Project and Data Management (PDM) Plan

#### AI-Based Approach for Anomaly Detection in IoT Network Dataflows Using the Bot-IoT Dataset

# 1. Introduction

The Internet of Things (IoT) has evolved various sectors through its ability to gather real-time information and automate processes together with intelligent decision systems which power various programs like smart cities and healthcare services and industrial systems and transportation networks. The accelerated development of IoT networks has created substantial security issues that have turned these systems into desirable cyber-attack targets for Distributed Denial of Service (DDoS) operations and malware spread and unauthorized permission violations (DeMedeiros et al., 2023). Intrusion detection systems that depend on predefined rules and signature-based detection fail to recognize emerging threats because of their established operational methods. AI-driven anomaly detection models stand crucial to protect IoT environments because they now require efficient systems for detecting security breaches (Dasgupta, Akhtar, & Sen, 2022).

## Research Background and Motivation

The technology boom of Internet of Things (IoT) has completely transformed smart cities as well as healthcare systems and industrial automation and transportation networks. The exchange of real-time data through IoT networks supports operational automation which increases company performance and better decision-making capabilities. The growing IoT device connectivity creates extensive cybersecurity threats because distributed denial of service attacks, malware infections and unauthorized access affect these devices (DeMedeiros et al., 2023). Several obstacles to implementing traditional security measures appear because IoT devices have limited resources and IoT ecosystems do not share standard security protocols (Swessi & Idoudi, 2022).

The standard use of Intrusion Detection Systems (IDS) for IoT security has such limitations that signature-based IDS detects only known attacks thus becoming ineffective when facing zero-day threats and changing cyberattacks (Baker et al., 2022). Solutioned-based anomaly detection systems produce large numbers of incorrect detection alerts which results in security monitoring becoming unreliable (Peterson, Khoshgoftaar, & Leevy, 2022). IoT security enhancement projects have started using Artificial Intelligence (AI) and Machine Learning (ML) models because traditional approaches have shown their limitations. AI-based anomaly detection models acquire adaptive learning capacities which enable them to detect IoT network traffic patterns for malicious activity identification without needing predefined signatures (Dasgupta, Akhtar, & Sen, 2022).

The development of an AI-driven anomaly detection system that identifies cyber threats in IoT networks constitutes the research motivation. The objective of this research is to develop an intrusion detection system through Support Vector Machine (SVM), Random Forest Classifier (RFC), and Multi-Layer Perceptron (MLP which would boost real-time intrusion detection and decrease false positives in order to enhance overall cyber resilience of IoT environments (Alimi et al., 2021).

## Research Questions and Objectives

Modern security needs advanced systems that detect live cyber threats in IoT networks which have become more extensive and difficult to protect. The current Intrusion Detection Systems (IDS) face multiple operational challenges that include excessive false positives as well as poor scalability and limited capability to identify unknown attack methods according to Dasgupta et al. (2022). The research develops AI-driven anomaly detection models to enhance IoT security because current systems have demonstrated limitations during detection operations. A research investigates the anomaly classification capability of Support Vector Machine (SVM), Random Forest Classifier (RFC), and Multi-Layer Perceptron (MLP) on the Bot-IoT dataset for IoT cybersecurity analysis (Peterson, Khoshgoftaar, & Leevy, 2022).

The main research inquiry of this investigation is:

The study explores the use of the Bot-IoT dataset to determine how AI-based models specifically SVM and RFC and MLP can detect anomalies in IoT network traffic while maintaining high detection rates and low false positive rates.

The study aims at answering this research question through the following important objectives.

