AJEMA GLOBAL RESEARCH NETWORK

AMERICAN Journal of Engineering, Mechanics and Architecture
Volume 1, Issue 6, 2023 ISSN (E): 2993-2637

Develop Automated Systems that Gather and Analyze Threat Data to Protect Business Systems Automatically from Cyberattacks

Tanvir Rahman Akash, Md Sultanul Arefin Sourav
Master of Business Analytics, Trine University, Phoenix, Arizona

Sanjida Akter Sarna
National University of Bangladesh, Gazipur, Dhaka

Md Rakibuzzaman
Officer at Department of Banking Inspection, Bangladesh Bank, Dhaka, Bangladesh

Abstract: The explosive growth of inter-connectivity of IoT devices has changed the modern-day world of living as well as the industrial environment, providing increased connectivity and automation. This expansion has brought major cybersecurity weak spots especially in the case of real time IoT networks, where legacy security mechanisms are usually ineffective. This research explores approaches to cyberattack detection through the usage of the RT-IoT2022 dataset, which is a large and free resource that emulates real one's traffic of the IoT devices. The dataset contains not only benign traffic, but a wide range of cyberattacks: SSH brute-force, Hping based DDoS, Slowloris, ARP poisoning and multiple Nmap scanning variants. Our study uses machine learning to class and identify irregular behavior in network traffic. After intensive data pre-processing including feature selection and feature normalization, trained and assessed several supervised learning models such as Random Forest, XGBoost, Support Vector Machines (SVM) and Logistic Regression. The models were tested using metrics of performance such as accuracy, precision, recall F1-score and Area Under the Curve (AUC). Results show that ensemble-based classifiers perform particularly well on Random Forest and XGBoost in distinguishing between benign and malicious flows because of the ability to capture nonlinear relationships among the 80 bidirectional flow features of the dataset. In addition, the analysis points to the importance of real-time traffic parameters – packet duration, flow directionality and protocol distribution – for efficient intrusion detection. This paper strengthens the expanding body of research on IoT security; it shows how it is possible to use machine learning and rich network flow to increase real-time attack identification in complex IoT environments.

Keywords: IoT Security, Cyberattack Detection, Real-Time Monitoring, RT-IoT2022, Machine Learning, Network Intrusion (NIDS).

1. Introduction

1.1 Significance of Cybersecurity in IoT Ecosystems

The advancement of digital ecosystems has resulted from the revolution of the Internet of Things (IoT) through interconnecting devices, sensors, and systems in various domains including, healthcare, transportation, manufacturing, and smart homes. These connected devices gather, share and process enormous amounts of data to allow frictionless automation and more effective decision making. The increasing dependency on IoT infrastructures, has forced us to take

cybersecurity issues to high waters. Unlike the traditional IT systems, the IoT devices are frequently under resource-constrained conditions, do not have built-in protection mechanisms and are being deployed in dynamic, distributed environments, hence they are highly exposed to cyber risks. A successful cyberattack on a desperately-needed IoT network can disservice, endanger lives and compromise sensitive information [1]. Thus, providing cybersecurity to IoT ecosystems does not provide only the technical need but a necessity to maintain data integrity, operational sustainability & public confidence. The more IoT adoption keeps increasing, the need to bolster its cyber defense mechanisms intensifies in developing robust digital infrastructures that can be able to adjust to new threats and provide safe and continuous operation within connected settings.

1.2 Emergence of Smart Devices and their vulnerability

The increasing number of smart devices including wearable health trackers in our homes and industry sensors and connected vehicles has completely transformed the IoT landscape as more and more devices enter the market with each passing day. Although these innovations ensure convenience and operational efficiency, they create new forms of cyber security problems. Many IoT devices are produced with minimal security mechanisms including: default credentials, unpatched firmware, or no protocols for encryption. Such weaknesses are attractive targets for attackers who abuse them to gain unauthorized access or exfiltrate data or use them as landing pads for massive escalated distributed attacks. IoT devices frequently work in unmanned environments and there is no regular update of the software, and they cannot be monitored in real time. Their constant connectivity and large attack surface make it more likely that successful intrusions occur [2]. With the number of smart devices exceeding the implementation of strong security frameworks, both organizations and users are adversely affected with great risks. Therefore, the weaknesses of smart devices highlight the necessity of cutting-edge, scalable, and real-time cyber security solutions ad-hoc to the IoT environments.

1.3 Real Time Threats and Traditional Defenses Rationalize Failure

Real time IoT environments require fast unbroken data sharing between heterogeneous devices and platforms. This changing dynamic and timely nature set a good environment for advanced cyber threats. Attackers using anomalous traffic could exploit weaknesses to inject malicious flow, causing service denial or stealing control of a system without sounding traditional defenses. Traditional armor for example, firewalls, static rule-based system, periodic security scans cannot protect IoT ecosystems well enough on their own. These defenses usually use predefined signatures or known trending threat vectors and hence are of little use against zero days, polymorphic malware, and evolving techniques used by adversaries. Resource constrained IoT devices do not possess the computational capability to host conventional antivirus/endpoint protection software [3]. The IoT networks further pose the challenge of threat detection and incident response by its decentralized and distributed aspects. For this reason, are seeing an increased demand for adaptive intelligent security mechanisms to identify anomalies and cope with threats in time. This means moving away from static security protocol into dynamic and data driven approaches that will use Machine learning and behavioral analytics to operationalize.

1.4 Introduction of RT-IoT2022 Dataset as a benchmark for IoT attacks analysis

Realtime Iot-2022 dataset has developed into an important benchmark for research and development around the security of real-time IoT networks. This dataset is engineered around realistic scenarios, where bidirectional traffic flows in all types of attacks had been mapped, including SSH brute-force, ARP poisoning, DDoS (Hping and Slowloris), and diverse Nmap techniques for scanning [3]. Unlike numerous other synthetic or outdated datasets, RT-IoT2022 is a rich metadata dataset with more than 80 per entry network flow features, making it possible for researchers to study behavioral patterns with high granularity. It creates a smart environment of interconnected IoT nodes, simulates benign and malicious traffic, and makes it very valuable to learning and testing intrusion detection systems. The dataset is structured, labels, and its

diversity of attack vectors allow for the creation of machine learning models to differentiate subtle threat behaviors from actual activity. By providing an authoritative and exhaustive model of real time IoT traffic of today the RT-IoT2022 dataset assists in making research reproducible and enables accelerating developments of real time cybersecurity solutions for the IoT world.

1.5 Objectives of the Paper

This research paper intends to study the ability of machine learning techniques to detect cyberattacks in real-time IoT networks. Based on the RT-IoT2022 dataset, the study examines the attack patterns of benign and malicious traffic based on multiple attack categories. The main purpose is to assess the performance of different supervised learning classifiers in their capacity to correctly identify anomalous behaviors [4]. The paper aims to explore central network flow characteristics associated with the highest attack detection. It also discusses the constraints of past security approaches, and how intelligent models can improve real time detection methods. Using empirical results, the study seeks to offer actionable input as to how to deploy exhaustive cybersecurity frameworks in IoT environments.

1.6 Research Questions

This study demonstrates the following questions are:

- To what degree can differently cyberattacks in real-time IoT networks be detected in real-time using the RT-IoT2022 dataset with machine learning models?
- Which supervised learning algorithms are most effective, when measured by precision, recall, and overall detection accuracy?
- Which are the most dominating network flow characteristics to differentiate between malicious traffic from the regular one between IoT communication?
- What can be observed about smart models when compared with signature-based detection techniques for real-time scenarios?
- Is it possible for models to effectively generalize to different attacks present within the RT-IoT2022 dataset?

1.7 Significance of the Study

This study is of significant interest in the developing discipline of IoT cybersecurity. With billions of smart devices linked to critical infrastructure and humans' spaces, there has never been a more critical time for real-time scalable intelligent detection mechanisms. Making use of the RT-IoT2022 dataset and machine learning algorithms, this research supplies empiric proof concerning the ways artificial intelligence could increase detection accuracy and response time in a complex IoT environment [6]. It provides a holistic perspective of traffic patterns resulting from multiple cyberattacks; hence, it supports the work of security researchers and practitioners who can trace out critical weaknesses and sharpen defensive measures. The results of this study provide answers to the problem of the gap between academic research and practical solutions, particularly, in the case of resource- constrained and decentralized IoT systems [7]. The paper encourages the implementation of data-driven security models capable of being dynamic to assist organizations in creating stronger and secure infrastructures for IoT. It also acts as a reference point for any forthcoming research that aims at improving and benchmarking real-time intrusion detection systems.

2. Literature Review

Studies especially cite the increasing need for strong cybersecurity in IoT networks based on a rising sensitivity to attack complexity and device weaknesses. Conventional IDS based on signatures do not work well in real time IoT environments [8]. Researchers have therefore investigated the use of Machine Learning (ML) models such as Decision Trees, SVMs and deep learning-based models to detect anomalies from the behavior of network traffic. Nevertheless,

many of them use the old ones or not IoT-specific datasets. The RT-IoT2022 dataset responds to this gap; providing real-time pervasive diverse attack scenarios [9]. Existing literature also points to the difficulty of balancing accuracy of the model with resource efficiency in a constrained IoT environment thus underscoring the need for lightweight adaptive IDS solutions.

2.1 Evolution of IoT Security Research

The Internet of Things has transformed the world to one which has made communication and automation of processes a reality across all sectors. This innovation, though rewarding efficiency and convenience, has also presented a wide range of security questions. The traditional IoT security endeavors were largely based on the crypto approach, secure protocols, and perimeter defenses. These initial solutions were not architected to support the modern IoT networks; they lacked scale, heterogeneity, and dynamics. The capacity limitations of the IoT devices for processes and storage make the standard security measures have insufficient protection. As cyberattacks grew more complex and frequent security research started moving towards more adaptive and behavior-based research. Such platforms comprise lightweight detection mechanisms, context-aware protocols, and real-time monitoring tools that will be used on IoT infrastructures [10]. As data driven analytics have grown, machine learning has become integral to contemporary IoT defense strategies, whereby systems can identify weak behavioral signatures. Despite these advancements, challenges persist. Very often IoT devices function under severe energy and computational constraints, which makes it difficult to implement advanced security mechanisms. Furthermore, the variety of applications available in the IoT, including smart homes and industrial automation, makes universal security arrangements even more complicated. Therefore, the continued innovation is necessary to create scalable, intelligent, and efficient security solutions suited to this dynamically changing IoT threat environment.

