Logo

Description automatically generated

GROUP ASSIGNMENT

|  |  |  |
| --- | --- | --- |
| **Module Code** | **:** | CT115-3-3-DLI (Deep Learning for Intrusion Detection) |
| **Intake Code** | **:** | APD3F2411CS(CYB) |
| **Lecturer Name** | **:** | DR. AITIZAZ ALI |
| **Date Assigned** | **:** | 16th of January |
| **Date Submitted** | **:** | 24th of March |

|  |  |
| --- | --- |
| **Student ID** | **Student Name** |
| TP071012 | ABDULRAHMAN GAMIL MOHAMMED AHMED |
| TP069210 | YAZEN ABOBAKR AHMED AL-MEHDHAR |
| TP072306 | HAZIQ IRFAN BIN RADZALI |
| TP071215 | AMANULLAH GHAURI |

**Table of Contents**

[1.0 INTRODUCTION 2](#_Toc193722987)

[2.0 GROUP COMPONENT 3](#_Toc193722988)

[2.1 ABDULRAHMAN GAMIL MOHAMMED AHMED (TP071012) 3](#_Toc193722989)

[2.2 YAZEN ABOBAKR AHMED AL-MEHDHAR (TP069210) 7](#_Toc193722990)

[2.3 HAZIQ IRFAN BIN RADZALI (TP072306) 9](#_Toc193722991)

[2.4 AMANULLAH GHAURI (TP071215) 12](#_Toc193722992)

[3.0 CONCLUSION 15](#_Toc193722993)

[1. REFERENCE 16](#_Toc193722994)

# 1.0 INTRODUCTION

In the rapidly evolving field of cybersecurity, the application of machine learning (ML) techniques has become a crucial approach for threat detection and defense. This group assignment brings together a comparative study of academic research papers selected by each group member, focusing on various ML algorithms and their application to pattern recognition and classification within the cybersecurity domain. Each member has individually analyzed papers from two members, offering insights into both internal and external cybersecurity threats, from insider threat detection and malware classification to adversarial defense mechanisms and secure software development. As a group, we have conducted a collective comparative analysis of all selected papers, evaluating them based on methodology, performance, applicability, and innovation. This examination aims to uncover current trends and justify the relevance of the chosen ML techniques, ultimately contributing to a better understanding of how intelligent systems are shaping the future of cybersecurity.

# GROUP COMPONENT

## 2.1 ABDULRAHMAN GAMIL MOHAMMED AHMED (TP071012)

**Introduction**

This part criticizes the research of Yazen Abobakr Ahmed Al-Mehdhar and Haziq Irfan Bin Radzali, who implement machine learning to different cybersecurity issues. Yazen discusses external threats to deep learning and software, whereas Haziq discusses internal threats such as insider threats and malware. Both offer insightful information on intelligent threat detection.

**Analysis of Yazen Abobakr Ahmed Al-Mehdhar's Papers**

**Paper 1: Adversarial-Aware Deep Learning System Based on a Secondary Classical Machine Learning Verification Approach**

**Analysis:** The paper introduces a new hybrid approach to make deep learning (DL) models more resistant to adversarial attacks, an old vulnerability of image classification architectures. With an additional secondary classical machine learning (ML) model, e.g., Random Forest (RF), as a verification layer, the technique exploits the supposed robustness of traditional ML against adversarial manipulations potentially ignored by the primary DL model. Tested on the ‎CIFAR-100 dataset, the technique employs adversarial attack generation (e.g., FGSM, PGD) and performance metrics include precision, recall, and F1-score. The results show a marked improvement in adversarial resistance and classification accuracy in adversarial ‎environments, outperforming standalone DL models and rivaling state-of-the-art defenses like adversarial training. Its light weight eschews computationally costly retraining, making it a desirable choice.

**Strengths:**

* The hybrid DL-ML model is novel yet pragmatic in combining the feature extraction abilities of DL with conventional ML's robustness.
* Low accuracy compromise for increased security supports practical deployment needs.
* Comparison to current defenses validates it.