* The detection capabilities of SVM and RFC and MLP are compared using accuracy parameters alongside precision and recall parameters and F1-score (DeMedeiros et al., 2023).
* IoT network traffic data undergoes analysis and preprocessing which includes applying scalability techniques along with encoding methods and selecting features because these enhancements improve machine learning model performance (Swessi & Idoudi, 2022).
* Organizations should make AI detection models perform faster through computational speedups while scaling them to support extensive IoT deployment networks (Ghimire and Rawat, 2022).
* Researchers need to evaluate deployment barriers for AI-based intrusion detection systems within constrained IoT systems together with real-time compliance and storage system capabilities and latency performance (Alazab et al., 2024).
* Examine how artificial intelligence frameworks can reinforce IoT security while preserving performance levels by integrating them into current IoT systems (Panda, Abd Allah, & Hassanien, 2021).

The research objectives focus on building strong AI-based anomaly detection methods that will enhance cyber safety in IoT systems while producing new insights into IoT security research.

# 2. Literature Review

The speed of Internet of Things (IoT) ecosystem expansion creates extensive cybersecurity problems because standard security methods no longer stop advanced cyber threats. AI-based anomaly detection proves to be an effective new method for detecting threats in real-time throughout IoT networks. This section analyzes IoT security difficulties in addition to explaining AI anomaly detection methods as well as exploring existing cybersecurity data datasets alongside AI challenges for IoT defense systems.

## ****2.1 IoT Security Landscape****

#### **2.1.1 Key Security Threats in IoT**

The infrastructure of IoT faces multiple cybersecurity threats that comprise distributed denial of service attacks and malware infections together with unauthorized access incidents and data breaches. Since most IoT devices have inadequate security settings cybercriminals view them as prime attack targets (Swessi & Idoudi, 2022).

* The network resources of IoT devices become overwhelmed by botnets that launch Distributed Denial of Service (DDoS) Attacks through their exploitation. During 2016 the Mirai botnet demonstrated how compromised Internet of Things devices inflicted world-wide damage to major internet services (Neupane et al., 2022).
* The BrickerBot and Mozi malware families use IoT devices to spread through unprotected devices thereby causing inoperability or botnet system control (Ghimire & Rawat, 2022).
* Attackers exploit weak authentication methods in IoT devices to take unauthorized control which results in data theft or sabotages industrial systems or hijacks devices (Alazab et al., 2024).
* The majority of Internet-of-Things systems involve the collection of sensitive personal and industrial data that faces a high risk of breach. Financial transactions along with patient health records and critical infrastructure information remain at risk during security breaches because they result in serious privacy complications and regulatory compliance problems (Dasgupta, Akhtar, & Sen, 2022).