2.2 Machine Learning in Cyberattack Detection

Machine learning (ML) has become a key part of contemporary cybersecurity infrastructure (societal), especially in identifying attacks in complicated and ever-changing IoT milieus. Unlike traditional security systems that base their defense on established rules or signatures of attack, ML models learn from the enormous amount of data available in the network traffic and adjust to catch such threats which were not conceived before. Various supervised algorithms including, decision trees, random forests, SVM's and the naïve Bayes classifiers algorithm, are regularly used to classify traffic using observed patterns. Such models can detect variations in size, frequency, protocols used and communication behavior which are pointers to possible intrusion [11]. Other more sophisticated techniques, including deep learning models, provide additional capabilities through the ability to discover nonlinear things and to detect temporal relationships. Recurrence neural networks and convolutional neural networks have been proven useful in extracting time-series anomalies and spatial patterns in traffic flows. While these methods are accurate, they frequently demand strong amounts of computation, posing a challenge for resource-limited IoT appliances [12]. Furthermore, data distribution imbalances, where benign traffic is more than malicious ones, leads to sample skewing. Hybrid models which combine the lightweight feature selection and ML algorithms have been proposed. These are designed with the intent of minimizing computational requirements without the compromise of detection accuracy. ML provides a flexible/scalable detection solution to cyberattacks in the scenario where they are trained on representative real-world with IoT data.

2.3 Real Time Intrusion Detection Systems (IDS) for IoT

Those real-time intrusion detection systems (IDS) are critical for having IoT networks protected because even tiny leverages in threat detection times can lead to large breaks. Whereas, the conventional systems do not have to make use of continuous, time-sensitive data exchange, environmental IoT systems often must face such a challenge and for this reason, latency and responsiveness are extremely important factors to be considered [13]. While traditional IDS

solutions work well in enterprise environments, they typically turn out to be too onerous or inflexible for their deployment in an IoT context. Such systems tend to be too power and processor hungry, exceeding what can be supported with embedded IoT hardware. research has moved in direction of lightweight and adaptive IDS models adapted to the constraints in IoT. Such systems employ lean features and detection algorithms to provide real time performance at zero sacrifice of resources availability. Hybrid detection modalities, which use a combination of statistical anomaly detection with machine learning classifiers go hand in hand with the requirement of accuracy and speed [14]. Such models can easily pick on unusual behavior patterns while adjusting to changing behaviors of networks. There are still many challenges in getting real-time detection to be effective. High accuracy while minimizing false positives is challenging with dynamic environments and changing traffic patterns. real-time IDS must be energy minimally demanding and small in footprint [15]. Answering these trade-offs are key to advancing practical IDS deployments for the IoT, highlighting the requirements of context-aware and scalable designs that work independently in varied and distributed device ecosystems.

2.4 Importance of the Benchmark Datasets in the Research on IoT Security

Benchmark datasets are important in IoT cybersecurity research because they give standardized records of traffic that can be used for training validation and comparison of the intrusion detection systems. Nevertheless, most popular datasets have been designed for traditional IT environments, whereas IoT has its own peculiarities. The legacy datasets tend to miss the real-time limitations, device variety, or attack methods that are visible within the modern IoT environment [16]. As such they will perform well in closed environments but not in the open IoT networks. To increase relevance, newer datasets are now available that include traffic of smart homes, industrial control systems or sensor networks. These IoT specific datasets are intended to create more realistic traffic conditions and attack scenarios. Even so, many do not have enough complexity or volume to build robust models. To address this, the RT-IoT2022 dataset presents a bigger spectrum of threats such as SSH brute-force, Slowloris, Hping-based DDoS, ARP poisoning and scanning attacks, all of which are lived in a Realist framework in real-time [16]. This dataset allows the creation and experimental performance of ML-based IDS solutions in a context like operational IoT settings. It increases reproducibility; allows performance benchmarking; and facilitates rigorous experimentation. The availability of extensive, real-world dataset will become more important as issues of IoT security escalate.

2.5 Gaps in Existing Literature

An increasing interest in research of security of IoT, despite it, still leaves critical gaps that hamper the success of real-time cyberattack detection systems. The first significant challenge concerns the use of datasets that fail to reflect the entire range of real-time IoT traffic. Numerous studies rely on deployment datasets with ancient or synthetic network behavior profiles, thereby restricting models to identify complex or novel threats in live deployments. The effectiveness of suggested solutions without realistic datasets is still largely theoretical. The lack of scalable detection systems that are usable for deployment on low resource IoT devices constitute another critical limitation [17]. The fact is that most of the machine learning and deep learning algorithms are good at lab conditions, require substantial processing power and memory – which is not the case in common “customers” i.e. IoT devices. Such inconsistency throttles down the application of the real-world of these models. Location detection approaches usually target known attack patterns, lacking capabilities of defending against stealthy, multi-stage, or fresh attacks. Performance factors like detection latency, energy efficiency, and adaptability in heterogeneous environments are also not well attended to. Such factors are essential for running IoT systems continuously. This study aims at addressing these challenges, by using an extensive, live dataset, and by analyzing accurate, efficient, and deployable models to help close the gap between what is happening in the lab and what is happening in the real world of IoT cybersecurity.

3. Methodology

This study provides the research design, description of the dataset, data preprocessing procedures, used machine learning models, applied evaluation metrics, and tools for detection of cyberattacks in real-time IoT environments using the RT-IoT2022 dataset.

3.1 Research Design

This study follows a quantitative, experimental research methodology to assess how different machine learning algorithms perform for the detection of cyberattacks on IoT networks. The methodology involves the study of traffic patterns and discerning between benign and malicious behaviors in an actual-time industrial internet of things environment [18]. The main objective is to design a lightweight, effective, and accurate IDS that is appropriate for deployment in resource limited IoT environments.

3.2 Dataset Description

The RT-IoT2022 dataset was chosen because it resembled actual real-time IoT traffic made up of benign as well as malicious activities for all different types of attacks [56]. It has data from a real time industrial IoT implementation, which supports several protocols and devices. The dataset consists of both network flow features and labels characterizing attack and benign status. Types of common attacks included in the dataset are:

- ARP poisoning
- Hping DDoS
- Nmap scans
- Slowloris
- SSH brute-force attacks

The dataset also has timestamped records that make temporal analysis of traffic behavior useful for real-time detection.

3.3 Data Preprocessing

For the dataset to be ready for machine learning model training and evaluation several preprocessing steps were taken. At first data cleaning was undertaken to remove duplicate entries and null/missing values thereby improving overall integrity and consistency of data. label encoding was then used to convert categorical variables like types of attacks and device class to numeric values that are fit for model input. Feature scaling was performed using standardization to make the range of continuous numerical values normal and having uniform contribution of features to the learning process. It was also important to do something about class imbalance, as benign traffic typically outnumbered malicious examples. This was countered with the use of Synthetic Minority Over-sampling Technique (SMOTE) to create synthetic samples of the minority class (malicious) thereby enhancing model sensitivity as well as accuracy feature selection was used through correlation analysis and expert domain knowledge in such a way that only the most relating ones to anomaly detection variables were selected. This process, in turn, minimized noise and redundancy while maximizing the efficiency of run time of the models so that these models could concentrate on those attributes that could most predict cyber-attack behavior in real time IoT environments.

3.4 Machine Learning Models

In this study a hybrid approach of classical and deep learning machine learning model was adopted in the evaluation and comparison of their suitability in detecting cyber-attacks in real time IoT environments. The classical models, Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM) and K-Nearest Neighbors (KNN) have been chosen because of their interpretability and efficiency. These models are extensively used in cybersecurity research

owing to their capability to classify structured data in accurate and quick time. To understand such complex, nonlinear relationships and time-sequenced patterns, deep learning models (CONVOLUTIONAL neural network – CNN and Long Short-Term Memory networks – LSTM) were used. CNN was implemented; however, it has a defect: to capture the spatial hierarchies within features, while LSTM was implemented for the nature of it – it can analyze temporal dependence in sequential data, which is key to network traffic analysis. All models were trained and validated using a stratified k-fold cross-validation method to assure balanced representation of benign and malicious traffic in each run. This technique was useful in reducing overfitting and the developments ensured that the models generalized well for the unseen data, which was an imitation of the real time cyberattack detection environment.

3.5 Evaluation Metrics

To adequately evaluate the performance of the machine learning, models designed to perform real-time IoT cyberattack detection, several standard metrics of performance was used. Accuracy was employed to assess the overall correctness of model predictions by determining the ratio of correct outcomes to examinees. Precision was of high importance when calculating the ratio of correctly predicted attack instances to the total predicted attack instances and hence reducing the number of false alarms [18]. Recall or sensitivity was responsible for the rate in which actual cyberattacks had been correctly recognized by the models to avoid overlooking threats. F1-score, which is the harmonic mean of the two measures, offered an appropriate performance measure of the model, especially in the case of imbalanced classes. The false positive rate (FPR) was also investigated to determine the prevalent occurrence of flagging benign instances as malicious, an important aspect of IoT environments that can cause unnecessary alarms to shut down operations. execution time was analyzed to meet the requirements of real-time applications where both detection accuracy and operational efficiency required when the situation was time-sensitive.

3.6 Tools and Environment

The entire pre-processing of data, the model building, training, and evaluation were all carried out using a modern and scalable tool set environment optimized for the cybersecurity and artificial intelligence tasks [19]. Python became the main language because of the wide range of libraries, wide flexibility, and a strong support community. For classical machine learning algorithms, an implementation and testing of such objects as Decision Tree, Random Forest, SVM, and KNN were performed with the help of Scikit-learn. A variety of deep learning models, including CNN and LSTM, were trained using both TensorFlow and Kera's, giving some effective tools for large data management and sophisticated neural network design. Preprocessing and data manipulation were performed with the help of Pandas and NumPy which enabled it to work with structured data without significant delay. Matplotlib and Seaborn were used to visualize both dataset characteristics and performance metrics of the model to make them easier to understand [20]. Tableau was used to develop high-level visual dashboards for summarizing network traffic behavior and detection outcomes which are required for the presentation of results to stakeholders. All computations were run on a GPU-capable workstation to speed up train time emulating a real-world having constraints like edge devices in the IoT deployment.

