

Anomaly Detection in Smart Homes IoT Network using Reinforcement Learning

A PROJECT REPORT

Submitted to

Amrita Vishwa Vidyapeetham

in partial fulfillment for the award of the degree of

**BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND
ENGINEERING**

By

ANGELA RAJ CHADHA

(Reg. No. CH.EN.U4CYS20088)

KETHAMREDDY KARTHIKEYA REDDY

(Reg. No. CH.EN.U4CYS20038)

Supervisor

Dr. S SOUNTHARRAJAN



AMRITA VISHWA VIDYAPEETHAM

AMRITA SCHOOL OF COMPUTING

CHENNAI – 601103

November 2023

Anomaly Detection in Smart Homes IoT Network using Reinforcement Learning

A PROJECT REPORT

Submitted to

Amrita Vishwa Vidyapeetham

in partial fulfillment for the award of the degree of

**BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND
ENGINEERING**

By

ANGELA RAJ CHADHA

(Reg. No. CH.EN.U4CYS20088)

KETHAMREDDY KARTHIKEYA REDDY

(Reg. No. CH.EN.U4CYS20038)

Supervisor

Dr. S SOUNTHARRAJAN



AMRITA VISHWA VIDYAPEETHAM

AMRITA SCHOOL OF COMPUTING

CHENNAI – 601103

November 2023



**SCHOOL OF
COMPUTING
CHENNAI**

BONAFIDE CERTIFICATE

Certified that this project report “**Anomaly Detection in Smart Homes IoT Network using Reinforcement Learning**” is the bonafide work of “**ANGELA RAJ CHADHA (Reg. No. CH.EN.U4CYS20088)**” and “**KETHAMREDDY KARTHIKEYA REDDY (Reg. No. CH.EN.U4CYS20038)**” who carried out the project work under my supervision.

SIGNATURE

Dr. A.G.SRIDEVI

PROGRAM HEAD

Department of CSE.

Amrita School Of Computing

Chennai

SIGNATURE

Dr. S SOUNTHARRAJAN

SUPERVISOR

ASSOCIATE PROFESSOR

Department of CSE.

Amrita School Of Computing

Chennai

INTERNAL EXAMINER

EXTERNAL EXAMINER



**SCHOOL OF
COMPUTING
CHENNAI**

DECLARATION BY THE CANDIDATE

I declare that the report entitled “**Anomaly Detection in Smart Homes IoT Network using Reinforcement Learning**” submitted by us for the degree of Bachelor of Engineering is the record of the project work carried out by us under the guidance of “ **ANGELA RAJ CHADHA(Reg. No. CH.EN.U4CYS20088)** ” and “ **KETHAMREDDY KARTHIKEYA REDDY (Reg. No. CH.EN.U4CYS20038)** ” and this work has not formed the basis for the award of any degree, diploma, associateship, fellowship, titled in this or any other University or other similar institution of higher learning.

SIGNATURE

ANGELA RAJ CHADHA
(Reg. No. CH.EN.U4CYS20088)

SIGNATURE

KETHAMREDDY
KARTHIKEYA REDDY
(Reg. No. CH.EN.U4CYS20038)

ABSTRACT

In the era of the Internet of Things (IoT), smart homes have become a cornerstone of

modern living, offering convenience, energy efficiency, and security. The extensive connectivity within these networks brings forth security challenges, making the detection of anomalies a critical aspect of IoT network security. Anomalies encompass a wide array of unexpected events, from irregular data patterns to communication anomalies, power fluctuations, behavioral deviations, security breaches, and environmental variations. This paper underscores the pivotal role of anomaly detection in securing IoT networks, highlighting its significance in identifying both known threats and emerging risks. Anomaly detection in IoT relies on machine learning and statistical techniques, encompassing data collection, preprocessing, feature extraction, model training, real-time anomaly detection, and responsive actions. RL, a subset of machine learning, emerges as a formidable tool in enhancing IoT network security. RL models continuously observe and adapt to device behavior, identifying anomalies and security breaches in real-time. RL offers adaptability in rapidly changing IoT environments, proactive responses to anomalies, and the ability to learn and evolve against new threats. In conjunction with Federated Learning, which enhances data privacy, RL strengthens network security without compromising individual device data. The integration of RL and Federated Learning is exemplified through Magpie, an advanced security system that refines its understanding of the smart home environment, collectively learns from anomalies, and bolsters network security. Synergy of IoT and RL is reshaping IoT network security, promising not only seamless device functionality but also the safeguarding of sensitive data and personal spaces.

Keywords: Reinforcement learning. Anomaly, Metadata Stream, Intrusion Detection system, smart homes.

ACKNOWLEDGEMENT

We are profoundly grateful to the esteemed Dr. Sountharajjan, whose unwavering support, invaluable guidance, and insightful suggestions have been the cornerstone of our project's success.

Furthermore, our profound appreciation extends to our Project Panel Teachers - Dr. S. Udhayaumar, Dr. Veluchamy, and Mr. Deepak, who, with their remarkable expertise, provided us with invaluable guidance, astute comments, and invaluable suggestions that enriched our project's development.

We owe a debt of gratitude to our esteemed Principal, Dr. V. Jayakumar, and our dedicated Head of Department, Dr. Sreedevi A. G, whose unwavering support has been instrumental in the flawless execution of our project.

We would be remiss not to acknowledge the boundless encouragement and wisdom provided by our parents, whose constant motivation and invaluable guidance have been the driving force behind our project's accomplishment.

Lastly, we are profoundly touched by the blessings and well wishes bestowed upon us by our beloved "Amma," which have undoubtedly played a pivotal role in our journey towards success.

ANGELA RAJ CHADHA
(Reg. No. CH.EN.U4CYS20088)

KETHAMREDDY KARTHIKEYA REDDY
(Reg. No. CH.EN.U4CYS20038)

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	Abstract	iv
	List of Tables	
	List of Figures	

	List of Symbols and Abbreviation	
1	Introduction	
	1.1 Introduction to IOT	
	1.2 Anomalities in IOT	
	1.3 Anomaly Detection	
	1.4 Reinforcement Learning	
2	Literature Review	
	2.1 Literature Survey	
3	Problem Statement	
4	System Design	
	4.1 Architecture Diagram	
	4.2 Proposed Model	
	4.3 Algorithm	
5	Experimental Work	

LIST OF TABLES

TABLE NO.	TITLE	PAGE NO.
------------------	--------------	-----------------

2.1	Literature Survey	
4.1	A 5 minute Capture of Data Stream sample	
5.1	Different types of Attacks on IoT network and their impact	
	Comparison of our model with existing model	

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE NO.
-------------------	--------------	-----------------

4.1	Architecture Diagram of the proposed model	
6.1	Establishing SSH connection to the raspberry PI	
6.2	Raspberry PI configuration	
6.3	Performing Data Pre-processing On the Dataset	
6.4	Data samples before pre-processing	
6.5	Data samples after pre-processing	
6.6	Performing DOS attack	
6.7	Result of the DoS attack in the tcpdump of raspberry PI	

LIST OF SYMBOLS AND ABBREVIATIONS

MDS	Meta Data Stream
------------	-------------------------

CHAPTER 1

INTRODUCTION

1.1. INTRODUCTION TO IOT

The Internet of Things has metamorphosed the lifestyle and interact with technology. In smart homes, IoT networks are the backbone, connecting an array of devices like thermostats, smart lights, smart security cameras, and voice-activated smart assistants. These networks enable automation and control, offering convenience, energy efficiency, and security. However, the extensive connectivity and data exchange in smart homes introduces security challenges. Protecting the integrity, privacy, and reliability of IoT networks is paramount. Traditional security measures often struggle to adapt to the dynamic and evolving nature of security threats in this complex environment.