**Limitations:**

* The assumption of classical ML's inherent adversarial robustness could be false against sophisticated, dual-target attacks, and should be scrutinized critically.
* Domain variation in performance outside CIFAR-100 shows low generalizability.
* While asserted to be effective, the paper does not have clear computational cost analysis for training and running two models in parallel.

**Paper 2: Machine Learning-Based Security Pattern Recognition Techniques for Code Developers**

**Analysis:** This study discusses software security in terms of suggesting an ML-driven system to identify source code vulnerabilities at the early stages of development and reduce chances of exploitation. Its language-agnostic approach translates code into vector representations using NLP algorithms (e.g., Word2Vec, K-Means clustering) to recognize semantic and structural patterns. Evaluating on ‎NIST benchmarks (C/C++ and Java), the system possesses high recall (e.g., 0.990 on Java) and ‎competitive F1-scores (e.g., 0.955 on Java), performing better than past baselines like Russell et al.'s ‎F1=0.84. The data flow and control tokens, analyzed by Gini Importance, enhance its ‎ability to detect Common Weakness Enumerations (CWEs), offering a scalable alternative to ‎traditional static application security testing (SAST) tools.‎

**Strengths:‎**

* Language-agnostic design applies across development environments.
* High recall prevents omissive vulnerabilities, a critical developer benefit.
* Improving upon prior baselines establishes its worth.

**Limitations:**

* Decreased precision on low-sample CWEs could produce false positives, which would swamp developers.
* Snippet-level accuracy (F1=0.778 for C/C++) is behind function-level results, implying noise sensitivity.
* Use of coding conventions can restrict adaptability to non-typical codebases.
* Possible Improvements:
* Precision for low-sample CWEs may be increased with selective sampling or feature enrichment to make it more useful.
* Static and dynamic analysis together may enhance snippet-level accuracy.
* Testing it on proprietary or niche codebases would test its readiness for enterprise use.

**Analysis of Haziq Irfan Bin Radzali's Papers**

**Paper 1: Identifying the Most Accurate Machine Learning Classification Technique for Insider Threat Detection**

**Analysi**s: The study is on insider threats in organizational networks, a new problem due to their capacity to inflict severe damage. Using the NSL-KDD dataset, it compares seven ML classifiers ranging from Support Vector Machines (SVM) to Extremely Randomised Trees (ERT) to determine the most accurate for threat detection like DoS, probing, and privilege escalation. AdaBoost distinguishes itself with 99% DoS and probe ‎attack accuracy, AUC scores (0.992 for DoS) to justify its accuracy. Methodological solidity, in the guise of validation datasets and hyperparameter tuning, ensures stable performance, placing AdaBoost in a promising position as a network security tool.

**Strengths:**

* Widespread comparison between classifiers picks out a clear, high-performing winner (AdaBoost).‎
* Encompassing support for multiple attack types justifies real-world applicability.‎
* Use of the updated NSL-KDD dataset is indicative of contemporary threats.‎

**Limitations:**

* Treatment of single datasets limits performance analysis in modern or heterogeneous ‎networks.‎
* Computational complexity for real-time usage is not treated.
* Failure to discuss the false positive rate hides operation trade-offs.

**Paper 2: Machine Learning-Based Cyber Threat Detection: An Approach to Malware Detection and Security with Explainable AI Insights**

**Analysis:** This paper enhances malware classification by interconnecting ML with explainable AI (XAI), finding an equilibrium between accuracy and transparency. Comparing four algorithms on a Kaggle dataset, Random Forest achieves impressive 100% accuracy, backed by extensive preprocessing (k-fold cross-validation, hyperparameter tuning). XAI tools (LIME, SHAP) illuminate key features like 'static\_prio' and 'vm\_truncate\_count,' substantiated by Chi-Squared tests and expert opinion. This ‎explainability enhances trust amongst cybersecurity practitioners, differentiating it from black box ‎ML systems and highlighting its potential for consistent, actionable malware detection.‎

**Strengths:**

* Optimal accuracy shows Random Forest's capability for malware classification.‎
* XAI incorporation delivers exceptional transparency, key to practitioner adoption.‎
* Statistical and expert validation provides credibility.‎

**Limitations:**

* 100% accuracy suggests possible dataset bias or overfitting, unrealistic in larger ‎contexts.‎
* Lack of error rate information (e.g., false negatives) limits reliability insights.
* Single dataset focus limits generalizability across malware variants.