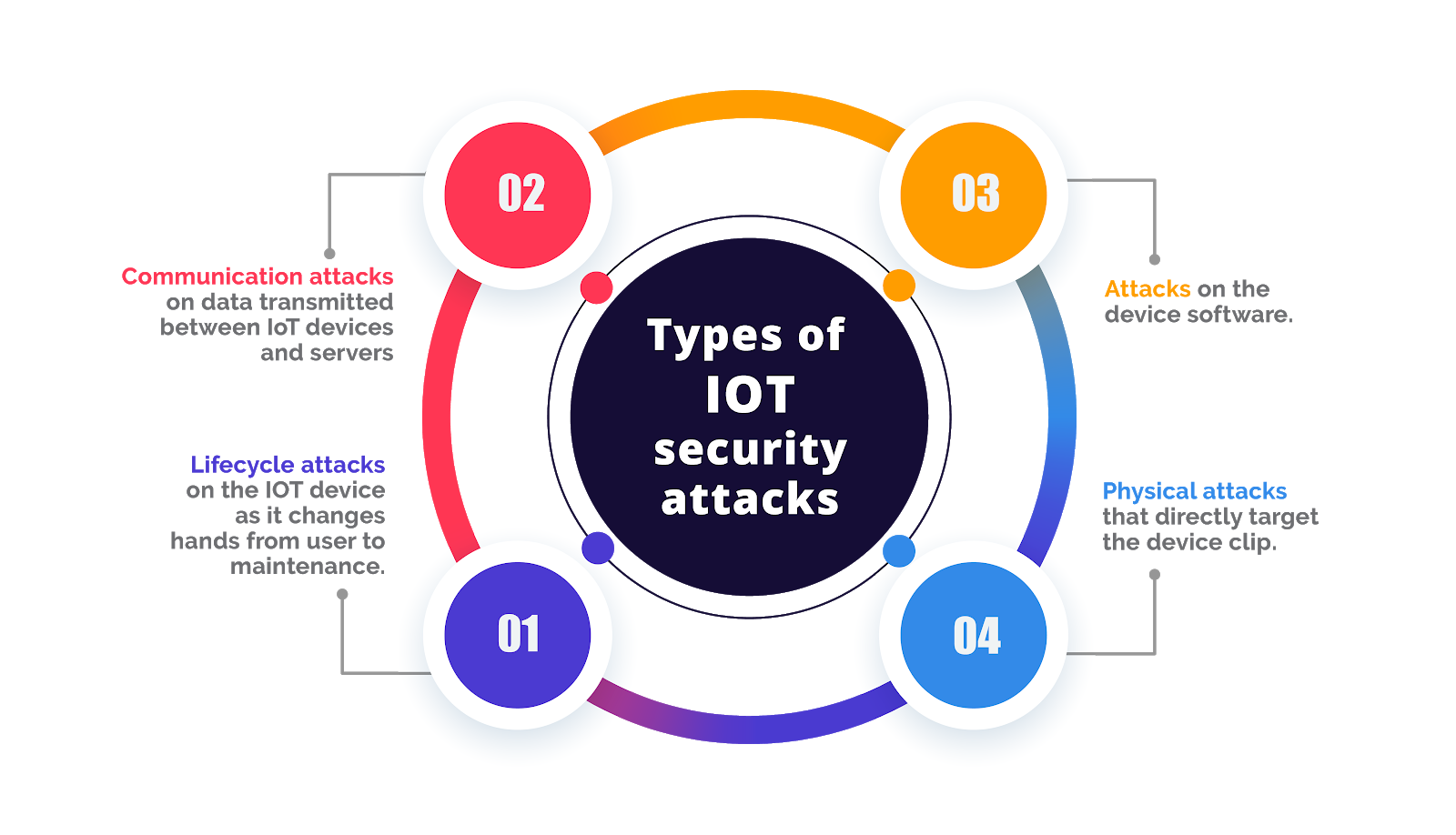


Fig1: IoT in Cybersecurity Threats

#### 2.1.2 Case Studies and Statistics on IoT Security Breaches

IoT security vulnerabilities reach serious levels based on numerous high-profile incidents that have occurred.

* The 2016 Mirai Botnet Attack spread through 600,000 IoT devices to carry out DDoS attacks that became record setters by disrupting Dyn DNS and both Twitter and Netflix platforms (Peterson, Khoshgoftaar, & Leevy, 2022).
* Stuxnet (2010) constituted a revolutionary malware attack which targeted Iran's nuclear facilities to reveal IoT's potential as an industrial hacking instrument (Panda, Abd Allah, & Hassanien, 2021).
* The Ring Camera breaches of 2019 occurred because of security flaws in authentication protocols thus exposing internet of things privacy weaknesses (Baker et al., 2022).
* AI-based proactive threat detection systems are necessary to boost IoT security resistance because of these recent incidents.

## 2.2 AI in Anomaly Detection

AI &ML has greatly enabled the identification and prevention of cyber threats in IoT networks due to the fast advancement of IoT technology. Intrusion Detection Systems (IDS) mainly employ two modes, namely, signature-based and anomaly-based modes, which have specific drawbacks. This is because SNIDS operates based on known binaries, and as a result, it cannot identify or prevent zero-day attacks or mutating malware as identified in DeMedeiros et al. (2023). Anomaly-based IDS, which detect deviations from the normal traffic pattern on the network, generate high amount of the false positives since they depend on such rules that cannot adapt to the new emerging IoT networks (Swessi and Idoudi, 2022). This has made stimulate researchers develop AI-based anomaly detection models that train from the patterns that are composed in the network traffic and adjust to upcoming threats.