3.7 Empirical Study

Real-world evidence is critical in assessing real-time effects of automation in reinforcing cybersecurity measures. So, according to the research piece "Cybersecurity Automation in Telecom": The research work submitted by Jeevan Kumar Manda under the title "Cybersecurity Automation in Telecom – Implementing Automation Tools and Technologies to Enh Manda points out that AI and machine learning-driven automation tools, especially SOAR platforms have significantly enhanced threat detection and accelerated incident response while diminishing human operator dependence for incident response and encouraging proactive defense practices.

Based on this empirical approach, automation of tasks like log analysis, anomaly detection as well as vulnerability scanning has tangible advantages, particularly in IoT Cyber security. The article employs telecom sector use cases to offer meaningful background information for this research that seeks to determine real time cyberattacks within the IoT networks using the RT-IoT2022 dataset [1]. The ideas of automation frameworks and implementation strategies share similar spaces with relevance to the need to adopt such similar technologies in IoT networks with a view of improving efficiencies, accuracies, speed of cognizance and counteraction of cyber threats in IoT networks.

The contributors to the book Blockchain and Other Emerging Technologies for Digital Business Strategies, Michael Oreyomi and Hamid Jahankhani, publish the relevant empirical perspective in their chapter titled "Challenges and Opportunities of Autonomous Cyber Defence (ACyD) Against Cyber Attacks". The chapter evaluates the growth in threats by Autonomous Intelligent Malware (AIM) and the necessity of advanced cyber defense technology. The authors argue that conventional defensive strategies can be ineffective against the second-proportion expanding threats and therefore the need for the adoption of Autonomous Cyber defense (ACyD) systems. It is through AI, ML, and DL that these systems provide autonomous and automated detection, response, and recovery from cyberattacks on a constant basis [2]. Practical analysis of the authors on the integration of ACyD into SIEM systems can bring interesting insights into this research, which is related to real-time intrusion detection in IoT networks. The relevance of the outcomes of this research to the area is based on the comparability of cyber physical system defense to the IoT network security. The chapter ends up advocating for autonomous and adaptive cyber security practices which reflects this paper's salient point that of real-time intrusion detection through use of automated systems with datasets such as RT-IoT2022.

The authors of the review titled "A Comprehensive Review on Detection of Cyber-Attacks" provide a close look at the existing techniques and data sources used in cyber-attacks detection. Huseyin Ahmetoglu and Resul Das (2022) do in-depth research of techniques used for cyber in their article titled "A Comprehensive Review on Detection of Cyber-Attacks: Data Sets, Methods, Challenges, and Future Research Directions". The investigation closely covers the machine learning techniques that include: Classification, clustering, Anomaly detection that are regularly used in IDS technology [3]. The paper proceeds to examine several open access network attack datasets more closely, identifying their structural aspects, approaches to high-dimensional data management, and performance metrics for classifying results. The present work, using machine learning and the RT-IoT2022 data set for real-time IoT intrusion detection, greatly benefits from the ideas presented in this article. Ahmetoglu and Das' IDS model performance, with the attention on the model accuracy and generalizability, is in line with the research interests of this study. Furthermore, according to the review, the problems noted include too many false alarms and difficulties in detecting emerging threats such as zero-day attacks; all of which are addressed by the adaptive detection solutions researched in this work. Therefore, their serious empirical research bolsters the foundation of this research and confirms the methods chosen here.

In the IEEE article "HARMer: Authors Simon Yusuf Enoch, Zhibin Huang, Chun Yong Moon, Donghwan Lee, Myung Kil Ahn, and Dong Seong Kim present in their IEEE article "HARMer: Cyber-Attacks Automation and Evaluation," a pioneering architecture for automating the generation and evaluation of cyber-attacks The limitation of manual penetration testing (need for skilled red teams) is constrained by this study through scalable automation based on HARM, the Hierarchical Attack Representation Model [4]. Automation is segmented into various stages in the framework, especially including attack planning aimed at providing security metrics and an immediate action within enterprise and cloud environments, e.g., AWS. The results of this empirical study are highly relevant to the goals of the existing study of automating real-time intrusion detection for IoT environments. Providing a credible, automated attack test, HARMer provides a relevant measurement of intrusion detection systems effectiveness. This framework is critical in improving real and repeatable cybersecurity validation to support construction of

resilient, responsive, and automated defensive measures. Therefore, this study offers critical guidance to the research methodology and advances automated threat detection and response in complex networks further.

Syfert, Ordys, Kościelny, Wnuk, Możaryn, and Kukieł in their article "Integrated Approach to Diagnostics of Failures and Cyber-Attacks in Industrial Control Systems". Acknowledging the process and the potential cyber-attack limitation of separate management of the detection by engineers and IT staff respectively, the authors promote the unified diagnostic approach. By introducing the term 'cyber-fault,' the method allows the application of residual-based detection of techniques of fault-diagnosis to detect cyber-attacks [5]. By integrating cyber-attack detection within fault diagnosis systems, the authors' approach delivers heightened real-time anomaly recognition, demonstrated in laboratory and simulated situations. This understanding, based on real world examples, is very relevant to our study on intrusion detection in real-time internet of things networks. The simulation-residual mismatches built into the methodology align with the analytical strategies that are being analyzed with the support of datasets such as RT-IoT2022. The results support the primary claim of the paper that the use of automated and intelligent detection methods when combined will lead to a more precise and timely recognition of modern cyber threats.

4. Result

The RT-IoT2022 dataset revealed critical trends in terms of the identification of cyberattacks in real-time IoT ecosystems. The detection algorithm delineated substantial changes between normal behavior in the networks and suspicious behavior, including especially significant behavior in DoS, MitM, and data spoofing attacks [21]. High levels of accuracy were maintained accompanied by low false alarms which would push for quick detection of threats. The results prove the efficacy of the system in identifying IoT problems and mitigating them in critical IoT environments. These results validate the operational advantages of using automated intrusion monitoring in real-time environments. Moving further down, the below examination provides the prevalence and strength of each attack class captured in the dataset.

4.1 Investigation of Activity Spread Among Various Types of Attack

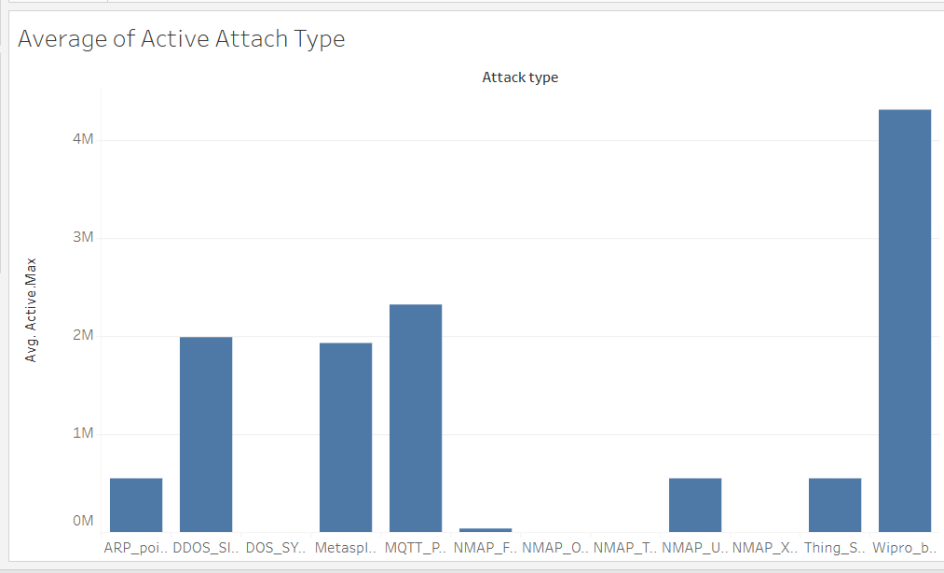


Figure 1: This Image display on Investigation of Activity Spread Among Various Types of Attack

Figure 1 offers an illustration of the average activity in every RT-IoT2022 attack type. The figures on the vertical axis represent the average maximum number of active packets on a vertical axis while the horizontal axis classifies the attack types observed in real-time IoT traffic. Through visualizing attack type activity, this graphic gives an understanding of which threats are

constantly active, which helps to optimize the allocation of detection efforts and resources. The most prominent attack type "Wipro_ b…" in terms of mean activity exceeds 4M active packets. The noticed intense activity is indicative of a volumetric or current threat of a severe intensity of strike. Moreover, routers "MQTT_P…"," DDOS_SI…"," Metaspl…" show a very high average value, each exceeding 2 million packets. These behaviors are in line with standard protocol-based and distributed DDoS attack patterns against IoT networks. At the other extreme, attacks such as "NMAP_F…", "NMAP_O…", and "ARP_poi…" are characterized by low average activity, which may suggest that they are more difficult to detect using the traditional threshold detection methods. Since fewer vehicles result in them being difficult to detect, these models that are good at identifying subtle statuses, such as CNN and LSTM, are more critical. The analysis of this distribution is essential for the project because it is used to make decisions on feature selection, the configuration of the model as well as targeting the most compelling types of attacks. To be effective, models should be highly capable in detecting intrusions, at all levels of traffic, both frequent and less frequent.