1.2. ANOMALIES IN IOT

Anomalies in IoT (Internet of Things) refer to unexpected or unusual patterns, events, or behaviours detected within the data generated or collected by IoT devices. Detecting anomalies is a crucial aspect of IoT security, data analysis, and system management, as it helps identify potential issues or threats. Different anomalies include Data Anomalies: These occur when the data generated by IoT devices deviates from expected or normal patterns. For example, a temperature sensor reading significantly higher or lower than the usual range could indicate a malfunction or tampering.

Communication Anomalies: IoT devices rely on communication protocols to send and receive data. Anomalies in communication can include unexpected traffic spikes, unusual data packet sizes, or unusual communication patterns that may indicate network attacks or device malfunctions. Power Anomalies: IoT devices often run on battery or limited power sources. Anomalies in power consumption can signal issues such as a malfunctioning device, an energy-efficient optimization opportunity, or even a security breach. Behavioural Anomalies:

These anomalies are related to the behaviour of IoT devices. For example, a motion sensor that triggers an alert when no motion is expected or a smart thermostat that changes settings without user input could indicate unusual behaviour. Security Anomalies: Security-related anomalies are among the most critical.

They can include unauthorized access attempts, suspicious login patterns, or unusual data access by IoT devices. Detecting these anomalies can help prevent data breaches and cyberattacks. Environmental Anomalies: IoT devices often operate in specific environments. Anomalies in the environment, such as sudden changes in humidity, light levels, or air quality, can provide valuable information for various applications, from home automation to industrial monitoring.

1.3. ANOMALY DETECTION

Anomaly detection plays a pivotal role in IoT network security. It entails identifying deviations from established behaviour patterns or potential threats within the network. These anomalies can manifest as unusual data patterns, suspicious activities, or unauthorized access attempts. Effective anomaly detection is not just about responding to known threats but also anticipating and mitigating emerging risks. Detecting anomalies in IoT data typically involves using machine learning and statistical techniques.

Anomaly detection techniques include Data Collection: Collect data from IoT devices, sensors, or other sources. Data Preprocessing: Clean and preprocess the data, including handling missing values and outliers. Feature Extraction: Extract relevant features or characteristics from the data that are suitable for anomaly detection. Model Training: Train the machine learning models, like random forest, Naive bayes, K-means clustering Isolation Forest, on historical data to learn normal behaviour patterns.

Anomaly Detection: Apply the trained models to real-time or incoming data to identify anomalies by comparing current behaviour to the learned ways. Alerting and Response: When an anomaly is detected, generate alerts or take appropriate actions, such as notifying administrators or triggering automated responses. Continuous monitoring and refinement of anomaly detection models are essential in IoT environments to adapt to changing conditions and evolving threats. Additionally, anomaly detection is the most essential .

1.4. REINFORCEMENT LEARNING

Reinforcement Learning (RL), a subset of Artificial intelligence, has come out as a potential tool for IoT network security. RL models continuously observe and analyse device behaviour and data flows in the network. They learn what constitutes normal patterns of operation and interactions in the smart home environment. When anomalies or potential security breaches occur, RL models can trigger alerts, implement countermeasures, and dynamically adapt to new threats in real-time.

RL offers several advantages over other learning methodologies. It excels in dynamic and uncertain environments, ideal for IoT networks where conditions change rapidly. Unlike rule-based systems or supervised learning, RL is proactive, taking real-time actions when anomalies are detected. Its adaptability ensures it can learn and evolve to recognize new and unforeseen threats. Federated Learning complements RL in securing IoT networks by preserving data privacy. In this collaborative approach, devices train models locally, reducing the need to transmit sensitive information to centralized servers. By learning collectively without exposing individual device data, federated learning strengthens privacy and bolsters overall network security.

RL algorithms analyse device behaviour, learn normal patterns, and detect deviations indicative of anomalies or security threats. This dynamic and adaptive method safeguards sensitive data and the integrity of smart home systems. Magpie, an advanced security system, embodies these principles. Integrating RL and federated learning, Magpie refines its understanding of the smart home environment, learns from anomalies, and collectively strengthens the IoT network's security posture. This convergence ensures that our homes are not just connected but also protected.

In conclusion, IoT, machine learning, and reinforcement learning are reshaping IoT network security. This convergence of IoT and RL promises to redefine the concept of home automation, ensuring not only the seamless functioning of devices but also the protection of sensitive data and the sanctity of personal spaces. In this exploration, we delve into the exciting realm of detecting the anomalies in Smart Homes IoT Network using Reinforcement Learning, uncovering the transformative potential of this synergy and its implications for the future of residential living.

CHAPTER 2

LITERATURE REVIEW

2.1. Literature Survey

Rimsha et.al [] proposed a solution that employs the K-means clustering technique for labelling the data in an automatic way and Random Forest classification for anomaly detection, achieving robust results. This research helps to enhance the anomaly detection in IoT networks. The model utilizes the Landsat Satellite dataset, originally designed for soil categorization, but modified to include anomaly labels. The hybrid model achieves a remarkable accuracy of 98%, demonstrating its effectiveness in labelling and classifying IoT data. Challenges include the scarcity of labelled IoT datasets and computational complexity. Future work aims to explore less resource-intensive AI techniques and adapt the approach to diverse dataset types for anomaly detection in smart cities and beyond.

Xiaofeng Wang et.al [] proposed system employs a federated learning approach, aggregating local DNN models' weights and utilizing mutual information-based feature selection (MI) for improved anomaly detection. The objective is to leverage the integration of federated and deep learning concepts to swiftly analyse local edge features and centralize the results for intrusion detection, enhancing response times and thwarting attacks. Evaluation is performed using the IoT-Botnet 2020 dataset, which contains IoT traffic data, ensuring the model's effectiveness in real-world scenarios. Challenges in federated learning encompass optimizing communication efficiency, addressing security concerns, and enhancing model robustness in adversarial settings. Future research could extend the proposed model to various IoT applications, such as blockchain, and evaluate its resilience against adversarial attacks in unsupervised scenarios, further enhancing IoT security and privacy.

Kinza Arshad et.al [] proposed review covers various DRL techniques such as Deep Q learning, Actor-critic, and deep policy gradient, used for anomaly detection in diverse applications. This systematic literature review (SLR) aims to comprehensively analyse Deep Reinforcement Learning (DRL) models applied in anomaly detection, specifically focusing on their frameworks, methods, dataset usage, and performance comparisons against alternative techniques. A total of 50 different anomaly detection datasets, including network intrusion, video anomalies, and more, were identified in the selected papers. The study revealed 17 distinct DRL models performing exceptionally well for anomaly detection. DRL outperformed alternative models, demonstrating its promise in handling massive-scale datasets and various applications. Limitations include a limited number of papers available from 2017-2022. Future research should explore more anomaly detection applications, dataset types, and novel DRL variants, such as combining DRL with deep learning models.

Benaddhi H et.al [] proposed model combines Distributional Reinforcement Learning (DRL) with Generative Adversarial Networks (GANs) to create a robust intrusion detection system. It aimed to enhance anomaly detection in Industrial IoT by developing a DRL-GAN-based model to address imbalanced datasets, improving attack identification accuracy. The DS2OS dataset, sourced from Kaggle, was employed, featuring various IoT attacks and normal data points with 13 distinct features. Challenges include computational resource requirements. Future work may focus on optimizing the model and exploring additional techniques for efficient anomaly detection in IoT networks.