Machine learning is then used in the AI-based intrusion detection in order to improve security in many IoT networks. Unlike unsupervised learning models, supervised learning models like Support Vector Machine (SVM), Random Forest Classifier (RFC) and Multi-Layer Perceptron (MLP) need classified data set through which the classifier is built to distinguish between the benign and malicious traffics (Panda, Abd Allah & Hassanien, 2021). These models have been found to have high accuracy in the security of IoT but has issues of large-scale labeled data which are not easily available. Cluster algorithms such as the K-means algorithm and the DBSCAN, as well as autoencoder models, find anomalies without using labelled datasets, which makes them suitable in discovering the unknown attacks and the zero-day threats (Ghimire & Rawat, 2022). Another more development area is the reinforcement learning (RL) that is an approach based on AI training agents to perform the detection task in the given environment and constantly improve the detection policies during the process (Alazab et al., 2024).

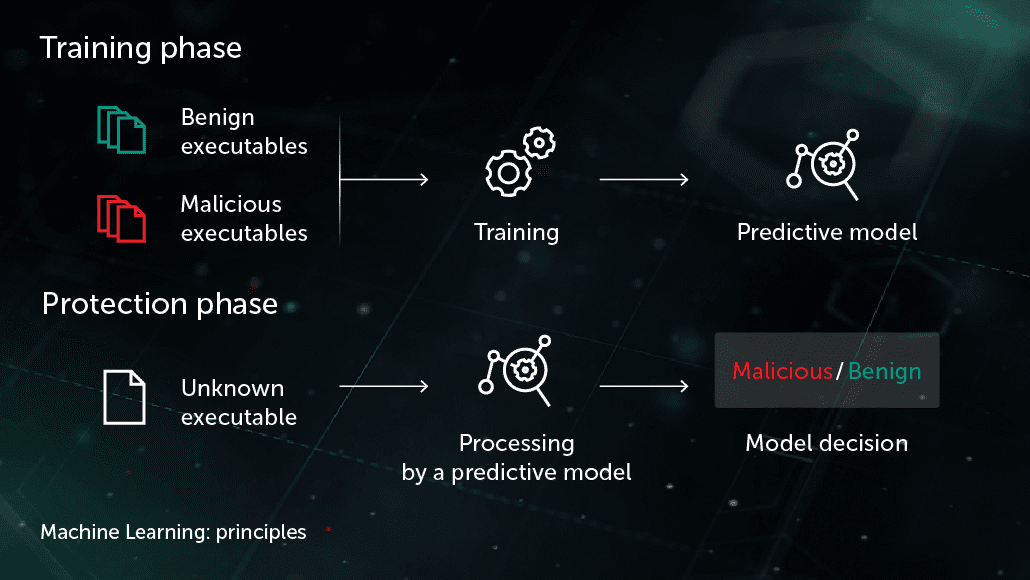


Fig2: Machine learning in cybersecurity

This is because some of the perks of using AI to develop IDS, its advantages over traditional IDS are as follows; As mentioned in Neupane et al., (2022), the use of AI models can address the issue of larger data processing by the IoT network by preventing the occurrence of attacks before they cause an increase in scale. However, some of the challenges which are present with the growing adoption of IoT and AI in its security include; Data imbalance, Adversarial attack, Computational complexity. To overcome these issues, researchers are trying to leverage federated learning to improve the scalability by reducing the amount of data transmitted for training the detector and the explainable AI (XAI) methodology to improve the interpretability of AI-based IDSs (Baker et al., 2022).

## 2.3 Relevant Datasets and Preprocessing Techniques

The general performance of anomaly detection models that employ AI is highly determined by the type and richness of data that is used in training and testing of the model. There are several well-known benchmark datasets that have been used to develop and evaluate IDS models in the field of cybersecurity. NSL-KDD dataset which is an improved version of KDD’99 is widely used in IDS performance assessment. However, one of them does not include the modern IoT specific attack traffic which can hinder its usefulness to researchers in IoT security (Panda, Abd Allah, & Hassanien, 2021). Likewise, for general cybersecurity reasons, the CICIDS2017 dataset covers different kinds of network attacks including DoS, brute force, botnet and others, but it does not include IoT network activity pattern (Peterson et al., 2022).