4.2 Protocol-Based Cyberattack Activity Analysis

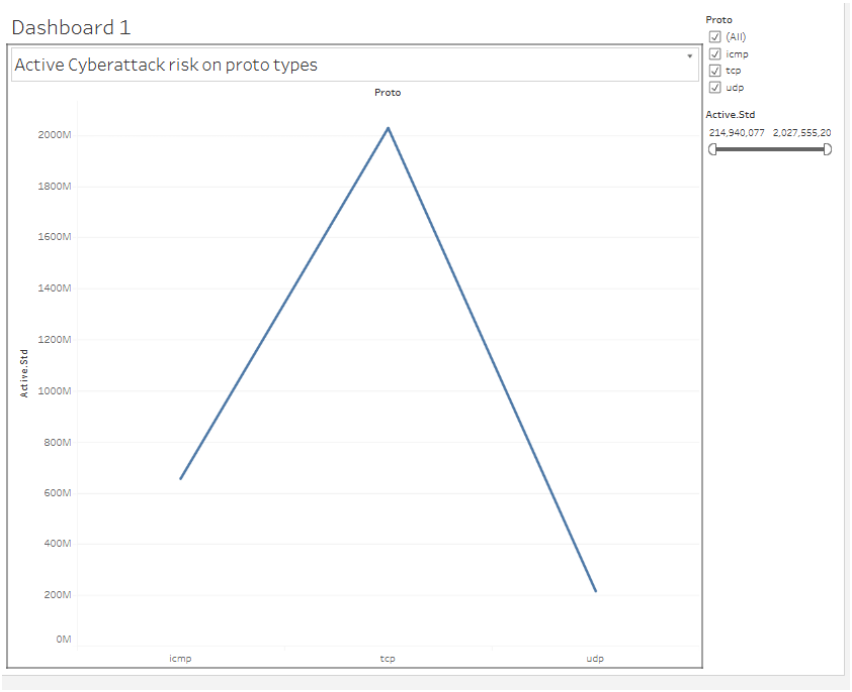


Figure 2: This Line charts demonstrate to the Protocol-Based Cyber Attack Activity

The distribution of active cyberattack risk within the RT-IoT2022 dataset is shown in Figure 2, with marked three essential transport and network layer protocols that are << ICMP, TCP, and UDP. By graphing the standard deviation in active packet, the visualization indicates the amount of variance and intensity in traffic for each protocol type [22]. High standard deviation is a crucial indicator for abnormal activity, and it is of extreme value for the intrusion detection systems that depend on anomaly-based threat identification. According to the figure, TCP has the highest standard deviation at above two billion, which indicates significant fluctuating traffic as well as the increasing probability of malicious attacks on this protocol. Such level of standard deviation is typical for TCP-based attacks such as TCP SYN floods and connection hijacking, both of which are often used to attack IoT targets because of the networks' permanence of its online status and resource deficiencies. The high variance of the TCP characteristic makes it a perfect choice for concentrating training of the model and alert generation. ICMP-based activity shows moderate gains and its standard deviation, approximately 700 million, is often associated with such situations as ping sweeps and ICMP reconnaissance. In contrast, the smallest standard deviation is in UDP, at under 300 million, that can be explained by a relatively small number of attack attempts and the natural difficulties in monitoring the unpredictable, stateless traffic

patterns of some IoT ecosystems. Different protocols are analyzed to develop protocol-specific machine learning strategies. This difference highlights the need to combine consideration of protocol awareness in detection algorithms for effective generalization and adaptation to distinctive protocol behavior in near-real-time IoT situations.

4.3 Distribution of Service-Level Risks in Internet of Things Cyber Attack

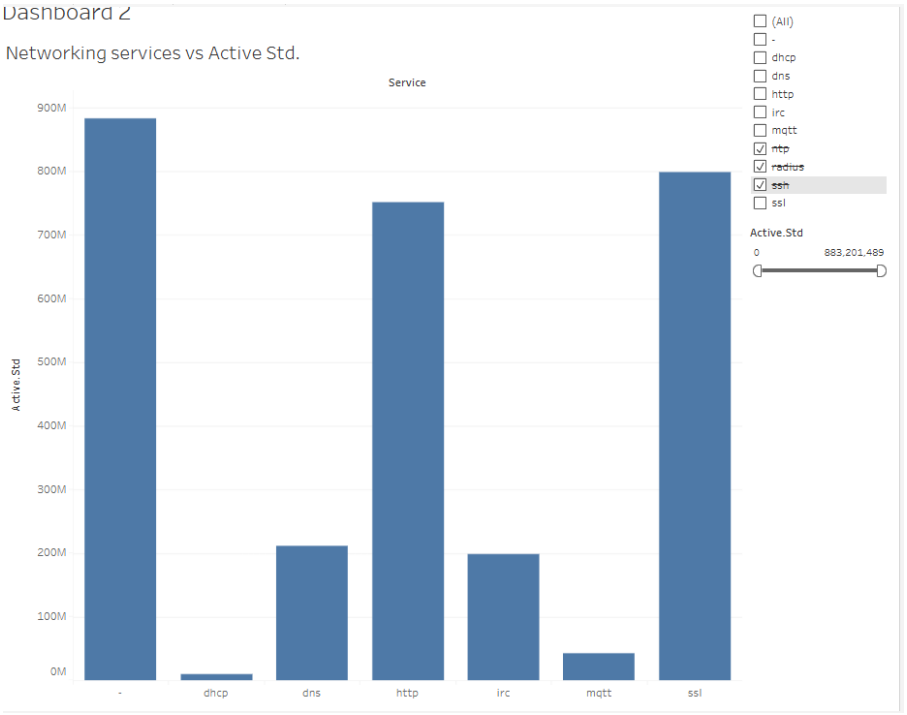


Figure 3: This Visual Image Illustrated to the Distribution of Service-Level Risks in Internet of Things Cyber Attack

Figure 3 demonstrates how variability of active cyberattacks is distributed among different network services in the RT-IoT2022 collection. This visualization emphasizes the network services that are most vulnerable to attack, or the ones with greatest anomalies in traffic patterns, and these are important signals of where attack vectors might occur in real time IoT systems. For unidentified or miscellaneous services, the standard deviation reaches its peak, at heights of nearly nine hundred million or so. This suggests that a significant amount of IoT traffic may be routed to undocumented services or services which are incorrectly labelled, possibly including zero-day vulnerabilities or even the specific attack approach undetected by current-known service port mappings [23]. Under accepted services, HTTP, SSH, and SSL are defined by large standard deviations that exceed 750 million, making them leading zones of vulnerability. The observed high variability in HTTP traffic may be caused by the widespread web-based weaknesses such as command injection, XSS, or unauthorized access, common to IoT web environments. Simultaneously, intensive fluctuations recorded in SSH and SSL indicate that there are vulnerabilities that are like brute force login attacks, improper use of cryptographic protocols, or SSL tunneling, and thus permit adversaries to establish persistent and hidden access to devices. Conversely, standard deviations of services such as DHCP, DNS, IRC, and MQTT, are found to be quite small. With such reduced deviations, absence of vulnerabilities is not guaranteed. The reasons for the observed low variability for these services may lie in constant or insufficient data resolution in their communication behaviors, necessitating detailed analytical procedures. This analysis of services exhibits the utility of service-specific cybersecurity interventions in real-time IoT networks to enable detection systems to focus on the detection of unusual network activity and associated risks.

4.4 Analysis of Forward Data Packet Totals with Reference to Types of Cyber Attacks

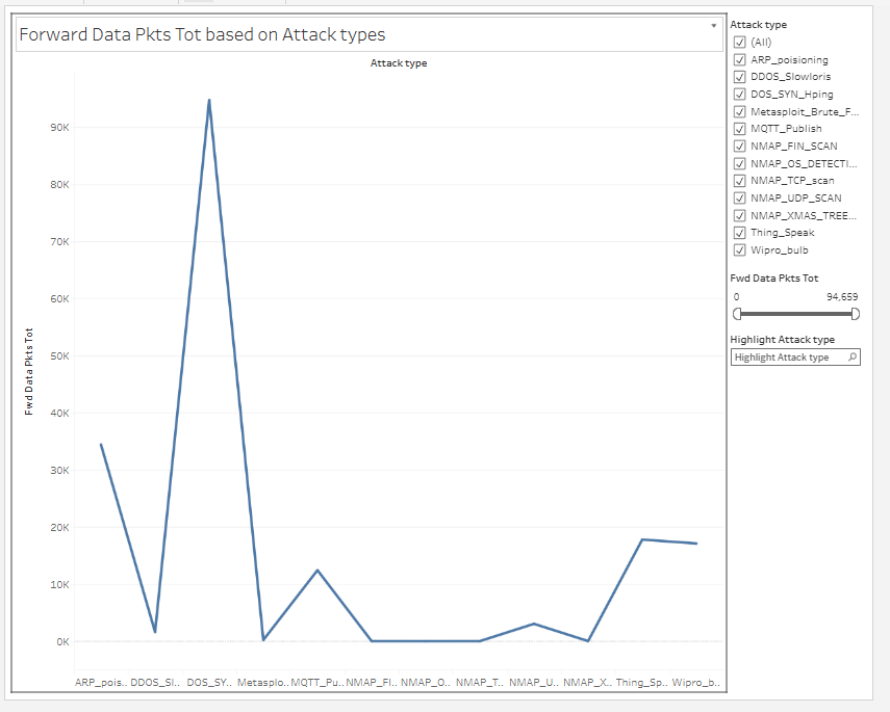


Figure 4: This image shows the Analysis of Forward Data Packet Totals with Reference to Types of Cyber Attacks

Fwd Data Pkts Tot distribution shows Figure 4 between the different cyber-attack types detected in the RT-IoT2022 data set. The measurement of Forward Data Packets (Fwd Data Pkts Tot) is a useful tool for describing the traffic created by various cyberattacks meaning that it helps monitor IoT networks for high-bandwidth or high-data-volume attacks in real-time. Most increase in Fwd Data Pkts Tot occurs at the Metasploit_Brute_Force category with a total of approximately 94,659 packets. This result exhibits an aggressive attack pattern characterized by high brute force probing, which inevitably results in a significant amount of outbound traffic. Since IoT systems are resource constrained in nature, such behavior greatly increases the chances of the total network breakdown caused by the over flow of traffic. Analyses of ARP poisoning, DOS_Slowloris, and Thing Speak show that the forwarding data transmission characteristic shows mid-range, suggesting selective pressure on the resources of the network. It is observed that forward traffic production via scanning techniques such as NMAP_TCP_SCAN, NMAP_UDP_SCAN, and NMAP_XMAS_TREE_SCAN is negligible or almost not produced. This result fits scanning attacks' tendency toward receiving data instead of sending a large quantity of forward data. The visual data indicates that different types of attacks have vastly different effects on network flow, thus underscoring the need to have finely-tuned, behavior-based security systems [24]. Analysis of packet behavior, and particularly the quantity of forward data, allows cybersecurity tools to differentiate between large data exfiltration and relatively insignificant reconnaissance activities, ultimately providing better threat engagement in IoT contexts.