Jeremy watts et.al., [] In the context of connected and automated vehicles, ensuring their successful operation relies on the timely detection and isolation of anomalous or faulty information. Conventionally, this has been achieved using fixed, pre-determined thresholds for judging data anomalies, which neglects feedback and potential changes in anomaly rates during a trip. To address this limitation, a dynamic threshold approach is proposed, utilizing a mathematical framework that combines a convolutional neural network (CNN)-based anomaly classification algorithm with a partially observable Markov decision process (POMDP) model. The dynamic threshold is determined in real-time through the asynchronous advantage actor critic (A3C) deep reinforcement learning algorithm, aiming to maximize trip safety. Numerical experiments demonstrate that this POMDP model outperforms existing benchmarks, particularly in detecting challenging anomaly profiles.

Duc Hong Tran et.al [] **objective** of this study was to enhance anomaly detection in industrial sensor data within a smart manufacturing environment. The authors employed a clustering Federated Learning framework with an Autoencoder - LSTM algorithm to achieve this. The dataset utilized was sourced from 53 pump sensors, divided into 50 clients, and pre-processed for analysis. The outcome showed significant improvement in anomaly detection accuracy compared to traditional methods, with an F1-score of 97.15%. Challenges included handling imbalanced data and privacy concerns. Future research may explore blockchain and generative adversarial networks for further advancements in IoT-based anomaly detection. 13 distinct features. Challenges include computational resource requirements. Future work may focus on optimizing the model and exploring additional techniques for efficient anomaly detection in IoT networks.

Zhang et.al [] **proposes** algorithm involves training a reinforcement learning agent to

dynamically select the most suitable anomaly detection model from a pool of base models based on observed input time series and predictions of each base model. The objective of this research is to enhance time series anomaly detection by developing a dynamic model selection framework using reinforcement learning. The goal is to improve the reliability and efficiency of anomaly detection in real-world systems, where different types of anomalies with diverse characteristics exist within time series data. The research utilizes the Secure Water Treatment (SWaT) Dataset, containing multivariate time series data with 51 features, including normal and attack data, to evaluate the model. Challenges include selecting appropriate reward settings and balancing precision and recall. Future work can explore incorporating additional data sources, adapting the framework to different domains, and further optimizing the model selection process to achieve even better anomaly detection results.

Elaziz et.al., [] This study addresses the critical task of detecting anomalous behavior in business process data, a crucial aspect of ensuring organizational performance. Traditional supervised learning methods are impractical due to the challenges associated with acquiring large volumes of labelled anomaly data. Rather, the article presents a novel deep weakly supervised reinforcement learning-based method for detecting anomalies in business processes. This method makes use of a large amount of unlabelled data to discover new classes of anomalies that are not present in the labelled set, while also making use of the limited amount of labelled anomaly data. The method uses a special reward function that mixes signals from the environment's reward signal with those from a variational autoencoder trained on unlabeled data. In order to address the prevalent problem of imbalanced data, a sampling strategy is presented for efficient exploration of unlabelled data, hence mitigating data scarcity. The method depends on how close together data samples are in the variational autoencoder's latent space. In addition, the reinforcement learning model uses a large short-term memory network with a self-attention mechanism to handle long-term dependencies and model the sequential character of business process data. This suggested strategy is shown to perform better than five competing methods in a variety of experimental tests conducted on both synthetic and real-world datasets. It does this by making better use of the few available anomalous cases for anomaly detection.

Liu Y et.al, [] introduced a framework that utilizes federated learning techniques to allow distributed edge computing devices to collaboratively train the global deep anomaly detection

models. It introduces an Attention Mechanism-based Convolutional Neural Network-LSTM (AMCNN-LSTM) model to detect the anomalies in time-series data accurately. Furthermore, a Top-k selection-based gradient compression strategy is suggested to improve communication effectiveness during model training. To test the framework's anomaly detection capabilities, four real-world datasets—power demand, space shuttle, ECG, and engine data—are used. Challenges addressed in this work include timely anomaly detection for IIoT devices with privacy concerns and communication efficiency. Future research can explore further improvements in privacy-preserving techniques, scalability, and the application of this framework to a broader range of IIoT scenarios.

Bikos et.al, [] uses a Reinforcement Learning (RL) technique to create a security threat index for early threat identification and identify DAG-based nodes' resource consumption parameters. By creating an adaptive RL-based anomaly detection method, this research aims to improve the security of IOTA, a DAG-based DLT, in Internet of Things scenarios. The study assesses the effectiveness of the suggested security framework using real-time data gathered from private Tangle networks and Internet of Things devices. Challenges include addressing double-spending attacks and refining the framework using Principal Component Analysis (PCA). Future work will explore dynamic programming and decision theory for further network security enhancements.

Himani Tyagi et.al., [] This paper addresses the growing cybersecurity concerns in IoT systems, emphasizing the need for robust Intrusion Detection Systems (IDS) to combat malicious activities. The proposed IDS leverages a unique feature set derived from the BoT-IoT dataset, containing just seven lightweight features tailored to IoT and agnostic to specific attack types, avoiding potential distortion of variables through feature reduction techniques like PCA. The study uses supervised machine learning techniques like KNN, LR, SVM, MLP, DT, and RF to demonstrate how well these seven features work in detecting a variety of assaults, such as DDoS, DoS, Reconnaissance, and Information Theft. While Decision Tree and Random Forest classifiers achieve identical accuracy rates of 99.9%, Random Forest outperforms in terms of training and testing times, thus highlighting its superior efficiency in enhancing IoT security. Performance metrics such as acc., prec., recall, F-Score, and ROC are used to validate the proposed system's effectiveness.

Zhipeng Liu et.al., [] addressed the pressing issue of enhancing security in IoT networks, which are vulnerable due to the limited computational abilities of IoT devices. The paper fo-

cuses on IDS and anomaly-based network intrusion detection in particular, using various ML algorithms. The authors introduce the IoT Network Intrusion Dataset specifically designed for IoT environments and conduct experiments using logistic regression, SVM, KNN, RF, and XGBoost. Results show promising accuracy, with KNN achieving 99% accuracy and XGBoost achieving 97%, making it suitable for real-time detection. Future work includes extending to multi-class classification and developing a secure IoT framework with efficient IDS for smart environments.

Maniriho P et.al., [] proposed a novel machine learning-based anomaly approach for IoT networks. The Random Forest algorithm is used in conjunction with a hybrid feature selection engine to identify the most pertinent features and categorize each piece of traffic as normal or anomalous. The IoTID20 dataset was used to assess the approach's performance, and the findings demonstrated that it can detect DoS, MITM, and scanning attacks with a high degree of accuracy. The paper is a valuable contribution to the field of anomaly detection for IoT networks. It proposes a new approach that is effective in detecting DoS, MITM, and Scanning attacks. The approach is also evaluated using a recent and comprehensive dataset, which makes the results more reliable.

Mahmudul Hasan et.al [] The paper proposes a machine learning approach to detect attacks and anomalies in IoT sensors. The authors used the NSL-KDD dataset to train and evaluate their models. They compared the performance of five different machine learning algorithms and found that the random forest algorithm achieved the best performance, with an accuracy of 99.4%. The authors conclude that machine learning is a promising approach for detecting attacks and anomalies in IoT sensors and suggest that future work should focus on developing more efficient and scalable machine learning algorithms for IoT applications.

Liu BinXiang et.al [] presented a novel malware detection method based on deep reinforcement learning, aiming to overcome the limitations of traditional antivirus and machine learning-based approaches in handling malware variants. By combining Q-learning and neural networks, the method efficiently extracts features from Portable Executable (PE) files and uses a Deep Q-learning Network (DQN) to analyse these features, allowing for real-time adaptation to the ever-evolving landscape of malware. Experimental results demonstrate that the proposed method outperforms traditional antivirus software and showcases the potential of reinforcement learning in enhancing malware detection techniques, making it a promising direction in the field of cybersecurity.