## 2.2 YAZEN ABOBAKR AHMED AL-MEHDHAR (TP069210)

**Introduction**

This section critically examines the contributions made by Abdulrahman and Haziq, whose research addresses distinct dimensions of cybersecurity challenges through machine learning. While their papers explore different threat domains—Abdulrahman focuses on external network-based issues and Haziq targets internal risks—they both contribute valuable insights into the application of intelligent systems for threat detection.

**Analysis of Abdulrahman’s Papers**

Abdulrahman's first paper introduces a new approach combining deep learning with synthetic data generation to reverse the inherent skewness of IoT data sets. Unlike concentrating only on high-level accuracy, this work seeks the potential benefits of increasing detection sensitivity to rare attack vectors. The application of a generative adversarial network to generate additional minority class samples is a novel method of enhancing model resilience that is not based on deep datasets with labeled data. Not only are detection rates enhanced, but it marks the path towards more adaptive models in situations where threats are multiple and dynamic.

Abdulrahman's paper two pursues a complementary strategy of deploying several machine learning classifiers with time-series forecasting methods. The most significant strength in this instance is the double benefit of classification and prediction of DDoS attacks as required by advance protection methods. With focus on prediction, the paper is open to demonstrating how historical network trends can be utilized in an effort to forecast incoming attacks. This vision encourages the construction of systems that respond and also offer early warning to organizations, while the reliance on correct feature selection and data purity remains a dire issue.

**Analysis of Haziq’s Papers**

Haziq's initial paper assesses the region of insider threat detection employing various forms of machine learning classifiers in classification on the NSL-KDD dataset. Such a comparison is significant in its proximity to the gamma value between various classifiers, where ensemble methods like AdaBoost offer absolutely excellent performance. Such a discussion brings out here that of fine-tuning and cross-validation in efforts to address insider threat behavior's complexity. Haziq's research clearly demonstrates that, irrespective of how good accuracy can become, detection of such fine-grained internal issues needs a tuning of model complexity in the face of overfitting risk.

In the second paper, it combines the power of traditional machine learning and explainability techniques to address the issue of malware detection. In the union of XAI techniques such as LIME and SHAP into a Random Forest classifier, the paper not only demonstrates impressive accuracy performance but also gives insight into why the detection is being done through which features. This is a two-fold emphasis on performance and interpretability that renders the research more practical in application, as it provides actionable results that can be used by cybersecurity professionals to better comprehend and rely on the automated system's predictions.

**Comparative Analysis**

The two authors address machine learning to enhance cybersecurity but in a variety of different manners:

* **Focus and Methodology:**
  + Abdulrahman's papers center on matters related to network vulnerability, and he innovates through using predictive analyses and data enrichment. His obsession with bringing together data and pre-emptively forecasting DDoS attacks shifts the paradigm to actually forecasting rather than merely reacting to threats.
  + Conversely, Haziq's papers are concerned with insider threats based on ensemble learning and explainable artificial intelligence to shed more light on and augment threat detection. His research is concerned with model interpretability to build trust in machine systems.
* **Operational Implications:**
  + The methodologies in Abdulrahman's papers point to a paradigm that can particularly be helpful in the context of multiple and fluctuating external threats if it is possible to overcome the computational complexity.
  + Solutions on haziq’s papers have their built-in focus on interpretability and consistency offer effective solutions to businesses that want to audit insider behavior and malware such that decision making will be open to audit and verifiable.

## 2.3 HAZIQ IRFAN BIN RADZALI (TP072306)

**Introduction**

This section critically evaluates the research contributions of Amanullah Ghauri and Yazen Abobakr Ahmed Al-Mehdhar, both of whom have explored distinct cybersecurity challenges using machine learning. Amanullah's research focuses on real-time anomaly detection through graph-based methods and fine-tuned large language models, while Yazen investigates adversarial robustness and secure code analysis. The following analysis highlights the strengths and weaknesses of their methodologies and discusses their implications for cybersecurity.