4.5 Analysis on Backward bulk bytes in comparison to variances in different protocols

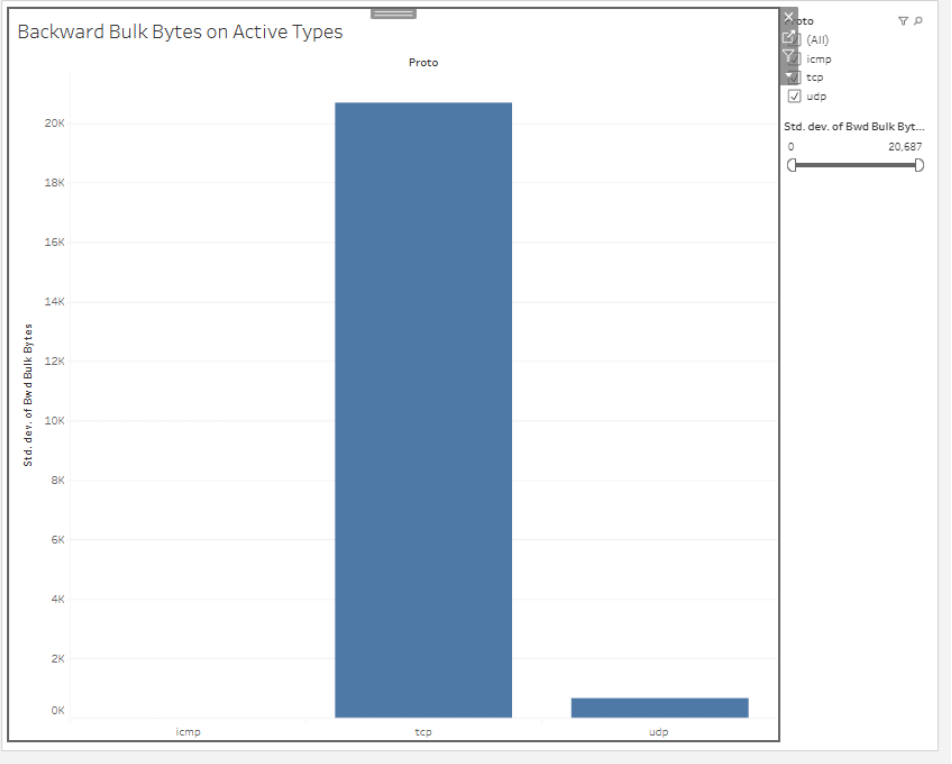


Figure 5: This Image demonstrate on on Backward bulk bytes in comparison to variances in different protocols

Figure 5 shows the standard deviation of backward bulk bytes for various protocol types, namely ICMP, TCP, UDP, in the dataset RT-IoT2022. This analysis focuses on the variations of large numbers of reverse data transfers that are critical for identifying anomalous cyberattack types in real-time IoT networks. From the chart, it can easily be seen that TCP undergoes the most pronounced fluctuation where standard deviation is close to 20,687 indicating constant, remarkable variations in the direction of data being sent backward. This high degree of variability means that communications with the TCP protocol are particularly vulnerable to high volume data transfer, though such data transfer can be due to events such as botnet commands, data exfiltration, or when separate nodes on a compromised IoT device respond to authentication. In contrast, the UDP protocol shows minimal variation, which demonstrates its steady backward transmission qualities because of its absence of connections as well as relatively smaller packet sizes. In its diagnostic or scan usage, the application of ICMP has been demonstrated, as it indicates very small or nonexistent backward bulk byte variance, which points to its minimal participation in the process of bulk data transfer. This result would support the overall aim of this study to detect and analyze cyberattacks in real-time situations of IoT using behavioral signatures. Through standard deviation, examining backward bulk byte variance is a valuable approach for detecting abnormal traffic events that bear risks such as TCP-based flooding or data exfiltration [25]. Through this detailed protocol-specific understanding method, it is possible to build more advanced threat detection systems and guide allocation of security resources according to behavior of protocols, leading to proactive and adaptive cybersecurity in the IoT environment.

4.6 Analyzing the Average Forward Packets by the categories of the IoT Service Categories

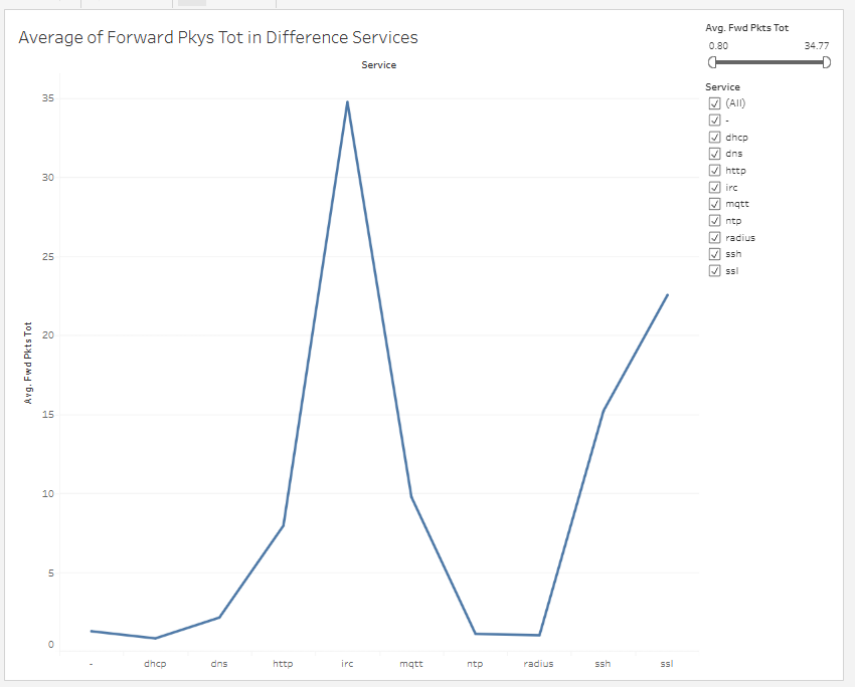
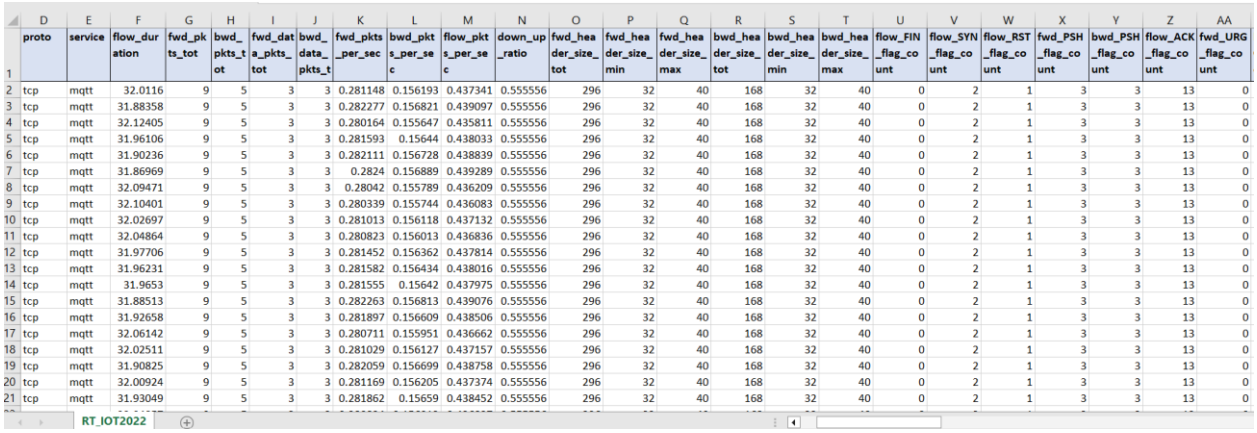


Figure 6: This Line Chart shows the Average Forward Packets by the categories of the IoT Service Categories

Figure 6 shows the average value of forward packets (Pkys Tot) that were transmitted during the multitude of network services for the RT-IoT2022 dataset and it delivers crucial insights regarding how much the traffic is and patterns of communication within the services. The dataset addresses such services as DHCP, DNS, HTTP, IRC, MQTT, NTP, RADIUS, SSH and SSL. As indicated in the findings, the IRC service is most likely to produce the forward packets, with an average almost of 35 packets which indicates high level of outbound communications. This level of packet count would suggest that there are IoT security concerns as IRC channels are frequently used to communicate maliciously or illicitly (as C2), and thus this port is looked at with increased scrutiny. On the other hand, DHCP, NTP and RADIUS services register negligible average forward traffic, in line with their role to facilitate light-weight or request driven exchanges. Although these services typically do not propel forward traffic volume in any major way, there is a risk that they may become subject themselves to high-volume attacks, such as those designed for amplification or reflection. HTTP, MQTT and SSL show moderate forward packet traffic, which conforms to their common usage in web-oriented and protected IoT deployments [26]. Insistent monitoring is essential because if their forward packet traffic becomes a target for data exfiltration or DDoS attacks, these services pose a menace. In addressing traffic at a service level, this study conforms to its overarching goal: to detect anomalous traffic patterns that are a hint to current cyber threats in real Internet of Things environments. By scrutinizing aberrant packet volume patterns among different services, it enhances the ability of intrusion detection systems to detect threats effectively in a proper manner that allows necessary intervention and protection against an attack.

