, model building, and performance are represented and compared.

5. Discussion

This section contains an explanation of the findings in the context of the literature, model comparison, sustainability challenges, and the management of the class imbalance.

6. Conclusion and Recommendations

This section summarizes the main findings of the study, relates them to the objectives, and is accompanied by recommendations, limitations, and future research problems.

References

Abdullah, M.M., Khan, H., Farhan, M. and Khadim, F., 2024. An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), pp.502-527.

Adhikari, D., Jiang, W., Zhan, J., Rawat, D.B. and Bhattarai, A., 2024. Recent advances in anomaly detection in Internet of Things: Status, challenges, and perspectives. Computer Science Review, 54, p.100665.

Alsaleh, N., Alnanih, R. and Alowidi, N., 2025. Hybrid Deep Learning Approach for Automating App Review Classification: Advancing Usability Metrics Classification with an Aspect-Based Sentiment Analysis Framework. *Computers, Materials & Continua*, *82*(1).

Altalhan, M., Algarni, A. and Alouane, M.T.H., 2025. Imbalanced Data problem in Machine Learning: A review. *IEEE Access*.

Azam, Z., Islam, M.M. and Huda, M.N., 2023. Comparative analysis of intrusion detection systems and machine learning-based model analysis through decision tree. IEEE Access, 11, pp.80348-80391.

Becker, T., Rousseau, A.J., Geubbelmans, M., Burzykowski, T. and Valkenborg, D., 2023. Decision trees and random forests. American Journal of Orthodontics and Dentofacial Orthopedics, 164(6), pp.894-897.

Boesch, G., (2024) What is Pattern Recognition? A Gentle Introduction. https://viso.ai/deeplearning/patternrecognition/#:~:text=Pattern%20recognition%20is%20the%20ability,artificial%20intelligenc e%20(AI)%20systems.

Chen, S., Huang, Z., Zuo, Z. and Guo, X., 2016, October. A feature selection method for anomaly detection based on improved genetic algorithm. In 2016 4th International Conference on Mechanical Materials and Manufacturing Engineering (pp. 186-189). Atlantis Press.

Chevrot, A., 2022. Detection of contextual anomalies in air traffic data using neural network models (Doctoral dissertation, Université Bourgogne Franche-Comté).

Gopalsamy, M., 2022. Scalable Anomaly Detection Frameworks for Network Traffic Analysis in cybersecurity using Machine Learning Approaches. Int. J. Curr. Eng. Technol, 12(06), pp.549-556.

Gummadi, A.N., Napier, J.C. and Abdallah, M., 2024. XAI-IoT: an explainable AI framework for enhancing anomaly detection in IoT systems. *IEEE Access*, *12*, pp.7102471054.

Intel., (2025) Accelerate Real-Time Machine Learning Based Anomaly Detection and Forecasting at Scale. https://www.intel.com/content/dam/www/central-libraries/us/en/documents/2022-11/ai-anodot-white-paper-111822.pdf

Ji, R., Padha, D., Singh, Y. and Sharma, S., 2024. Review of intrusion detection system in cyber-physical system based networks: Characteristics, industrial protocols, attacks, data sets and challenges. Transactions on Emerging Telecommunications Technologies, 35(9), p.e5029.

Jithish, J., Alangot, B., Mahalingam, N. and Yeo, K.S., 2023. Distributed anomaly detection in smart grids: a federated learning-based approach. IEEE Access, 11, pp.7157-7179. Kashif, M., 2024. Deploying Machine Learning Models on Resource Constrained Devices:A Case Study. https://essay.utwente.nl/101088/1/Kashif_BA_EEMCS.pdf

Keerthana, P., Devith, M.D., Hariharan, G. and Muthukumar, S., 2024, March. Machine Learning-Based Anomaly Detection for Imbalanced Network Traffic. In *2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)* (pp. 1-5). IEEE.

Khorasgani, A.T., Shirani, P. and Majumdar, S., 2024, September. An Empirical Study on Learning Models and Data Augmentation for IoT Anomaly Detection. In 2024 IEEE Conference on Communications and Network Security (CNS) (pp. 1-9). IEEE.

Kumari, S., Prabha, C., Karim, A., Hassan, M.M. and Azam, S., 2024. A Comprehensive Investigation of Anomaly Detection Methods in Deep Learning and Machine Learning: 2019–2023. IET Information Security, 2024(1), p.8821891.

Liu, R., Shi, J., Chen, X. and Lu, C., 2024. Network anomaly detection and security defense technology based on machine learning: A review. Computers and Electrical Engineering, 119, p.109581.

Miguel-Diez, A., Campazas-Vega, A., Álvarez-Aparicio, C., Esteban-Costales, G. and Guerrero-Higueras, Á.M., 2025. A systematic literature review of unsupervised learning algorithms for anomalous traffic detection based on flows. arXiv preprint arXiv:2503.08293.

Mirsadeghi, S.M.H., Bahsi, H., Vaarandi, R. and Inoubli, W., 2023. Learning From Few Cyber-Attacks: Addressing the Class Imbalance Problem in Machine Learning-Based Intrusion Detection in Software-Defined Networking. IEEE Access, 11, pp.140428-140442.

Nassif, A.B., Talib, M.A., Nasir, Q. and Dakalbab, F.M., 2021. Machine learning for anomaly detection: A systematic review. *Ieee Access*, *9*, pp.78658-78700.

Neri, M. and Baldoni, S., 2025. Unsupervised Network Anomaly Detection with Autoencoders and Traffic Images. arXiv preprint arXiv:2505.16650.