In the effort to overcome the limitation of the common datasets, researchers have then proposed the IoT-specific intrusion detection dataset with the Bot-IoT as the most popular and vast one in the IoT cybersecurity field today. Bot-IoT developed by the Cyber Range Lab at the University of New South Wales Canberra; reproduces real-world IoT environment; records normal and intrusive network traffic from different IoT devices (M. Baker et al., 2022). DDoS, keyloggers, OS scan, and data transfer are the types of attacks present in the dataset; as a result, the data is appropriate to use to develop machine learning models for IDS (DeMedeiros et al., 2023). Moreover, the large volume of data representation in Bot-IoT is beneficial to learning realistic attack patterns in real IoT deployments that assist the AI models in detecting more real anomalies.

Many important parameters and algorithms in cybersecurity datasets have to be enhanced by the best methods of preprocessing. The techniques of feature selection and dimensionality reduction make it possible to remove all irrelevant features to improve the performance of the model in addition to making analysis less computationally intensive (Swessi & Idoudi, 2022). Normalization techniques such as Min-Max scaling is also used to standardize all the numerical data to be with in a specific range to avoid the models considering large numerical data (Neupane et al., 2022). Parameter encoding techniques including the one-hot encoding are applied to the categorical data like the protocol types and the state of connection which are more appropriate for transformation into a form that can be processed by an AI.

This is because, as described earlier, it possesses realistic attack simulations, diverse representation of IoT network traffic, as well as scalability, making it possible to classify it as suitable for this research project. For instance, feature selection, scaling, and encoding help to make AI models suitable for high detection rates while also making them relevant to be implemented in the IoT security systems in real-time.

## 2.4 Challenges in AI-Based Security for IoT

#### 2.4.1 Key Challenges

* Alas, there are still some issues worth preventing associated with AI development in IoT:
* Imbalanced Dataset: A number of real attack samples are less than normal traffic data, which makes the learning algorithms skewed (Neupane et al., 2022).
* They can interfere with AI models by creating false traffic as stated by Alazab et al. (2024).
* This is due to the complexity in deploying the models running on AI, as it demands a lot of computational resource power, a challenge that will be hard for IoT devices.

#### 2.4.2 Proposed Solutions

* FL: A decentralized approach to machine learning to enhance the former’s privacy and overall capacity (Swessi & Idoudi, 2022).
* Explainable AI (XAI): Raises them to make model interpretability thus enhance security decisions in a more transparent manner (Baker et al., 2022).
* Lightweight AI Models: One way of dealing with this issue is to optimize the AI models for low power IoT environment in order to improve the real time processing of such models (Panda, Abd Allah, & Hassanien, 2021).

# 5. References

Adil, M., & Khan, M. K. (2021). Emerging IoT applications in sustainable smart cities for COVID-19: Network security and data preservation challenges with future directions. Sustainable Cities and Society, 75, 103311. https://doi.org/10.1016/j.scs.2021.103311

Alazab, M., Khurma, R. A., Castillo, P. A., Abu-Salih, B., Martín, A., & Camacho, D. (2024). An effective network intrusion detection approach based on hybrid Harris Hawks and multi-layer perceptron. Egyptian Informatics Journal, 25, 100423. https://doi.org/10.1016/j.eij.2024.100423

Alimi, O. A., Ouahada, K., Abu-Mahfouz, A. M., Rimer, S., & Alimi, K. O. A. (2021). A review of research works on supervised learning algorithms for SCADA intrusion detection and classification. Sustainability, 13(17), 9597. https://doi.org/10.3390/su13179597