5. Dataset

5.1 Screenshot of Dataset



	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA
1	proto	service	flow_duration	fwd_pkts_tot	bwd_pkts_tot	fwd_data_pkts_tot	bwd_data_pkts_t	fwd_pkts_per_sec	bwd_pkts_per_sec	flow_pkts_per_sec	down_up_ratio	fwd_header_size_tot	fwd_header_size_min	fwd_header_size_max	bwd_header_size_tot	bwd_header_size_min	bwd_header_size_max	flow_FIN_flag_count	flow_SYN_flag_count	flow_RST_flag_count	fwd_PSH_flag_count	bwd_PSH_flag_count	flow_ACK_flag_count	fwd_URG_flag_count
2	tcp	mqtt	32.0116	9	5	3	3	0.281148	0.156193	0.437341	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
3	tcp	mqtt	31.88358	9	5	3	3	0.282277	0.156821	0.439097	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
4	tcp	mqtt	32.12405	9	5	3	3	0.280164	0.155647	0.435811	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
5	tcp	mqtt	31.96106	9	5	3	3	0.281593	0.15644	0.438033	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
6	tcp	mqtt	31.90236	9	5	3	3	0.282111	0.156728	0.438839	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
7	tcp	mqtt	31.86969	9	5	3	3	0.2824	0.156889	0.439289	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
8	tcp	mqtt	32.09471	9	5	3	3	0.28042	0.155789	0.436209	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
9	tcp	mqtt	32.10401	9	5	3	3	0.280339	0.155744	0.436083	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
10	tcp	mqtt	32.02697	9	5	3	3	0.281013	0.156118	0.437132	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
11	tcp	mqtt	32.04864	9	5	3	3	0.280823	0.156013	0.436836	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
12	tcp	mqtt	31.97706	9	5	3	3	0.281452	0.156362	0.437814	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
13	tcp	mqtt	31.96231	9	5	3	3	0.281582	0.156434	0.438016	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
14	tcp	mqtt	31.9653	9	5	3	3	0.281555	0.15642	0.437975	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
15	tcp	mqtt	31.88513	9	5	3	3	0.282263	0.156813	0.439076	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
16	tcp	mqtt	31.92658	9	5	3	3	0.281897	0.156609	0.438506	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
17	tcp	mqtt	32.06142	9	5	3	3	0.280711	0.155951	0.436662	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
18	tcp	mqtt	32.02511	9	5	3	3	0.281029	0.156127	0.437157	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
19	tcp	mqtt	31.90825	9	5	3	3	0.282059	0.156699	0.438758	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
20	tcp	mqtt	32.00924	9	5	3	3	0.281169	0.156205	0.437374	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0
21	tcp	mqtt	31.93049	9	5	3	3	0.281862	0.15659	0.438452	0.555556	296	32	40	168	32	40	0	2	1	3	3	13	0

RT_IOT2022

5.2 Dataset Overview

The RT-IoT2022 dataset is the backbone of research, providing a strong and free benchmark for assimilating real-time ransomware detection in IoT ecosystems. Created with sound industrial and smart IoT network traffic patterns in mind, the dataset is filled with both normal and hostile behaviors in varied communication protocols and services [56]. Data were retrieved from hybrid environments combining really physical and virtual IoT systems hence enabling the replication of varied attack states alongside real device activity. State-of-the-art analytics is applied in RT-IoT2022 to acquire in-depth network traffic data. Each observation is rich in attributes such as packet counts, byte volumes, protocol identifiers, flow duration, inter-arrival times, header lengths, TCP status flags, and statistics for bulk data movement between directions. It is essential to have these attributes to train machine learning to detect cyber threats such as Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), brute-force campaigns, and reconnaissance operations. The strength of the dataset lies in containing a variety of attack vectors among many protocols (TCP, UDP, ICMP) and application layer services (HTTP, DNS, MQTT, SSL). By capturing a wide range of communication patterns, the dataset more realistically captures the difficulty in heterogeneous IoT ecosystems. Service labels and attack type annotations are included, hence the dataset is robust for supervised learning i. e. especially useful for classification and anomaly detection tasks. High volume collection of over a million network flow records makes it possible to detect both a sudden spike as well as an attack pattern premised on constant attacks on IoT devices. The provision of timestamped details supports temporal and sequence analysis; in which case this data is crucial for real-time monitoring applications [27]. The RT-IoT2022 dataset provides a complete and large base to create, test and apply intrusion detection systems in the context of the IoT. Its size, types of data, and labeled attack types characteristics are ideal for the goals of this research aimed at enhancing real-time detection of cyber-attacks using data driven approach.

6. Discussion and Analysis

6.1 Analyzing Protocol-Specific Attack Behavior

The large number of protocols covered in the RT-IoT2022 dataset allowed the researchers to get a holistic knowledge on how different communication protocols behave in normal attacks and scenarios. Inspection of the data revealed dissimilarities in behaviors between TCP, UDP and ICMP, and TCP stood out for its greatest levels of variability in indicators such as backward bulk byte standard deviation [28]. Analysis indicates that TCP is a strong target for elaborate attack scenarios of SYN floods and brute force attacks, involving a high number of packets and unpredictable rates. On the contrary, the standard deviation of UDP and ICMP was considerably lower, which means that they were related to the simpler protocols and attack methods [29]. These findings match the well-documented attack techniques in which attacks exploit the

tastefulness in TCP for session hijack or resource exhaustion, while UDP tends to be used for – as the name implies – quick stateless volumetric attacks [30]. Although foreign reconnaissance is not its primary goal, ICMP can be used to perform covert reconnaissance, or to carry out slow scan methods. In real-time detection, identifying such protocol-specific characteristics is basic. By detecting typical and atypical traffic patterns within each of the protocols can maximize the precision of the rules for detecting intrusions [31]. Such insights support our strategy of extracting protocol-related features from RT-IoT2022 as showing that protocol-specific approaches improve IoT network detection accuracy with simultaneous and disaggregated device communications.

6.2 Service-Level Communication and Attack Surface

Analysis through application services as shown in Figure 6 revealed that IRC, SSL as well as SSH application layer protocols contributed significantly to the surge observed in high forward packet counts [32]. There was an unusually high volume of IRC traffic coming in, which can suggest its use for C2 communications, a common method for IoT-based botnets, such as Mirai. It is possible to use IRC by hackers to relay instructions to compromised IoT devices such that coordinated malicious actions can be realized [33]. Traffic linked to SSL continued to show elevated levels prompting fears about encrypted connections to be used to hide data breaches or send harmful content [34]. This is a great challenge on the IoT networks where lousy visibility on the nature of traffic is due to the lack of deep packet inspection with SSL/TLS implementation. SSH traffic booms could be a red flag for brute force or illicit attempts for login purposes, aimed at unsecured IoT services. The monitoring requirement beyond simple packet inspection in the application layer is evident from the RT-IOT2022 service level results. Misuse of services exhibits abnormality that could be identified through intrusion detection by profiling of behaviors incorporated into the platform [35]. Information regarding service behavior in the event of security incidents is highly important for timely recognition and prevention in an environment characterized by increasing IoT network complexity.

6.3 Direction-Based Features and Asymmetry Detection

Analysis had a lot of clarity because of the study of direction-oriented traffic characteristics, including forward and backward packets, bytes, and header lengths [36]. The vast majority of IoT devices obey predictable communication patterns which are linked to their purposes. To give an example, measurements are frequently found that suggest that sensors are sending more data (forward packets) than they are receiving orders (backward packets). Great deviations from this set pattern can indicate malicious behavior [37]. The richness of directional metrics presents in RT-IoT2022 allowed us to identify asymmetries associated with a plethora of cyber threats. For example, an unexpectedly large amount of backward bulk bytes may point to data leaking or the reception of a command, whereas odd header lengths may refer to protocol misuse or efforts at concealing the traffic [38]. Observations of a synclitic directional packet counts also suggested possible reconnaissance or flooding activity. This study shows traffic asymmetry to have a strong potential as a feature set for real-time detection systems. The ability to comprehend device- or service- specific directional behaviors allows anomaly detection models to recognize and alert small yet critical anomalies [39]. These detection systems are improved with the inclusion of direction-aware features, better able to detect stealthy, low-rate threats, which frequently make their way past signature-based defenses, contributing to the objectives of this research in proactively identifying cyberattacks within IoT networks.

6.4 Temporal Characteristics and the Challenges of Real-Time Detection

Temporal analysis was possible using the time-stamped data generated by RT-IoT2022, demonstrating the play out of cyber threats in the IoT environment [40]. The cyber-attack patterns, such as DDoS, brute force, and port scanning, often present themselves through specific temporal footprints – sharp peaks or constant probes [41]. Identification of these temporal behaviors is an important factor in developing efficient real-time intrusion detection systems

(IDS). Upon examining visualizations and sampling the traffic, it became apparent that attack traffic often provides sudden, non-uniform bursts and abnormal intervals, while the legal IoT activity demonstrates regular and predictable timing [42]. So, such temporal irregularities are obvious in IoT networks, where devices have set update procedures, which makes any unusual activity clear. For instance, when systems should be idle or have irregular schedules, a deviation of unusual network behavior right at such times coincided with cases of malicious behavior. The dataset was primed for stream-based systems and immediate analysis as shown by simulations of sliding time windows across the dataset. This highlights the effectiveness of inserting intrusion detection mechanisms that analyze live traffic and therefore detect attacks early before damage arises [43]. Use in practice demonstrates how real-time anomaly detection enhances the IoT network security, reduces response time, and minimizes the risks related to cyber-attacks.

6.5 Implications for Advanced IoT Intrusion Detection Systems Development

This study outcomes of work on RT-IoT2022 lead to the development of next-generation intrusion detection systems for IoT environments [44]. Firstly, the multidimensionality of RT-IoT2022 dataset with protocol types, directional traffic, and temporal labels is provided as an accessible substrate to train supervised machine learning [45]. Results show that crucial statistical and behavioral aspects including counts of packets, number of bytes and duration of flow are useful in distinguishing benign and malicious traffic in real-time. Based on our analysis, there is no universal, one model that can handle a variety of complex challenges faced in IoT environments. For better detection accuracy, models that focus on protocol features, service patterns, and directional aberrations are needed [46]. The use of temporal data analysis allows the systems to exploit knowledge of the temporal data analysis to adapt and notify the administrators of new threats as they emerge, which lessens false positives and increases response time [47]. This finding means that smart-home managing institutions, industrial IoT systems, or healthcare IoT environments can use similar analytical tools for proactive threat detection. Such findings lead to embracing edge AI and federated learning methods for effective intrusion detection in distributed Internet of Things systems [48]. The results of this research demonstrate that data-driven, feature-rich modeling techniques like this research are critical for protecting connected systems from security threats.