**Analysis of Amanullah Ghauri’s Paper**

**Paper 1: LogSHIELD - A Graph-Based Real-Time Anomaly Detection Framework Using Frequency Analysis**

The paper presents a sophisticated technique for identifying anomalies in business security logs. LogSHIELD improves efficiency and accuracy in cyber threat detection by utilising Graph Neural Networks (GNNs) and Frequency-Domain Analysis (FDA). The system attains an exceptional 98% AUC for graph-based detection and 97% AUC for frequency-based transformations, surpassing current models. This approach's primary strengths involve contextual analysis via provenance graphs, enhanced detection accuracy, and computational efficiency. The complex structure of GNNs is a difficulty for real-time implementation, and the FDA approach's lack of interpretability might limit security analysts' assessment of reported anomalies.

**Paper 2: Confront Insider Threat - Precise Anomaly Detection in Behavior Logs Using LLM Fine-Tuning**

The paper introduces an innovative insider threat detection methodology employing a two-stage fine-tuned Large Language Model (LLM). This method converts behaviour logs into normal language, enhancing accuracy and flexibility in identifying harmful user actions. The ITDLM-II model achieves an F1-score of 0.8941, illustrating its superiority compared to conventional anomaly detection systems. Its merits are the capacity to differentiate harmless user deviations from dangers, the clarity provided by behaviour tracing, and its scalability inside enterprise contexts. Nonetheless, the model relies on high-quality structured logs and encounters difficulties in comprehending complex contextual behaviours, resulting in some misclassifications.

**Analysis of Yazen’s Paper**

**Paper 1: Adversarial-Aware Deep Learning System Based on a Secondary Classical ML Verification Approach**

This research examines adversarial attacks on deep learning models. This hybrid methodology combines CNN-based deep learning with an additional classical machine learning model (e.g., Random Forest) to mitigate hostile perturbations. The approach exhibits enhanced adversarial resilience while preserving computing efficiency. Nonetheless, its applicability beyond datasets is vague, and more complex attacks may circumvent the dual-model structure. Moreover, executing two models concurrently prolongs inference time, potentially restricting real-time detection capabilities.

**Paper 2: Machine Learning-Based Security Pattern Recognition for Code Developers**

This research examines automated detection of vulnerabilities in software source code. The system utilises NLP-based vectorisation and ML classifiers to attain high recall rates (0.990 for Java, 0.899 for C/C++), establishing it as a reliable alternative to conventional Static Application Security Testing (SAST) methods. The language-agnostic methodology and scalability for extensive codebases are significant advantages. Nonetheless, decreased accuracy for minimal sample vulnerabilities and sensitivity to coding rules restrict its generalisability.

**Comparative Analysis**

Although both researchers focus on the cybersecurity applications of machine learning, the approaches they use contrast considerably. Amanullah's work emphasises real-time anomaly detection with graph-based and LLM-driven approaches, rendering it exceptionally useful for enterprise safety monitoring. Conversely, Yazen’s research highlights adversarial robustness and secure coding methodologies, enhancing AI-driven security resilience. Amanullah's techniques provide superior scalability and real-time application, while Yazen's contributions improve explainability and adversarial defence strategies.

The fundamental difference is in their application. Amanullah’s LogSHIELD framework and insider threat detection approach is especially designed for enterprise-level network security, where real-time surveillance is essential. Yazen's adversarial robustness methodologies and security pattern recognition frameworks offer robust solutions for software security and AI-driven threat mitigation. Both approaches encounter limitations: Amanullah’s models demand substantial computational resources, whilst Yazen’s strategies require additional validation across several domains. Future research may investigate the integration of graph-based anomaly detection with adversarial-resistant machine learning models to bolster cybersecurity resilience across various domains.

