Securing and Detecting Attacks in Industrial IoT: An Efficient Intrusion Detection System (IDS) to detect the DOS Attack in IIoT

MSc Research Project
Cyber Security

Uche Lawrence Irobunda
Student ID: x21116113

School of Computing
National College of Ireland

Supervisor: Rohit Verma

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Uche Lawrence Irobunda		
Student ID:	X21116113		
Programme:	M.Sc Cyber Security	**Year:**	2022-2023
Module:	M.Sc. Research Project		
Supervisor:	Rohit Verma		
Submission Due Date:	25/04/2023		
Project Title:	Securing and Detecting Attacks in Industrial IoT: An Efficient Intrusion Detection System (IDS) to detect the DOS Attack in IIoT		
Word Count:	4750	**Page Count**	20

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ....

Date: ....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

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

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

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Securing and Detecting Attacks in Industrial IoT:

An Efficient Intrusion Detection System (IDS) to detect the DOS Attack in IIoT

Abstract

A large rise in the number of Internet of Things (IoT) devices has been caused by the quick development of interconnected computer devices and the appearance of new network technologies. Remote monitoring and cognitive analytics are being introduced with the Industrial Internet of Things (IIoT), resulting in further developments. While these gadgets simplify and automate routine tasks, they also present serious security dangers.

Implementing an intrusion detection system (IDS) and assessing its effectiveness within an Internet of Things (IoT) network are the main goals of this thesis. The goal of the study is to ascertain how well the IDS works to improve the IoT network's security and performance. The study specifically focuses on detecting and mitigating DOS attacks using SVM classification to detect cyber-attack on the network.

The study highlights the significance of integrating an IDS equipped with the ability to detect unusual traffic using SVM classification and a dataset.

1. Introduction

The Internet of Things (IoT) refers to the network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, and network connectivity, which enables them to collect and exchange data. These interconnected devices communicate with each other and with central data centers or cloud services, enabling real-time data analysis, monitoring, and control (Chandra Priya et al., 2021). The IoT technology provides numerous possibilities for diverse industries and use cases, as it is enabling seamless communication and collaboration among devices. However, like any novel technology, IoT is also accompanied by inherent security risks. (Ahamed & Rajan, 2017).

According to (Vorakulpipat et al., 2018), IoT devices are often designed to be user-friendly, lightweight, and portable, making them a convenient choice for a wide range of applications. The number of active IoT devices worldwide is projected to increase continuously, with more than 152,200 devices expected to be connected to the internet every minute by 2025. It is predicted that by 2030, there will be over 25.4 billion active IoT devices in use (Chawdhry et al., 2022). One of the driving factors for the growth of IoT in the region is the increasing use of smart sensors, which can be embedded into equipment and machines to collect and transmit data in real-time. This data can then be used to optimize operations, improve efficiency, and reduce costs. Another factor contributing to the growth of IoT in the region is the push for digital transformation, which is increasingly being adopted by businesses and governments. This includes the use of automation, data analytics, and cloud computing to improve processes and decision-making.

As IoT continues to grow, so does the risk of cyber-attacks on the industrial infrastructure. One such attack is the DoS attack, which can cause significant damage such as financial loss and potential safety hazards. To mitigate such attacks, it is crucial to secure IoT devices and implement proper detection and response mechanisms using an IoT hub and IDS. In today's interconnected world, such cyber-attacks are a growing concern for organizations.

This thesis aims to explore the use of IDS and IoT technology to prevent DoS attacks, with a focus on improving the performance of an IDS by machine learning. The research will begin with a review of current literature and case-studies of real-world scenarios of cyber-attacks. The use of an Intrusion Detection System (IDS) is a critical component of a comprehensive cyber-security strategy, as it can help to detect and respond to malicious activity on a network. When integrated with an IoT hub, an IDS can analyze traffic from many connected devices to identify signs of a cyber-attack.

To improve the performance of an IDS, a supervised machine learning model will be used based on the registration-based node authentication process to train an IDS to detect malicious activity more effectively. Using Support Vector Machines (SVM), the IDS can detect attacks based on its classification of network activities.

1.1. Motivation and Problem Definition

Recent studies by AT&T reveal that there has been a significant increase in the number of enterprises adopting IoT, with approximately 85% of them utilizing this technology. However, despite the widespread adoption, only 10% of these enterprises are confident that their IoT systems are fully secure and protected from cybercriminals (Iansiti et al., 1997). The low level of confidence in the security of IoT systems is not surprising considering the increasing frequency of attacks targeting these devices. Such attacks are particularly concerning for critical industrial sectors like healthcare, manufacturing, and power plants, where successful cyberattacks could have severe consequences. The interconnected nature of modern devices and systems creates numerous vulnerabilities that cybercriminals can exploit to launch their attacks (Saini & Saini, 2019).

There have been several instances of cyber-attacks that have been linked to IoT devices and the lack of security measures in place. One common type of attack is Distributed Denial of Service (DoS) attacks, which involve overwhelming a target system with traffic from multiple sources (Shah & Sengupta, 2020). These incidents highlight the importance of securing IoT devices and implementing measures to prevent cyber-attacks. One such measure is the use of an IoT hub with an IDS (Simpson et al., 2017; Sofia Anthi, 2022), which can help detect and prevent cyber-attacks on IoT devices. By monitoring network traffic and detecting anomalies, an IDS can identify and block malicious traffic before it can overload a network and cause disruption (Jesús et al., 2019).

The security of IoT devices is a significant concern, primarily due to their own vulnerability to cyber-attacks that can compromise individual devices and provide attackers with a gateway to more extensive networks. It is essential to have effective security mechanisms in place to prevent, detect, and mitigate these threats, particularly as IoT becomes more widely used in critical infrastructure and various industries.