Ness, S., Eswarakrishnan, V., Sridharan, H., Shinde, V., Janapareddy, N.V.P. and Dhanawat, V., 2025. Anomaly Detection in Network Traffic using Advanced Machine Learning Techniques. IEEE Access.

Nguyen, D.C., Ding, M., Pathirana, P.N., Seneviratne, A., Li, J. and Poor, H.V., 2021. Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *23*(3), pp.1622-1658.

Nguyen, T.D., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N. and Sadeghi, A.R., 2019, July. DÏoT: A federated self-learning anomaly detection system for IoT. In *2019 IEEE 39th International conference on distributed computing systems (ICDCS)* (pp. 756-767). IEEE.

Ogah, M.D., Essien, J., Ogharandukun, M. and Abdullahi, M., 2024. Machine Learning Models for Heterogenous Network Security Anomaly Detection. Journal of Computer and Communications, 12(6), pp.38-58.

Oyewola, D.O., Akinwunmi, S.A. and Omotehinwa, T.O., 2024. Deep LSTM and LSTMAttention Q-learning based reinforcement learning in oil and gas sector prediction. *Knowledge-Based Systems*, *284*, p.111290.

Pervin, N. and Mokhtar, M., 2022. The interpretivist research paradigm: A subjective notion of a social context. *International Journal of Academic Research in Progressive Education and Development*, *11*(2), pp.419-428.

Pillai, S. and Sharma, A., 2023. Hybrid unsupervised web-attack detection and classification–A deep learning approach. *Computer Standards & Interfaces*, *86*, p.103738.

Sauce, B. and Matzel, L.D., 2022. Inductive reasoning. In *Encyclopedia of animal cognition and behavior* (pp. 3414-3421). Cham: Springer International Publishing.

Saxena, A., (2025) Computational Learning Theory in Machine Learning.https://www.appliedaicourse.com/blog/computational-learning-theory-in-machinelearning/

Sezar, S., (2025) Top 5 AI Network Monitoring Use Cases and Real Life Examples.https://research.aimultiple.com/ai-network-monitoring/

Shanmugam, V., Razavi-Far, R. and Hallaji, E., 2024. Addressing Class Imbalance in Intrusion Detection: A Comprehensive Evaluation of Machine Learning Approaches. *Electronics*, *14*(1), p.69.

Sharif, F., 2024. The role of ensemble learning in strengthening intrusion detection systems: A machine learning perspective. Int. J. Comput. Eng. Technol.

Singh, A. and Jang-Jaccard, J., 2022. Autoencoder-based unsupervised intrusion detection using multi-scale convolutional recurrent networks. arXiv preprint arXiv:2204.03779. Singh, P.K., Jyoti, J.S. and Singh, M., 2025. Real-Time Network Traffic Anomaly Detection Using Unsupervised Machine. *Computer Vision and Robotics: Proceedings of CVR 2024*, p.333.

Sofaer, H.R., Hoeting, J.A. and Jarnevich, C.S., 2019. The area under the precision-recall curve as a performance metric for rare binary events. *Methods in Ecology and Evolution*, *10*(4), pp.565-577.

Sowjanya, A.M. and Mrudula, O., 2023. Effective treatment of imbalanced datasets in health care using modified SMOTE coupled with stacked deep learning algorithms. *Applied Nanoscience*, *13*(3), pp.1829-1840.

Sowmya, T. and Anita, E.M., 2023. A comprehensive review of AI based intrusion detection system. Measurement: Sensors, 28, p.100827.

Taik, A., Nour, B. and Cherkaoui, S., 2022. Empowering prosumer communities in smart grid with wireless communications and federated edge learning. *IEEE Wireless Communications*, *28*(6), pp.26-33.

Thwaini, M.H., 2022. Anomaly detection in network traffic using machine learning for early threat detection. Data and Metadata, 1, pp.34-34.

Ullah, F., Ullah, S., Srivastava, G. and Lin, J.C.W., 2024. IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic. *Digital Communications and Networks*, *10*(1), pp.190-204.

Ullah, I., Liu, K., Yamamoto, T., Zahid, M. and Jamal, A., 2022. Prediction of electric vehicle charging duration time using ensemble machine learning algorithm and Shapley additive explanations. *International Journal of Energy Research*, *46*(11), pp.15211-15230.

Vanam, L., (2017) Part 2: Information Theory | Statistics for Deep Learning.https://medium.com/machine-learning-bootcamp/demystifying-information-theorye21f3af09455

Vu, T.T.N., 2021. Understanding validity and reliability from qualitative and quantitative research traditions. *VNU Journal of Foreign Studies*, *37*(3).

Xu, H., Pang, G., Wang, Y. and Wang, Y., 2023. Deep isolation forest for anomaly detection. IEEE Transactions on Knowledge and Data Engineering, 35(12), pp.12591-12604.

Xu, W., Jang-Jaccard, J., Singh, A., Wei, Y. and Sabrina, F., 2021. Improving performance of autoencoder-based network anomaly detection on nsl-kdd dataset. *IEEE Access*, *9*, pp.140136-140146.

Yang, Y.M., Chang, K.C. and Luo, J.N., 2025. Hybrid Neural Network-Based Intrusion Detection System: Leveraging LightGBM and MobileNetV2 for IoT Security. *Symmetry*, *17*(3), p.314.

Zhang, C., Wang, N., Hou, Y.T. and Lou, W., Machine Learning-Based Intrusion Detection Systems: Capabilities, Methodologies, and Open Research Challenges. Authorea Preprints.