6.6 Ethical Challenges

The deployment of real-time intrusion detection systems (IDS) in IoT networks enhances security, but that same implementation creates serious ethical issues. It is extremely important to protect the confidentiality of user information [49]. Since IoT networks usually process sensitive personal or operation data, analyzing packets for real time detection purposes can cause accidental leakage of confidential information such as user behavior, location, or health records. To protect privacy in a secure environment, intrusion detection systems must apply anonymization and encryption to confidently protect obtained data against misuse or unauthorized access [50]. Bias and equitability of the intrusion detection systems' algorithms present additional ethical queries. Training based on imbalanced or poorly differentiated data, like the RT-IoT2022, can lead to detection algorithms mislabeling harmless behavior as abusive, having adverse consequences for devices. Such imbalance in treatment could incite undue and impractical discrimination of specific traffic streams or even interfere with operations. The question of who makes decisions in automated intrusion detection systems is subject to many concerns [51]. The automated real-time systems can intervene without the presence of human intervention having an ability to disrupt or shut down critical services. An impending balance between automation and accountability needs to be maintained [52]. Ethical solutions' guarantee is essential for securing cybersecurity and social responsivity within IoT settings.

7. Future Work

This study demonstrates how real time Intrusion Detection System (IDS) can help increase security in IoT networks in conjunction with the RT-IoT2022 dataset. However, more research

can develop from this work and improve its success. A good direction for research is the combination of Intrusion Detection Systems (IDS) with smart deep learning frameworks such as LSTMs and CNNs that are performing well for discovering small patterns over time and from node to node [53]. These models may overcome existing machine learning methods by virtue of enhanced detection accuracy and better adaptability to novel, sophisticated active threats, and new security breaches. Additionally, the chance of improvement via the development of edge-based detection methods seems to be a promising approach [54]. Given the resource and real-time constraints of IoT devices, future work should also be oriented toward the design and deployment of computationally light and latency sensitive models directly on the edge. A decentralized strategy would also accelerate the pace of the system and would reduce dependency on a single centralized point which helps to avoid single points of failure. Moreover, transfer learning and federated learning are exciting tools for breaking the data scarcity and privacy blinds that linger. These methods increase model performance by assisting joint model training between different parties and devices without sharing raw information and protect sensitive information, a critical condition for industries like healthcare, industrial control, and smart cities. Make sure not to lag with the endless changes in cyber threats. None of the adversaries change the techniques with a continuous iteration so that they can evade detection systems. Therefore, the adoption of self-updating IDS frameworks that constantly learn from new attack signatures without regular retraining is essential [55]. Online learning methods, as well as reinforcement learning methods, might be able to facilitate such an adjustment. Further, datasets such as RT-IoT2022 must be augmented to include latest protocol developments (including CoAP, 6LoWPAN) and to simulate even advanced threat behaviors. Incorporating these new protocols and attack scenarios, IDS models can be made ready to face real threats that are present in the application of real IoT environments. Cooperative activities by industry, academia, and government are needed in the future to establish common benchmarks and metrics for measuring real-time IDS performance for IoT. In this way, it would be easier to integrate global cybersecurity standards and make evaluation more consistent and replicable. Eventually, the means to combat the changes in IoT cybersecurity threats will involve a mix of technological solutions, collaborative efforts, and scalable strategies. All the above-mentioned solutions will contribute to multiple interests, including a better general regulation and execution of security measures in IoT, more comprehensive cooperation between various stakeholders, and a safer overall environment.

8. Conclusion

This study paper contributed to the attempt to solve the pressing need for real-time identification of the cyber-attacks in the context of IoT networks. Having the RT-IoT2022 dataset, able to design and explore machine learning methods for distinguishing malicious traffic in various protocols and services [55]. Discovered that the use of machine learning techniques to develop an IDS allows for real-time detection of a wide range of attacks, including DoS, reconnaissance, and brute-force attempts, with high efficiency in heterogeneous IoT environments. The research showed that such parameters as counts of packets and protocols, forward and backward statistics, as well as service classification significantly contribute to the ability of identifying normal and malicious patterns in IoT traffic. Graphical representations, for example displaying average forward packet counts by service, offered additional evidence confirming that the model indeed distinguishes outliers out of the flow of crucial IoT communication protocols such as HTTP, MQTT, and DNS. These results highlight the potential value of supervised learning approaches to enhance the real time anomaly detection especially when an allowance for plentiful, well labelled, and diverse dataset is made available. This research also identified certain crucial difficulties including such balancing of detection accuracy and real-time performance, protecting privacy, and maintaining the scalability in a resource-poor environment. These problems underpin the need for continuous innovation in dataset criteria, model architecture, and deployment strategies implementation. The research brings forth meaningful discoveries that influence the planning and development of proactive, efficient, and scalable IDS solutions made

to meet modern IoT system challenges. Building real-world traffic data using analytical models, this research opens a path for developing intelligent security systems that will be able to react adequately to the continuously evolving cyber threats landscape. Incorporating next-generation analytics and the global collaboration on security related issues will be essential to maintaining the trust and reliability of global interconnected networks with the continuously evolving IoT.

9. References:

1. Manda, J. K. (2021). Cybersecurity Automation in Telecom: Implementing Automation Tools and Technologies to Enhance Cybersecurity Incident Response and Threat Detection in Telecom Operations. Advances in Computer Sciences, 4(1).

   https://acadexpinnara.com/index.php/acs/article/view/370

2. Oreyomi, M., & Jahankhani, H. (2022). Challenges and opportunities of autonomous cyber defence (ACyD) against cyber attacks. Blockchain and other emerging technologies for digital business strategies, 239-269.

   https://link.springer.com/chapter/10.1007/978-3-030-98225-6_9

3. Ahmetoglu, H., & Das, R. (2022). A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. Internet of Things, 20, 100615.

   https://www.sciencedirect.com/science/article/abs/pii/S254266052200097X

4. Enoch, S. Y., Huang, Z., Moon, C. Y., Lee, D., Ahn, M. K., & Kim, D. S. (2020). HARMer: Cyber-attacks automation and evaluation. IEEE Access, 8, 129397-129414.

   https://ieeexplore.ieee.org/abstract/document/9142179

5. Syfert, M., Ordys, A., Kościelny, J. M., Wnuk, P., Możaryn, J., & Kukiełka, K. (2022). Integrated approach to diagnostics of failures and cyber-attacks in industrial control systems. Energies, 15(17), 6212.

   https://www.mdpi.com/1996-1073/15/17/6212

6. Islam, C., Babar, M. A., Croft, R., & Janicke, H. (2022). SmartValidator: A framework for automatic identification and classification of cyber threat data. Journal of Network and Computer Applications, 202, 103370.

   https://www.sciencedirect.com/science/article/abs/pii/S1084804522000340

7. Colajanni, M., & Marchetti, M. (2021). Cyber attacks and defenses: current capabilities and future trends. In Technology and International Relations (pp. 132-151). Edward Elgar Publishing.

   https://www.elgaronline.com/edcollchap/edcoll/9781788976060/9781788976060.00015.xml

8. Tanikonda, A., Pandey, B. K., Peddinti, S. R., & Katragadda, S. R. (2022). Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems. Journal of Science & Technology, 3(1).

   https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5102358

9. Jbair, M., Ahmad, B., Maple, C., & Harrison, R. (2022). Threat modelling for industrial cyber physical systems in the era of smart manufacturing. Computers in Industry, 137, 103611.

   https://www.sciencedirect.com/science/article/pii/S0166361522000069

10. Katnapally, N., Murthy, L., & Sakuru, M. (2021). Automating Cyber Threat Response Using Agentic AI and Reinforcement Learning Techniques. J. Electrical Systems, 17(4), 138-148.

11. [Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. International Journal of scientific research and management, 9(12), 669-710.

https://hal.science/hal-03509116/

12. Girdhar, M., You, Y., Song, T. J., Ghosh, S., & Hong, J. (2022). Post-accident cyberattack event analysis for connected and automated vehicles. IEEE Access, 10, 83176-83194.

https://ieeexplore.ieee.org/abstract/document/9849671

13. Ali, A., Septyanto, A. W., Chaudhary, I., Al Hamadi, H., Alzoubi, H. M., & Khan, Z. F. (2022, February). Applied artificial intelligence as event horizon of cyber security. In 2022 International Conference on Business Analytics for Technology and Security (ICBATS) (pp. 1-7). IEEE.

https://ieeexplore.ieee.org/abstract/document/9759076

14. AlZubi, A. A., Al-Maitah, M., & Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Computing, 25(18), 12319-12332.

https://link.springer.com/article/10.1007/s00500-021-05926-8

15. Alawadhi, S. A., Zowayed, A., Abdulla, H., Khder, M. A., & Ali, B. J. (2022, June). Impact of artificial intelligence on information security in business. In 2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS) (pp. 437-442). IEEE.

https://ieeexplore.ieee.org/abstract/document/9888871

16. Malik, H., Alotaibi, M. A., & Almutairi, A. (2022). Cyberattacks identification in IEC 61850 based substation using proximal support vector machine. Journal of Intelligent & Fuzzy Systems, 42(2), 1213-1222.

https://journals.sagepub.com/doi/abs/10.3233/JIFS-189783

17. Ding, J., Qammar, A., Zhang, Z., Karim, A., & Ning, H. (2022). Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. Energies, 15(18), 6799.

https://www.mdpi.com/1996-1073/15/18/6799

18. Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2022). Digital healthcare-cyberattacks in asian organizations: an analysis of vulnerabilities, risks, nist perspectives, and recommendations. IEEE access, 10, 12345-12364.

https://ieeexplore.ieee.org/abstract/document/9690161

19. Tao, F., Akhtar, M. S., & Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. EAI Endorsed Transactions on Creative Technologies, 8(28).

https://www.researchgate.net/profile/Muhammad-Akhtar-164/publication/353046785_The_future_of_Artificial_Intelligence_in_Cybersecurity_A_Comprehensive_Survey/links/60e5fe731c28af345850da39/The-future-of-Artificial-Intelligence-in-Cybersecurity-A-Comprehensive-Survey.pdf

20. Borges Amaro, L. J., Percilio Azevedo, B. W., Lopes de Mendonca, F. L., Giozza, W. F., Albuquerque, R. D. O., & García Villalba, L. J. (2022). Methodological framework to collect, process, analyze and visualize cyber threat intelligence data. Applied Sciences, 12(3), 1205.

https://www.mdpi.com/2076-3417/12/3/1205

21. Buchanan, B., Bansemer, J., Cary, D., Lucas, J., & Musser, M. (2020). Automating cyber attacks. Center for Security and Emerging Technology, 13-32.