Attou, H., Guezzaz, A., Benkirane, S., Azrour, M., & Farhaoui, Y. (2023). Cloud-based intrusion detection approach using machine learning techniques. Big Data Mining and Analytics, 6(3), 311-320. https://doi.org/10.26599/BDMA.2023.9020023

Baker, M., Fard, A. Y., Althuwaini, H., & Shadmand, M. B. (2022). Real-time AI-based anomaly detection and classification in power electronics dominated grids. IEEE Journal of Emerging and Selected Topics in Industrial Electronics, 4(2), 549-559. https://doi.org/10.1109/JESTIE.2022.3164321

Choubisa, M., Doshi, R., Khatri, N., & Hiran, K. K. (2022, May). A simple and robust approach of random forest for intrusion detection system in cybersecurity. In 2022 International Conference on IoT and Blockchain Technology (ICIBT) (pp. 1-5). IEEE. https://doi.org/10.1109/ICIBT53968.2022.9796891

Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: A comprehensive survey. The Journal of Defense Modeling and Simulation, 19(1), 57-106. https://doi.org/10.1177/15485129211057677

DeMedeiros, K., Hendawi, A., & Alvarez, M. (2023). A survey of AI-based anomaly detection in IoT and sensor networks. Sensors, 23(3), 1352. https://doi.org/10.3390/s23031352

Dhiman, H. S., Deb, D., Muyeen, S. M., & Kamwa, I. (2021). Wind turbine gearbox anomaly detection based on adaptive threshold and twin support vector machines. IEEE Transactions on Energy Conversion, 36(4), 3462-3469. https://doi.org/10.1109/TEC.2021.3082681

Ghimire, B., & Rawat, D. B. (2022). Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things. IEEE Internet of Things Journal, 9(11), 8229-8249. https://doi.org/10.1109/JIOT.2021.3114847

Karale, A. (2021). The challenges of IoT addressing security, ethics, privacy, and laws. Internet of Things, 15, 100420. https://doi.org/10.1016/j.iot.2021.100420

Larriva-Novo, X., Villagrá, V. A., Vega-Barbas, M., Rivera, D., & Sanz Rodrigo, M. (2021). An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets. Sensors, 21(2), 656. https://doi.org/10.3390/s21020656

Neupane, S., Ables, J., Anderson, W., Mittal, S., Rahimi, S., Banicescu, I., & Seale, M. (2022). Explainable intrusion detection systems (X-IDS): A survey of current methods, challenges, and opportunities. IEEE Access, 10, 112392-112415. https://doi.org/10.1109/ACCESS.2022.3223092

Ozkan-Okay, M., Akin, E., Aslan, Ö., Kosunalp, S., Iliev, T., Stoyanov, I., & Beloev, I. (2024). A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cyber security solutions. IEEE Access, 12, 12229-12256. https://doi.org/10.1109/ACCESS.2024.3212145

Panda, M., Abd Allah, A. M., & Hassanien, A. E. (2021). Developing an efficient feature engineering and machine learning model for detecting IoT-botnet cyber-attacks. IEEE Access, 9, 91038-91052. https://doi.org/10.1109/ACCESS.2021.3091986

Peterson, J. M., Leevy, J. L., & Khoshgoftaar, T. M. (2021, August). A review and analysis of the Bot-IoT dataset. In 2021 IEEE International Conference on Service-Oriented System Engineering (SOSE) (pp. 20-27). IEEE. https://doi.org/10.1109/SOSE52839.2021.00015

Soenen, J., Van Wolputte, E., Perini, L., Vercruyssen, V., Meert, W., Davis, J., & Blockeel, H. (2021, August). The effect of hyperparameter tuning on the comparative evaluation of unsupervised anomaly detection methods. In Proceedings of the KDD'21 Workshop on Outlier Detection and Description (pp. 1-9). Outlier Detection and Description Organizing Committee.

Swessi, D., & Idoudi, H. (2022). A survey on internet-of-things security: threats and emerging countermeasures. Wireless Personal Communications, 124(2), 1557-1592. https://doi.org/10.1007/s11277-021-08661-5