Nguyen et.al, [] employs a GRU-based neural network for anomaly detection, utilizing historical communication data to identify deviations from normal IoT device behaviours. It also utilizes federated learning for aggregating anomaly-detection profiles. The objective of this study is to develop D-IOT, a self-learning system for detecting compromised IoT devices. It aims to autonomously create anomaly detection models without human intervention, addressing the vulnerability issues arising from insecure IoT devices. Multiple datasets, including an activity dataset capturing user interactions, a Deployment dataset for realistic scenarios, and an Attack dataset containing malicious traffic, were collected for evaluation. Challenges include the diversity of IoT devices and evolving malware. Future work can enhance scalability and adaptability to emerging threats while considering IoT device heterogeneity.

Min Seok Kim et.al [] introduced a novel 2D anomaly detection method for network intrusion detection, addressing the challenges posed by the increasing diversity of network attacks and the limitations of traditional intrusion detection approaches. The proposed method, suitable for resource-constrained environments like IoT devices, employs three distinct approaches: Binaryscale-based, original scale-based, and Grayscale-based anomaly detection. It demonstrates competitive performance compared to existing models, with Binaryscale-based detection achieving the highest accuracy. The paper also introduces a novel evaluation metric to assess the significance of detected anomalies. Overall, this research offers an innovative and efficient solution for network intrusion detection, with practical applications in IoT and autonomous vehicles.

Table 2.1. Literature survey

Title	Year	Algorithm Used	Technology	Challenge	Dataset	Acc.
A Hybrid Learning Approach for Automatic Data Labelling and Anom-	2023	K mean Clustering and Random Forest	Python programming, Intel Core i5-7200U CPU and 1 TB hard disk	Scarcity of labelled IoT datasets, computational complexity, and adaptability to various IoT do-	Landsat Satellite dataset	98%

aly Detec- tion in IoT				mains		
Federated deep learn- ing for anomaly detection on the in- ternet of things	2023	DNN and Federated Learning model	ReLU, Bi- nary cross entropy, Mutual In- formation, IoT sensor	Optimizing communication efficiency, ad- dressing security concerns, and enhancing model robustness in ad- versarial settings	IoT-Botnet 2020 da- taset	99.4%
Deep rein- forcement learning for data- efficient weakly su- pervised business process anomaly	2023	Deep rein- forcement learning, deep double Q network, LSTM, FFNN	Python, de- noising au- toencoder, BINET, VAE	Data imbalanced, No working ef- fective sampling strategy	DS1, DS2, BPIC12, BPIC17	98.9% - 83.4%
An Im- proved Sensor Anomaly Detection Method in IoT System using Fed- erated Learning	2022	Deep Neu- ral Net- works, Fed- erated learning, Deep Learning	Cyber- Physical System, Py- thon,	Maintaining time synchronization with FL, proper feature selection.	IoT- BoT- Net2020	99.67 %- 96.43 %
A Dynamic Deep Rein- forcement	2022	Reinforce- ment learn- ing, Bayesi-	Vanet, RSU, CAV	Implicit assump- tions are made	research data ex- change da-	80.4% - 94.5%

Learning-Bayesian Framework for Anomaly Detection		an network, CNN, POMDP			tabase for the Safety Pilot Model Deployment	
Deep Reinforcement Learning for Anomaly Detection: A Systematic Review	2022	DRL techniques such as Deep Q learning, Actor-critic, and deep policy gradient	IoT Devices, Video Analysis, Network Data	Privacy, Data Distribution, Algorithm Complexity, Data Quality, Scalability	50 different anomaly detection datasets	99.4%
Anomaly Detection in Industrial IoT Using Distributional Reinforcement Learning and Generative Adversarial Networks	2022	Distributional Reinforcement Learning (DRL) with Generative Adversarial Networks (GANs)	TensorFlow, Kaggle, RL framework	Computational resource requirements	DS2OS dataset	98.85 %
An Improved Sensor Anomaly Detection Method in IoT System	2022	Autoencoder Long Short-Term Memory	FL Framework	Handling imbalanced data and privacy concerns	53 pump sensors, divided into 50 clients	97.15 %

using Fed-erated Learning						
Time Series Anomaly Detection via Rein-forcement Learning-Based Model Se-lection	2022	Reinforce-ment Learn-ing-based Model Se-lection Framework for Anoma-ly Detection (RLMSAD)	PyTorch, Stable-Baselines3, High per-formance GPUs	Selecting appro-priate reward set-tings and balanc-ing precision and recall	Secure Wa-ter Treat-ment (SWaT) Dataset	Max-imum reache d 81.05 %
Deep Anomaly Detection for Time Series Data in Industrial IoT: A Communi-cation-Efficient On-device Federated Learning Approach	2021	Federated Learning and Deep Anomaly Detection, Attention Mecha-nism-based Convolu-tional Neu-ral Net-work-Long Short-Term Memory	PySyft, AWS, Communi-cation Pro-tocol	Timely anomaly detection for IIoT devices with privacy concerns and communication efficiency	Four real-world da-tasets, in-cluding power de-mand, space shut-tle, ECG, and engine data	96.85 %
Attack and anomaly detection in IoT net-works using supervised machine	2021	KNN, LR, SVM, MLP, DT, and RF	Python, AWS, IoT sensors, Raspberry pi	Complex with multiple number of algorithms be-ing implemented	BoT-IoT dataset	99.9%

learning approaches						
Reinforcement Learning-Based Anomaly Detection for Internet of Things Distributed Ledger Technology	2021	Reinforcement Learning, DAG based DLT	Distributed Ledger Technology, Private Tangle Network, Linux OS	Addressing double-spending attacks and refining the framework using Principal Component Analysis (PCA)	Real-time data collected from IoT devices and private Tangle networks	97.5%
Anomaly-based Intrusion Detection Approach for IoT Networks Using Machine Learning	2020	Random Forest, Hybrid feature selection engine	Python, Waikato environment,	Complex implementation	Dataset for Anomalous Activity Detection in IoT Networks (IoTID20)	DoS: 99.94 % MITM : 99.96 % Scanning: 99.93 %
DIOT: A Federated Self-learning Anomaly Detection System for IoT	2019	GRU-based neural network	Network protocol, Cloud Services, Audi	Diverse IoT device landscape and limited network traffic.	Activity dataset, a Deployment dataset, and an Attack dataset	95.6%
Attack and	2019	Logistic re-	Eddy cur-	Doesn't work	DS2OS	94%

anomaly detection in IoT sensors in IoT sites using machine learning approaches		gression, Support vector machine, Decision tree, random forest	rent testing,	with real-time data	from Kaggle	
---	--	--	---------------	---------------------	-------------	--

CHAPTER 3

PROBLEM STATEMENT

Internet of Things (IoT) networks consist of a multitude of interconnected devices and sensors that collect and exchange data autonomously. These networks are susceptible to various security threats, including anomalies and malicious activities. Anomaly detection in IoT networks is crucial to ensure the integrity, availability, and confidentiality of data and devices. Using reinforcement learning techniques to identify abnormal behaviors or potential security breaches in an IoT network. Anomaly detection in IoT using reinforcement learning poses several challenges, including sparse and imbalanced data, handling high-dimensional and time-series data, designing appropriate rewards, ensuring overfitting prevention and ge-

neralization. Addressing these complexities requires thoughtful algorithm selection, data preprocessing, reward engineering, and model architecture design.