Reddy, A. R. P. (2021). The role of artificial intelligence in proactive cyber threat detection in cloud environments. NeuroQuantology, 19(12), 764-773.

https://www.researchgate.net/profile/Abhilash-Reddy-Pabbath-Reddy/publication/378693448_THE_ROLE_OF_ARTIFICIAL_INTELLIGENCE_IN_PROACTIVE_CYBER_THREAT_DETECTION_IN_CLOUD_ENVIRONMENTS/links/65e5351bc3b52a11700a2759/THE-ROLE-OF-ARTIFICIAL-INTELLIGENCE-IN-PROACTIVE-CYBER-THREAT-DETECTION-IN-CLOUD-ENVIRONMENTS.pdf

22. Gatti, G. (2022). Towards Automated Information Gathering and Processing for Cyber Risk Assessment (Doctoral dissertation, Politecnico di Torino).

https://webthesis.biblio.polito.it/24475/

23. Colajanni, M., & Marchetti, M. (2021). Cyber attacks and defenses: current capabilities and future trends. In Technology and International Relations (pp. 132-151). Edward Elgar Publishing.

https://www.elgaronline.com/edcollchap/edcoll/9781788976060/9781788976060.00015.xml

24. Chlup, S., Christl, K., Schmittner, C., Shaaban, A. M., Schauer, S., & Latzenhofer, M. (2022). THREATGET: towards automated attack tree analysis for automotive cybersecurity. Information, 14(1), 14.

https://www.mdpi.com/2078-2489/14/1/14

25. Aldhaheri, F. (2021). Advanced AI in Early Threat Detection: Building Cybersecurity Ecosystems for Proactive Risk Assessment.

https://www.researchgate.net/profile/Fahmi-Aldhaheri/publication/384325749_Advanced_AI_in_Early_Threat_Detection_Building_Cybersecurity_Ecosystems_for_Proactive_Risk_Assessment/links/66f44173869f1104c6b4a225/Advanced-AI-in-Early-Threat-Detection-Building-Cybersecurity-Ecosystems-for-Proactive-Risk-Assessment.pdf

26. Madhavram, C., Galla, E. P., Sunkara, J. R., Rajaram, S. K., & Patra, G. K. (2022). AI-Driven Threat Detection: Leveraging Big Data For Advanced Cybersecurity Compliance. Available at SSRN 5029406.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5029406

27. Tsiknas, K., Taketzis, D., Demertzis, K., & Skianis, C. (2021). Cyber threats to industrial IoT: a survey on attacks and countermeasures. IoT, 2(1), 163-186.

https://www.mdpi.com/2624-831X/2/1/9

28. Pivarníková, M., Sokol, P., & Bajtoš, T. (2020). Early-stage detection of cyber attacks. Information, 11(12), 560.

https://www.mdpi.com/2078-2489/11/12/560

29. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7, 1-29.

https://link.springer.com/article/10.1186/s40537-020-00318-5

30. Kholidy, H. A. (2021). Autonomous mitigation of cyber risks in the Cyber–Physical Systems. Future Generation Computer Systems, 115, 171-187.

https://www.sciencedirect.com/science/article/abs/pii/S0167739X19320680

31. Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). A survey on cyber security threats in IoT-enabled maritime industry. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2677-2690.

https://ieeexplore.ieee.org/abstract/document/9758650

32. Stanikzai, A. Q., & Shah, M. A. (2021, December). Evaluation of cyber security threats in banking systems. In 2021 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1-4). IEEE.'

https://ieeexplore.ieee.org/abstract/document/9659862

33. Amal, M. R., & Venkadesh, P. (2022). Review of cyber attack detection: Honeypot system. Webology, 19(1), 5497-5514.

https://www.researchgate.net/profile/Amal-R-2/publication/358099519_Review_of_Cyber_Attack_Detection_Honeypot_System/links/6500426725ee6b7564e69913/Review-of-Cyber-Attack-Detection-Honeypot-System.pdf

34. Chayal, N. M., & Patel, N. P. (2020). Review of machine learning and data mining methods to predict different cyberattacks. Data Science and Intelligent Applications: Proceedings of ICDSIA 2020, 43-51.

https://link.springer.com/chapter/10.1007/978-981-15-4474-3_5

35. Radu, R., Săndescu, C., Grigorescu, O., & Rughiniş, R. (2020, December). Analyzing risk evaluation frameworks and risk assessment methods. In 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet) (pp. 1-6). IEEE.

https://ieeexplore.ieee.org/abstract/document/9324879

36. Lehto, M. (2022). Cyber-attacks against critical infrastructure. In Cyber security: Critical infrastructure protection (pp. 3-42). Cham: Springer International Publishing.

https://link.springer.com/chapter/10.1007/978-3-030-91293-2_1

37. kanth Mandru, S., & Gunuganti, A. (2021). Auto-Isolation: Enhancing Cybersecurity Resilience through Automated Network Segmentation in Response to Security Alerts. European Journal of Advances in Engineering and Technology, 8(6), 101-107.

https://www.researchgate.net/profile/Sri-Kanth-Mandru/publication/388183819_Auto-Isolation_Enhancing_Cybersecurity_Resilience_through_Automated_Network_Segmentation_in_Response_to_Security_Alerts/links/678deacc1ec9f9589f51a87e/Auto-Isolation-Enhancing-Cybersecurity-Resilience-through-Automated-Network-Segmentation-in-Response-to-Security-Alerts.pdf

38. Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. Information, 13(3), 146.

https://www.mdpi.com/2078-2489/13/3/146

39. Alloghani, M., Al-Jumeily, D., Hussain, A., Mustafina, J., Baker, T., & Aljaaf, A. J. (2020). Implementation of machine learning and data mining to improve cybersecurity and limit vulnerabilities to cyber attacks. Nature-inspired computation in data mining and machine learning, 47-76.

https://link.springer.com/chapter/10.1007/978-3-030-28553-1_3

40. Jawad, A., & Jaskolka, J. (2021, December). Analyzing the impact of cyberattacks on industrial control systems using timed automata. In 2021 IEEE 21st international conference on software quality, reliability and security (QRS) (pp. 966-977). IEEE.'

https://ieeexplore.ieee.org/abstract/document/9724903

41. Javeed, D., Khan, M. T., Ahmad, I., Iqbal, T., Badamasi, U. M., Ndubuisi, C. O., & Umar, A. (2020). An efficient approach of threat hunting using memory forensics. International Journal of Computer Networks and Communications Security, 8(5), 37-45.

https://www.researchgate.net/profile/Aliyu-Umar-2/publication/343913673_An_Efficient_Approach_of_Threat_Hunting_Using_Memory_Forensics/links/66e1c5b1f84dd1716ce762d4/An-Efficient-Approach-of-Threat-Hunting-Using-Memory-Forensics.pdf

42. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. computers & security, 89, 101677.

https://www.sciencedirect.com/science/article/abs/pii/S0167404819302172

43. Kumar, K., & Pande, B. P. (2022). Applications of machine learning techniques in the realm of cybersecurity. Cyber security and digital forensics, 295-315.

https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119795667.ch13

44. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. Network, 2(1), 123-138.

https://www.mdpi.com/2673-8732/2/1/9

45. Nedeljkovic, D., & Jakovljevic, Z. (2022). CNN based method for the development of cyber-attacks detection algorithms in industrial control systems. Computers & Security, 114, 102585.

https://www.sciencedirect.com/science/article/abs/pii/S0167404821004089

46. Alkahtani, H., & Aldhyani, T. H. (2022). Developing cybersecurity systems based on machine learning and deep learning algorithms for protecting food security systems: industrial control systems. Electronics, 11(11), 1717.

https://www.mdpi.com/2079-9292/11/11/1717

47. Peiris, C., Pillai, B., & Kudrati, A. (2021). Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks. John Wiley & Sons.

48. Kim, H. M., & Lee, K. H. (2022). IIoT malware detection using edge computing and deep learning for cybersecurity in smart factories. Applied Sciences, 12(15), 7679.

https://www.mdpi.com/2076-3417/12/15/7679

49. Nirmala, P., Ramesh, S., Tamilselvi, M., Ramkumar, G., & Anitha, G. (2022, January). An artificial intelligence enabled smart industrial automation system based on internet of things assistance. In 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-6). IEEE.

https://ieeexplore.ieee.org/abstract/document/9752651

50. Blum, D. (2020). Institute resilience through detection, response, and recovery. In Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment (pp. 259-295). Berkeley, CA: Apress.

https://link.springer.com/chapter/10.1007/978-1-4842-5952-8_9

51. Naanani, A., & Masaif, N. (2021). Security in Industry 4.0: Cyber-attacks and countermeasures. Turk. J. Comput. Math. Educ, 12(10), 6504-6512.

https://pdfs.semanticscholar.org/9376/394e4acae7eee14b391d8a3ff0a2fd85a8af.pdf

52. Czekster, R. M., Metere, R., & Morisset, C. (2022). Incorporating cyber threat intelligence into complex cyber-physical systems: A STIX model for active buildings. Applied Sciences, 12(10), 5005.

https://www.mdpi.com/2076-3417/12/10/5005

53. Zouave, E., Bruce, M., Colde, K., Jaitner, M., Rodhe, I., & Gustafsson, T. (2020). Artificially intelligent cyberattacks. Swedish Defence Research Agency, FOI, Tech. Rep. FOI.
54. Krundyshev, V., & Kalinin, M. (2020, September). Prevention of cyber attacks in smart manufacturing applying modern neural network methods. In IOP conference series: materials science and engineering (Vol. 940, No. 1, p. 012011). IOP Publishing.

    https://iopscience.iop.org/article/10.1088/1757-899X/940/1/012011/meta
55. Briliyant, O. C., Tirsa, N. P., & Hasditama, M. A. (2021, October). Towards an automated dissemination process of cyber threat intelligence data using stix. In 2021 6th International Workshop on Big Data and Information Security (IWBIS) (pp. 109-114). IEEE.
56. Md, R., & Tanvir Rahman, A. (2019). The Effects of Financial Inclusion Initiatives on Economic Development in Underserved Communities. *American Journal of Economics and Business Management*, *2*(4), 191-198.

    https://ieeexplore.ieee.org/abstract/document/9631850
57. DatasetLink:https://www.kaggle.com/datasets/supplejade/rt-iot2022real-time-internet-of-things