The research conducted by Amanullah and Yazen significantly improves machine learning in the field of cybersecurity. Amanullah's research offers resilient real-time detection systems tailored for extensive enterprise networks, whilst Yazen's investigations emphasise enhancing adversarial resistance and software security. Both approaches possess distinct advantages and disadvantages. Nonetheless, collectively, they underscore the progressive function of machine learning in tackling cybersecurity issues. Future research should focus on integrating real-time anomaly detection with robust machine learning models to develop more comprehensive and resilient cybersecurity solutions.

## 2.4 AMANULLAH GHAURI (TP071215)

**Introduction**

Cybersecurity increasingly relies on machine learning (ML) and deep learning (DL) to enhance security and counter threats. This section analyzes four research papers from two members, Abdulrehman and Yazen, covering network intrusion detection, adversarial attack defense, and security pattern recognition. The selected techniques are evaluated for their efficiency, ability to handle imbalanced data, and response to emerging threats. Through comparison, this section examines their effectiveness, scalability, and real-world feasibility.

**Analysis of Abdulrahman’s Papers**

The first paper, "A Network Intrusion Detection System Based on Deep Learning in the IoT," presents a deep learning model designed to address the challenge of imbalanced data distribution in IoT network intrusion detection. By utilizing a Conditional Tabular Generative Adversarial Network (CTGAN) to generate synthetic data for minority attack classes, the paper demonstrates a substantial improvement in classification accuracy. The model is validated on three comprehensive datasets: UNSW-NB15, CIC-IDS2018, and CIC-IOT2023. The work effectively enhances detection rates for underrepresented attack types, but its dependency on labeled data may hinder its ability to detect zero-day attacks. Moreover, the high computational cost of training CTGAN and deep learning models presents challenges for real-time deployment.

The second paper, "A Machine Learning Based Classification and Prediction Techniques Used for DDoS Attacks," explores a range of ML algorithms—Decision Trees, Random Forests, Support Vector Machines, and Neural Networks—to classify and predict DDoS attacks. Notably, the paper integrates time-series analysis and boosting techniques to enhance predictive capabilities. The fusion of classification and prediction approaches significantly reduces false positives and allows organizations to respond proactively. However, the model's performance is heavily dependent on dataset quality and feature selection. Future improvements include real-time implementation, scalability to large networks, and the incorporation of Explainable AI (XAI) for greater transparency and usability.

**Analysis of Yazen’s Papers**

The first paper, "Network and Cybersecurity Applications of Defense in Adversarial Attacks: A State-of-the-Art Using Machine Learning and Deep Learning Methods," conducts a systematic review of ML- and DL-based defense strategies against adversarial attacks. Through an extensive literature review spanning 2019 to 2024, the study categorizes security enhancement techniques and identifies gaps in current research. Findings indicate that DL architectures excel in analyzing high-dimensional data and detecting adversarial patterns, though they often suffer from high computational costs. The paper emphasizes the necessity for future advancements in edge computing and semi-supervised learning to improve real-time adaptability and resilience against zero-day threats.

The second paper, "Machine Learning-Based Security Pattern Recognition Techniques for Code Developers," introduces a ML-driven system that automates vulnerability detection in source code. By transforming source code into vector representations using NLP techniques, the model effectively classifies secure and vulnerable code segments. The ensemble approach, integrating Decision Trees, Support Vector Machines, and Neural Networks, achieves a recall rate of over 0.94, even with limited vulnerable instances. However, the effectiveness of this technique depends on the representativeness of the dataset. The study suggests incorporating XAI and developing real-time scanning tools for widespread industry adoption.

**Comparative Analysis**

Both researchers study how machine learning (ML) can be used in cybersecurity, but they focus on different areas. Abdulrehman works on detecting network intrusions and preventing DDoS (Distributed Denial-of-Service) attacks. They use both deep learning and traditional ML techniques to classify threats. A key part of their research is addressing data imbalance, when certain attack types are underrepresented in training data. To fix this, they use synthetic data, including generative models like CTGAN, which help improve detection accuracy. They also explore time-series analysis to predict DDoS attacks, showing the increasing use of time-based modeling for proactive cybersecurity.