CHAPTER 4

SYSTEM DESIGN

4.1. ARCHITECTURE DIAGRAM

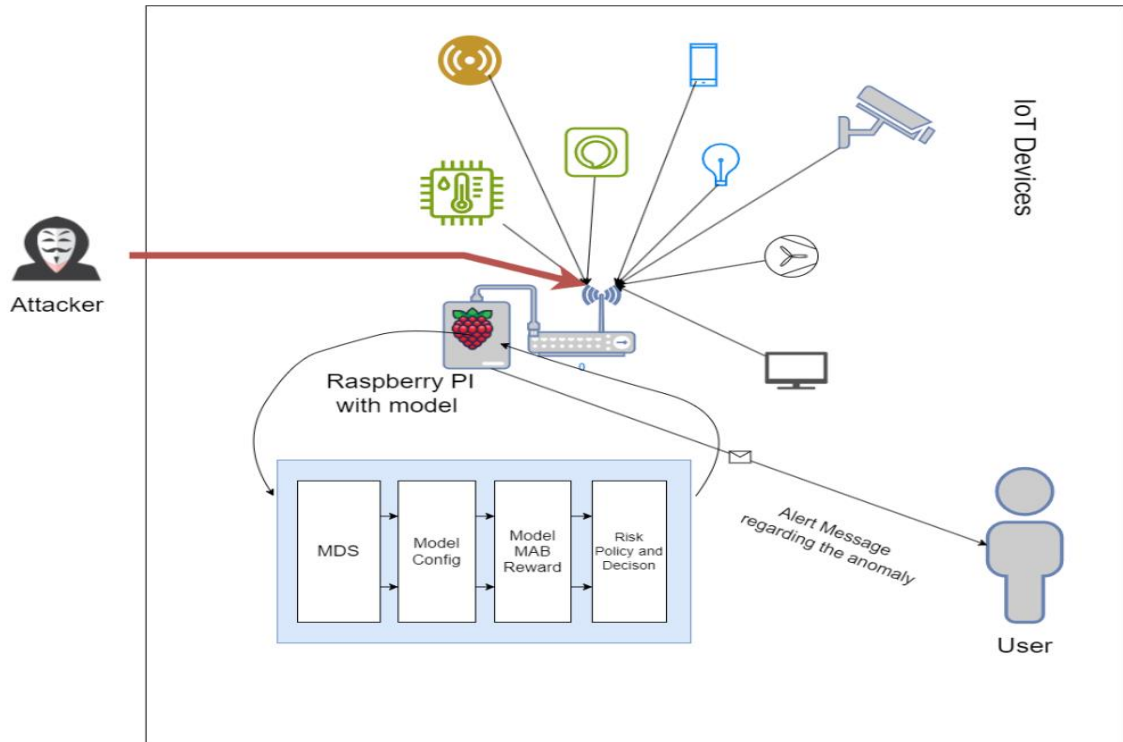


Fig. 4.1. Architecture Diagram of the proposed model

In the world of data-driven decision-making, an intricate dance unfolds as data flows from various sources, converging at a central intelligence hub. This dynamic process, laden with complexity and precision, combines IoT sensors and a cutting-edge reinforcement learning model. This fusion enables swift anomaly detection, empowering users to take prompt action in the realm of IoT networks. At its core, this system operates on the principles of reinforcement learning, leveraging a reward/state mechanism to continuously enhance its capabilities. As data pours in from IoT sensors and other sources, the model eagerly receives this influx of information for ongoing training and improvement.

A crucial element in this process is the analysis of metadata extracted from data packets. This analysis is an ongoing endeavour, conducted in real-time to ensure the system remains vigilant against anomalies and irregularities in the data stream. Before diving into the intricacies of training, data preprocessing takes place, employing the K-nearest neighbours (KNN) algorithm to refine the incoming data. This preprocessing step is essential to ensure that the model's training is based on clean and reliable data.

The raw data feeds from IoT interfaces undergo a decoding process, enabling further parsing and manipulation. This crucial step makes sure that the data is in a particular form that can be easily processed and understood by the model. A pivotal stage in this operation is the synchronization and aggregation of data from all IoT devices. This aggregation is indispensable for engineering the metadata stream, which plays a pivotal role in model identification and anomaly detection. The metadata stream, meticulously crafted, is synchronized in time and mapped according to predefined protocols and parsing logics. The inclusion of interpolation techniques further refines this data, ensuring its accuracy and reliability.

Central to this system's intelligence is the Multi-Armed Bandit (MAB) reward generation algorithm. This algorithm, a cornerstone of the reinforcement learning model, is responsible for generating rewards based on the model's performance. These rewards fuel the continuous training process, allowing the model to adapt and improve in real-time. The training itself is a two-fold process. First, the data is divided into training and testing sets to facilitate rigorous evaluation. Then, hyperparameter tuning algorithms are applied to fine-tune the model's configuration, ensuring optimal performance and adaptability.

In summary, this sophisticated system seamlessly integrates IoT sensors and a reinforcement learning model to detect anomalies in data streams. It employs a range of techniques, from preprocessing with KNN to metadata stream engineering and reward generation through MAB algorithms. This holistic approach ensures that the model remains vigilant, adapting and evolving as it encounters new data, ultimately empowering users to take swift action in the ever-evolving landscape of IoT networks.

4.2. PROPOSED MODEL

The data collection phase of this model is in charge of gathering and interpreting data from multiple sources, including physical feeds like audio or signal strength and cyber feeds (computation and communication). It can decode the associated raw feeds, which could include network datagrams or sensor readings, and dynamically activate or deactivate interfaces. A substantial amount of encrypted data is produced by smart homes, and the amount varies widely depending on the surroundings. The model concentrates on consistent metadata across

various smart homes during the transcription phase. Unlike other approaches that require encrypted and authenticated device API queries or passively intercept content using decryption keys, ours avoids becoming a single point of failure and an attack target. By focusing only on smart home network communication flow metadata, this model is better positioned to protect privacy.

Using particular DataStream parsing logic, the model extracts metadata streams (MDS) for interfaces such as communication, applications, and sensor protocols. It uses a rolling window-based parser extraction and buffering system to guarantee processing efficiency. Following the process of aggregation, statistical data such as mean, standard deviation, minimum, maximum, sample frequency, content/message type, size, length, delay, and flow direction are extracted from the metadata features. The inter-arrival rate, measured in milliseconds, between packets or frames for identical source-destination message type pairs is represented by the delay metadata feature. For example, Table I shows sample volume and inter-arrival rates in a 5-minute window during times when occupant activity is low in our smart home testbed.

Table 4.1. A 5-min capture of DataStream sample (inter-arrival time in seconds.)

Datastream	Samples	Average	Minimum	Maximum	Standard Deviation
IP	569	0.536	0.00002	4.0338	0.9539
Wi-Fi	3555	0.089	0.0008	0.2048	0.1023
Sound	12465	0.024	0.0121	0.0718	0.0146
Zigbee	390	0.784	0.0002	5.387	1.3882
RF	300	1	1	1	0

These findings demonstrate that it is not feasible to analyze DataStream samples in real-time on resource-constrained platforms without windowing and buffering. Furthermore, throttling, file size, and upstream network bandwidth restrictions may make handling such massive volumes of data difficult. A synchronized "end of window" DataStream buffer is where parsing instances start the process of windowing, which includes feature extraction, interpolation, discretization, and statistical data generation.

After that, the DataStream window is sent to an interpolation and parsing logic phase. In this

phase, raw DataStream is used for metadata extraction and feature interpolation, which are identified using protocol mapping identifiers (such as addressing and data type). As a result, an aggregated sample (aMDS) is created by combining data points from all MDS DataStreams into the MDS window feed, which is then sent to the MDS datastore for storage. In addition to taking snapshots of MDS data samples for use in reinforcement learning-based adaptation, the datastore serves as a data historian for anomaly detection training.

Common statistical features from all MDS feeds are extracted by the aMDS fusion and used to train a presence inference function inside the smart home. Even though each MDS may have a different sample rate, the aMDS dataset aggregates common features from all MDS feeds to produce a single feature-vector sample per window. The window buffering latency plus the prediction latency of the reasoning engine add up to the real-time threat monitoring latency.

During each monitoring window interval, all received MDS feeds are processed, interpolated, normalized, and scaled in real-time. In order for concept discovery training data to learn "normal" behavior and produce an independent anomaly detection model for every interface, this process supplies the feature structures that are required. Please be aware that the sample rate, the type of data source, and whether the data source is connection-oriented all affect how complex the model transcription phase is. For instance, the computational complexity for network data sources (IP, WiFi, ZigBee) is $O(n\delta)$, where δ is the computation of unique source-destination pairs and n is the number of samples per window. The computational complexity for physical data sources (RF and Audio) is $O(n)$. Each isolation forest model has an individual linear time complexity of $O(\mu\psi \log\psi)$ for training.

Algorithm:

Algorithm for the IDS RL reward

```
func Reward:
  for t ∈ [1, T] do
     $A_x \leq a_{t,x}$ 
  end
```

```

    k=2;
    Cx = KMeanclust(Ax, k);
    Rx,i = SilhouetteScore(Cx);
    return Rx,i;
end func

```

The reward logic can be summarized as follows: within a given time window range $[1, T]$, each Multi-Armed Bandit (MAB) iteration corresponds to a specific action-state, which is represented by a contamination hyperparameter denoted as x . We define " a_x " as the vector containing all anomaly scores for x over various time windows and " $a_{t,x}$ " as the anomaly score value for the contamination hyperparameter x at time window t . Then, using Euclidean distance and K-means clustering, we generate two clusters: one with higher anomaly scores and the other with lower scores. The silhouette score, which measures the degree of cluster similarity, is used to compute the reward value for a specific snapshot, represented by the notation " $R_{x,i}$ ".

CHAPTER 5

EXPERIMENTAL WORK

After conducting a comprehensive evaluation of our prototype system by seamlessly integrating it within a real household's smart home, which consisted of three occupants. This integration was executed to assess the system's performance and effectiveness. In this setup, we deployed a variety of devices, each governed by specific automation rules that enhanced the overall functionality of the smart home.

The smart home infrastructure featured a standard home Internet router, which served as the central hub for all network operations. This router supported a WiFi local area network, catering to WiFi-enabled devices, and a ZigBee gateway, facilitating communication with Zigbee devices. These devices were all inter-connected with the home router via Ethernet, allowing them to interact with one another seamlessly. Moreover, to enable remote connectivity and control, we leveraged cloud services, which extended access to WiFi and ZigBee devices over the internet.

The prototype system, which was powered by a Raspberry Pi, played a pivotal role in this setup. Via an Ethernet SPAN port on the home router, the Raspberry Pi was in charge of keeping an eye on and recording all local and Internet traffic. Its ZigBee and WiFi interfaces also passively observed network frames on their assigned RF channels, guaranteeing the integrity and safety of the wireless networks. A software-defined radio (SDR) interface was also used by the system to record spectrum readings in the 2.4 GHz WiFi and ZigBee frequency range. Moreover, the Raspberry Pi had a microphone attached directly to it, which improved its ability to identify anomalies or intruders.

Table 5.1. Different types of attacks on IoT networks and their impact

Attack	Layer	Cyber Impact	Physical Impact
Wifi Deauth	Data Link	Availability	Prevention and Delayed Actuation
Wifi Evil Twin	Data Link	Confidentiality, Integrity and Availability	Prevention and Delayed Actuation
ZigBee Jamming	Physical	Availability	Prevention Actuation
ZigBee node	Network	Integrity and Availability	Delayed Actuation

amplification		lity	
Malware Audio Injection	Physical & Application	Integrity	Unauthorized
Security Camera	Application	Confidentiality	Unauthorized and Breach Actuation
Workflow automation	Application	Confidentiality	Unauthorized and Breach Actuation

This smart home environment was not only susceptible to local threats but also remote attacks. An adversary within the smart home's wireless range may be able to carry out WiFi and ZigBee attacks with the use of specialized hardware, such as an attack laptop, SDR peripherals, and ZigBee antennas with customized firmware. The adversary may also use compromised cloud services or compromised devices to launch a remote attack against the smart home.

The setup of the detection system is done using the raspberry PI4 device. Once the Raspberry PI is boot loaded with the same wifi network as the system remote access to raspberry PI device is obtained.

CHAPTER 6

RESULT & ANALYSIS

```
pi@raspberrypi: ~  
SHA256:cSZgmjDKv3Y9bRohrOj3zE6b70VcAFuPY3Fj3v2Hq14.  
Please contact your system administrator.  
Add correct host key in C:\\Users\\karth/.ssh/known_hosts to get rid of this message.  
Offending ECDSA key in C:\\Users\\karth/.ssh/known_hosts:3  
Host key for 192.168.78.68 has changed and you have requested strict checking.  
Host key verification failed.  
  
C:\\Windows\\System32>ssh-keygen -R 192.168.78.68  
# Host 192.168.78.68 found: line 1  
# Host 192.168.78.68 found: line 2  
# Host 192.168.78.68 found: line 3  
C:\\Users\\karth/.ssh/known_hosts updated.  
Original contents retained as C:\\Users\\karth/.ssh/known_hosts.old  
  
C:\\Windows\\System32>ssh pi@192.168.78.68  
The authenticity of host '192.168.78.68 (192.168.78.68)' can't be established.  
ED25519 key fingerprint is SHA256:cSZgmjDKv3Y9bRohrOj3zE6b70VcAFuPY3Fj3v2Hq14.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.78.68' (ED25519) to the list of known hosts.  
pi@192.168.78.68's password:  
Linux raspberrypi 5.10.103-v7l+ #1529 SMP Tue Mar 8 12:24:00 GMT 2022 armv7l  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
pi@raspberrypi:~$
```