Yazen, on the other hand, focuses on defending against adversarial attacks and recognizing security patterns. Their work highlights the importance of reviewing cybersecurity research and analyzing code for vulnerabilities. This aligns with the growing focus on software security, particularly in DevSecOps, where security is integrated into the development process from the start. A notable aspect of their research is the use of natural language processing (NLP) to convert source code into numerical representations, demonstrating how AI-driven language models are being applied beyond text analysis to cybersecurity.

Despite their different focuses, both researchers rely on ML-based classification methods, often using ensemble learning techniques and considering Explainable AI (XAI) to make their models more transparent and understandable for security experts. This reflects a broader trend in cybersecurity, where achieving high accuracy is important, but so is ensuring that AI models are interpretable. They also recognize the challenge of balancing computational efficiency with detection accuracy, an important factor when deploying AI solutions at scale.

Looking ahead, future research in this area is likely to explore edge computing, lightweight ML models, and hybrid approaches that combine supervised and unsupervised learning. These innovations aim to improve cybersecurity, especially in detecting new (zero-day) threats more effectively.

# 3.0 CONCLUSION

Through our group analysis, we observed a diverse set of strategies being employed to tackle modern cybersecurity challenges using artificial intelligence. The individual papers examined a range of threats and solutions from enhancing deep learning strength against adversarial attacks and securing code development, to real-time anomaly detection using graph-based models and explainable AI for malware classification. Some methods focused on how well and accurately they could detect threats, while others aimed to make the results easier to understand, work better on a large scale, and predict threats before they happen. Even though the papers focused on different topics, they all showed that cybersecurity research is increasingly using ensemble methods, time-based analysis, and natural language processing (NLP) techniques. Our comparison shows that no single model or method works best in every situation. Instead, how well a technique performs depends on the type of data, the kind of threat, and how the system is being used. Looking ahead, we see the potential in using hybrid models that mix real-time detection, easy-to-understand results, and the ability to learn and adapt. These models could lead to stronger and transparent cybersecurity solutions.

# 4.0 REFERENCE

* Alkhowaiter, M., Kholidy, H., Alyami, M., Alghamdi, A., & Zou, C. (2023). *Adversarial-aware deep learning system based on a secondary classical machine learning verification approach.* arXiv. <https://arxiv.org/abs/2306.00314>
* Wang, X., Dai, L., & Yang, G. (2024). A network intrusion detection system based on deep learning in the IoT. *The Journal of Supercomputing*, *80*(16), 24520–24558. https://doi.org/10.1007/s11227-024-06345-w

‌

* Ismail, Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., Raza, M., Rahman, I. U., & Haleem, M. (2022). A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks. *IEEE Access*, *10*, 21443–21454. https://doi.org/10.1109/access.2022.3152577
* Zaharia, D., Rebedea, T., & Trausan-Matu, S. (2022). **Machine learning-based security pattern recognition techniques for code developers**. *Applied Sciences, 12*(23), 12463. <https://doi.org/10.3390/app122312463>
* Roy, K. C., & Chen, Q. (2024, October 29). LogSHIELD: A Graph-based Real-time Anomaly Detection Framework using Frequency Analysis. arXiv.org. <https://arxiv.org/abs/2410.21936>
* Song, S., Zhang, Y., & Gao, N. (2025, January 1). Confront Insider Threat: Precise anomaly detection in behavior logs based on LLM Fine-Tuning. ACL Anthology. <https://aclanthology.org/2025.coling-main.574/>
* Farouk, M., Sakr, R. H., & Hikal, N. (2024). Identifying the most accurate machine learning classification technique to detect network threats. Neural Computing and Applications, 36(16), 8977–8994. <https://doi.org/10.1007/s00521-024-09562-9>
* Farida Siddiqi Prity, Islam, M. S., Fahim, E. H., Hossain, M. M., Bhuiyan, S. H., Islam, M. A., & Mirza Raquib. (2024). Machine learning-based cyber threat detection: an approach to malware detection and security with explainable AI insights. Human-Intelligent Systems Integration. https://doi.org/10.1007/s42454-024-00055-7