Fig. 6.1. Establishing SSH connection to the raspberry PI

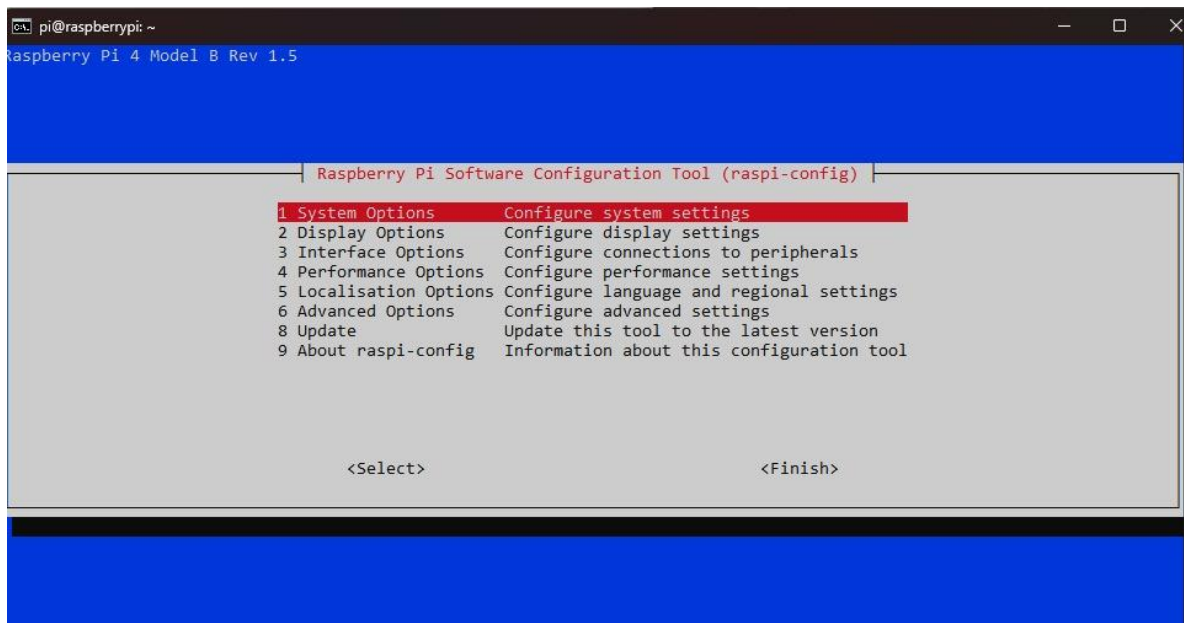


Fig. 6.2. Raspberry PI configuration

```

pi@raspberrypi: ~/Desktop/projec...ie-master/v1.0/RaspberryPi Build
File Edit Tabs Help

pi@raspberrypi:~/Desktop/project/magpie-master/v1.0/RaspberryPi Build $ ls
dpkg-selections.txt  magpie_datapreproc.py  magpie_run.pyc  __pycache__
get-pip.py           magpie_datapreproc.pyc  magpie_train.py  wifimon_init.sh
init_magpie.sh       magpie_main.py         magpie_train.pyc
jackdaw_init.sh      magpie_run.py          push_feed.py
pi@raspberrypi:~/Desktop/project/magpie-master/v1.0/RaspberryPi Build $ python m
agpie_datapreproc.py
pi@raspberrypi:~/Desktop/project/magpie-master/v1.0/RaspberryPi Build $ s

```

Fig. 6.3. Performing Data Pre-processing On the Dataset

A	B	C	D	E	F	G	H	I	J
timestamp	src	dest	freq	subtype	avg_sz	avg_rssi	std_rssi	avg_del	std_del
1.55E+09	8c:0d:76:64	90:70:65:2d	2	5	302	-3	0	3805	0
1.55E+09	8c:0d:76:64	ff:ff:ff:ff:ff	31	8	193	-2.55	0.51	102316.93	104068.77
1.55E+09	f0:18:98:10	ff:ff:ff:ff:ff	2	4	158	-6	0	9612	0
1.55E+09	8c:0d:76:64	f0:18:98:10	7	5	302	-3	0	9970	15426.97
1.55E+09	8c:0d:76:64	ff:ff:ff:ff:ff	27	8	193	-2.48	0.51	102383.69	104418.18
1.55E+09	8c:0d:76:64	ff:ff:ff:ff:ff	30	8	193	-2.87	0.35	102379.93	104194.21
1.55E+09	8c:0d:76:64	90:70:65:2d	8	5	302	-3	0	4664.71	5723.71
1.55E+09	8c:0d:76:64	ff:ff:ff:ff:ff	29	8	193	-3	0	102399.29	104281.62

Fig. 6.4. Data samples before pre-processing

A	B	C	D	E	F	G	H	I	J
timestamp	src	dest	freq	subtype	avg_sz	avg_rssi	std_rssi	avg_del	std_del
1.55E+09	8c:0d:76:64	ff:ff:ff:ff:ff	31	8	193	-2.77	0.43	102407.87	104158.61
1.55E+09	8c:0d:76:64	90:70:65:2d	3	5	302	-2.67	0.58	10872	18329.62
1.55E+09	8c:0d:76:64	ff:ff:ff:ff:ff	25	8	193	-2.68	0.48	102453.96	104657.83
1.55E+09	8c:0d:76:64	ff:ff:ff:ff:ff	31	8	193	-2.71	0.46	102396.9	104154.42
1.55E+09	8c:0d:76:64	ff:ff:ff:ff:ff	30	8	193	-2.77	0.43	102401.17	104215.49
1.55E+09	8c:0d:76:64	ff:ff:ff:ff:ff	31	8	193	-2.77	0.43	102419.6	104179.62

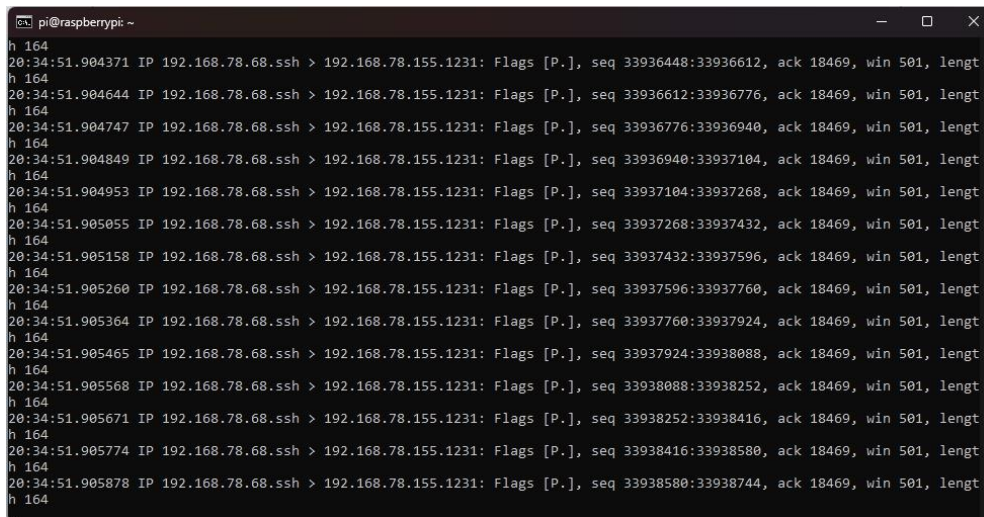
Fig. 6.5. Data samples after pre-processing

```

IA ERRORS W  GROUPED W  OVERRUNS W  CARRIER W  COLLISIONS W
(karthikeya@kali)-[~]
$ sudo hping3 -S --flood -V -p 1234 10.0.2.15
using eth0, addr: 10.0.2.15, MTU: 1500
HPING 10.0.2.15 (eth0 10.0.2.15): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

```

Fig. 6.6. Performing DOS attack



```

pi@raspberrypi: ~
h 164
20:34:51.904371 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33936448:33936612, ack 18469, win 501, lengt
h 164
20:34:51.904644 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33936612:33936776, ack 18469, win 501, lengt
h 164
20:34:51.904747 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33936776:33936940, ack 18469, win 501, lengt
h 164
20:34:51.904849 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33936940:33937104, ack 18469, win 501, lengt
h 164
20:34:51.904953 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33937104:33937268, ack 18469, win 501, lengt
h 164
20:34:51.905055 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33937268:33937432, ack 18469, win 501, lengt
h 164
20:34:51.905158 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33937432:33937596, ack 18469, win 501, lengt
h 164
20:34:51.905260 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33937596:33937760, ack 18469, win 501, lengt
h 164
20:34:51.905364 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33937760:33937924, ack 18469, win 501, lengt
h 164
20:34:51.905465 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33937924:33938088, ack 18469, win 501, lengt
h 164
20:34:51.905568 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33938088:33938252, ack 18469, win 501, lengt
h 164
20:34:51.905671 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33938252:33938416, ack 18469, win 501, lengt
h 164
20:34:51.905774 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33938416:33938580, ack 18469, win 501, lengt
h 164
20:34:51.905878 IP 192.168.78.68.ssh > 192.168.78.155.1231: Flags [P.], seq 33938580:33938744, ack 18469, win 501, lengt
h 164

```

Fig. 6.7. Result of the DoS attack in the tcpdump of raspberry PI

Data preprocessing is a critical and often overlooked phase in any data-driven project, whether it's machine learning, data analysis, or any data-centric application. Its importance cannot be overstated as it directly impacts the quality and reliability of your results. First and foremost, data preprocessing is crucial for ensuring the data's quality and consistency. Raw data often contains missing values, outliers, noisy data points, or inaccuracies. By cleaning and preprocessing the data, you can address these issues, resulting in a more accurate and reliable dataset. Furthermore, data preprocessing can help in feature engineering, where you create new features or transform existing ones to improve the model's performance. Properly scaled and normalized data can lead to better model convergence and predictions. Another significant aspect is data reduction and dimensionality reduction, which can help eliminate redundant or irrelevant features, making the model more efficient and easier to interpret.

CHAPTER 7

CONCLUSION

In this exploration of IoT network security, we delved into the transformative impact of Reinforcement Learning (RL) and anomaly detection techniques, particularly in the context of smart homes. The Internet of Things (IoT) has revolutionized the way we interact with technology, especially within smart homes, where IoT networks serve as the backbone connecting

a myriad of devices. However, with this interconnectedness comes security challenges, necessitating innovative solutions.

Anomalies in IoT, ranging from data irregularities to behavioral anomalies and security-related threats, pose significant risks. Recognizing the importance of anomaly detection, we explored the pivotal role it plays in IoT network security. Machine learning techniques, especially RL, emerged as powerful tools in continuously monitoring device behavior and dynamically adapting to potential threats.

Reinforcement Learning, a subset of Artificial Intelligence, demonstrated its prowess in smart home environments where conditions change rapidly. Its adaptability, proactivity, and real-time response to anomalies set it apart. The integration of Federated Learning further addressed privacy concerns by preserving data confidentiality in a collaborative training approach.

The proposed model's architecture, outlined in Chapter 4, showcased a sophisticated blend of IoT sensors and RL models. This fusion enabled swift anomaly detection, empowering users to take prompt action. The Multi-Armed Bandit reward generation algorithm played a crucial role, ensuring continuous model improvement based on real-time performance.

The experimental work, conducted in a real smart home environment, provided insights into the practical application of the proposed model. The system, powered by a Raspberry Pi, demonstrated its effectiveness in monitoring and recording local and internet traffic, RF channels, and spectrum readings.

The data preprocessing phase emerged as a critical aspect, ensuring the quality and reliability of the dataset. Addressing missing values, outliers, and noise, data preprocessing laid the foundation for accurate anomaly detection. Additionally, the importance of feature engineering, scaling, and dimensionality reduction highlighted the holistic approach required for robust IoT network security.

In conclusion, the synergy of IoT, machine learning, and reinforcement learning is reshaping the landscape of network security. The proposed model, with its emphasis on anomaly detection and continuous improvement through RL, presents a promising avenue for safeguarding smart home environments. As we navigate the ever-evolving IoT ecosystem, the integration of cutting-edge technologies becomes paramount in ensuring not only seamless device func-

tioning but also the protection of sensitive data and the sanctity of personal spaces. This exploration sets the stage for a future where innovation in IoT security aligns with the dynamic nature of emerging threats, fostering a secure and connected living environment.

References

1. Kanwal, R., Noor, U., & Rashid, Z. (2023). A Hybrid Learning Approach for Automatic Data Labelling and Anomaly Detection in IoT Networks. 3rd IEEE International Conference on Artificial Intelligence, ICAI 2023, 238–241. <https://doi.org/10.1109/ICAI58407.2023.10136687>
2. Wang, X., Wang, Y., Javaheri, Z., Almutairi, L., Moghadamnejad, N., & Younes, O. S. (2023). Federated deep learning for anomaly detection on the internet of things. Computers and Electrical Engineering, 108, 108651. <https://doi.org/https://doi.org/10.1016/j.compeleceng.2023.108651>
3. Elaziz, E. A., Fathalla, R., & Shaheen, M. (2023). Deep reinforcement learning for data-efficient weakly supervised business process anomaly detection. Journal of Big Data, 10(1). <https://doi.org/10.1186/s40537-023-00708-5>
4. Tran, D. H., Nguyen, V. L., Utama, I. B. K. Y., & Jang, Y. M. (2022). An Improved Sensor Anomaly Detection Method in IoT System using Federated Learning. 2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN), 466–469. <https://doi.org/10.1109/ICUFN55119.2022.9829561>
5. Benaddi, H., Jouhari, M., Ibrahimi, K., ben Othman, J., & Amhoud, E. M. (2022). Anomaly Detection in Industrial IoT Using Distributional Reinforcement Learning and Generative Adversarial Networks. Sensors, 22(21). <https://doi.org/10.3390/s22218085>
6. Arshad, K., Ali, R. F., Muneer, A., Aziz, I. A., Naseer, S., Khan, N. S., & Taib, S. M. (2022). Deep Reinforcement Learning for Anomaly Detection: A Systematic Review. In IEEE Access (Vol. 10, pp. 124017–124035). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/ACCESS.2022.3224023>
7. Zhang, J. E., Wu, D., & Boulet, B. (2022). Time Series Anomaly Detection via Reinforcement Learning-Based Model Selection. Canadian Conference on Electrical and Computer Engineering, 2022-September, 193–199. <https://doi.org/10.1109/CCECE49351.2022.9918216>

8. Liu, Y., Garg, S., Nie, J., Zhang, Y., Xiong, Z., Kang, J., & Hossain, M. S. (2021). Deep Anomaly Detection for Time-Series Data in Industrial IoT: A Communication-Efficient On-Device Federated Learning Approach. *IEEE Internet of Things Journal*, 8(8), 6348–6358. <https://doi.org/10.1109/JIOT.2020.3011726>
9. Tyagi, H., & Kumar, R. (2021). Attack and anomaly detection in IoT networks using supervised machine learning approaches. *Revue d'Intelligence Artificielle*, 35(1), 11–21. <https://doi.org/10.18280/ria.350102>
10. Bikos, A. N., & Kumar, S. (2021). Reinforcement Learning-Based Anomaly Detection for Internet of Things Distributed Ledger Technology. *Proceedings - IEEE Symposium on Computers and Communications*, 2021-September. <https://doi.org/10.1109/ISCC53001.2021.9631384>
11. Liu Zhipeng, K. R. et. al, Institute of Electrical and Electronics Engineers. South African Section, & Institute of Electrical and Electronics Engineers. (2020). Anomaly Detection on IoT Network Intrusion Using Machine Learning.
12. Maniriho, P., Niyigaba, E., Bizimana, Z., Twiringiyimana, V., Mahoro, L. J., & Ahmad, T. (2020). Anomaly-based Intrusion Detection Approach for IoT Networks Using Machine Learning. *CENIM 2020 - Proceeding: International Conference on Computer Engineering, Network, and Intelligent Multimedia 2020*, 303–308. <https://doi.org/10.1109/CENIM51130.2020.9297958>
13. Nguyen, T. D., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., & Sadeghi, A.-R. (2019). D²IoT: A Federated Self-Learning Anomaly Detection System for IoT. *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 756–767. <https://doi.org/10.1109/ICDCS.2019.00080>
14. Hasan, M., Milon Islam, M., Ishrak Islam Zarif, M., & Hashem, M. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. <https://doi.org/10.1016/j.iot.2019.10>
15. Binxiang, L., Gang, Z., & Ruoying, S. (2019). A deep reinforcement learning malware detection method based on PE feature distribution. *Proceedings - 2019 6th International Conference on Information Science and Control Engineering, ICISCE 2019*, 23–27. <https://doi.org/10.1109/ICISCE48695.2019.00014>
16. Seok Kim, M., Hoon Shin, J., & Seon Hong, C. (n.d.). Network Intrusion Detection System using 2D Anomaly Detection.