1.2. Research Objective

1. What are the best practices that can be investigated to optimize the utilization of multiple IoT devices in IoT?
2. What are the key challenges associated with using an IDS integrated with an IoT hub, and how can they be addressed to improve the system's performance in preventing DoS attacks?
3. How can the use of an IDS integrated with an IoT hub and machine learning algorithms be implemented in real-world scenarios to effectively prevent DoS attacks?

1.3. Research Question

To evaluate the effectiveness of using machine learning to enhance the performance of an Intrusion Detection System (IDS) integrated with an IoT hub at preventing DoS attacks.

1.4. Justification

Industries are rapidly adopting IoT technology, which has led to the need for better network security measures. The Industrial Internet of Things (IIoT) allows for automation of tasks and the collection of data from various sources, resulting in improved efficiency and productivity for industries.

As industries rapidly adopt IoT technology, there is an increasing need for better network security measures. The Industrial Internet of Things (IIoT) allows for the automation of tasks and the collection of data from various sources, resulting in improved efficiency and productivity. The benefits of IIoT are numerous, including real-time monitoring and optimization of industrial processes, which can prevent downtime and improve product quality, reducing costs, and enhance safety by continuously monitoring equipment and processes. These advantages are made possible with sensors that detect changes in parameters set by the administrator. The literature review provides a comprehensive analysis of IoT technology and its integration with the Industrial IoT, utilizing emerging technologies such as Smart Hubs and Intrusion Detection Systems to enhance security measures.

2. Related Work

The rapid growth of the Internet of Things (IoT) has revolutionized various industries, enabling seamless connectivity and data exchange among devices, but it has also introduced significant security risks that need to be addressed. The IoT consists of different layers that interconnect to ensure smooth functioning. However, with the increasing number of connected devices, the IoT faces various challenges. One of the significant challenges facing IoT technology is the lack of adequate infrastructure and security mechanisms, which can compromise the protection of the various layers embedded in the IoT architecture. The scope of IoT technology extends across multiple sectors, including homes where wireless routers connect devices such as smoke alarms, refrigerators, thermostats, and lighting. The interconnectedness of these devices creates a seemingly seamless network, but it also presents a significant security risk as cyber-attacks on any of these devices can potentially compromise the entire network. The challenges and opportunities presented by the IoT are discussed in more detail in the literature review.

(Talwana & Hua, 2017) research focused on the functions and applications of IoT technology in various domains in our environment, including healthcare, transportation, agriculture, and energy management. The technology enables different devices and systems to communicate and share data with each other, but (Ling et al., 2018) emphasized the importance of end-to-end security for IoT architecture due to potential vulnerabilities that can lead to devastating consequences and financial losses. Their study also highlighted cyber security issues, such as botnets, and proposed measures to safeguard IoT architecture from such threats. The authors' research underscores the importance of addressing security concerns to ensure the safe and secure implementation of IoT technology. Additionally, (Agarwal et al., 2018) highlighted that the security of IoT devices is a significant issue because cybercriminals can target these devices and use them as a medium for launching larger attacks, such as distributed denial of service (DoS) attacks. IoT devices' vulnerability to such attacks arises because many users fail to change the default login credentials for their devices, making it easier for cybercriminals to detect and access these devices. Hackers can exploit tools like Shodan, which allow users to scan for connected devices on the internet, to identify vulnerable IoT devices.

The lack of uniform standardization in communication protocols used by IoT devices can also pose security risks, as highlighted in research by (Mohamed et al., 2022). Despite the widespread use of protocols like Message Queuing Telemetry Transport (MQTT), Advanced Message Queuing Protocol (AMQP), Long Range Wide Area Network (LoRaWAN), Data Distribution Service (DDS), and ZigBee in IoT devices, there is currently no clear framework for their implementation, leaving them vulnerable to exploitation. It is imperative that IoT device manufacturers prioritize security during the design phase and that users take necessary precautions to protect their devices, such as changing default login credentials and regularly updating them with the latest security patches.

Based on recent studies, it has been noted that the security of the Internet of Things (IoT) is dependent on securing every layer of the architecture that underlies the IoT system (Abdullah et al., 2020; Mrabet et al., 2020; Rizvi et al., 2018). Such layers may include smart device networks, gateways, user platforms, and the end application. It is crucial to ensure the security of all these layers as they play a significant role in determining the overall security of the IoT system.

2.1. Industrial Internet of Things

(Mosteiro-Sanchez et al., 2020) highlighted that the IIoT pertains to the integration of IoT technology in the industrial sector, wherein industrial products and equipment are linked to the internet, enabling communication and data exchange among them and other systems. The IIoT can boost the effectiveness, productivity, and safety of industrial processes and systems, but it is also susceptible to the security risks and vulnerabilities that are associated with IoT technology.

According to a study by (Asemani et al., 2019), the IIoT architecture comprises two classifications: Information Technology (IT) and Operational Technology (OT). By adopting IIoT, organizations can provide value-added services such as remote monitoring, maintenance, and insurance, which can generate additional revenue. The availability of real-time and accurate information from IoT sensors and connectivity makes these services more profitable and feasible, while also reducing overall expenses by enabling remote management.

2.2. Cyber-Security in Industrial Internet of Things

Security is a major concern for all industries. As manufacturing becomes more connected, it is important to understand the vulnerabilities that could affect consumers. When considering industrial or manufacturing IoT initiatives, organizations must be aware of potential risks and attack vectors that could harm the company and consumers. Research conducted by (Andrea et al., 2015; Pongle & Chavan, 2015; Shukla, 2017) have demonstrated that cyber criminals have taken advantage of security vulnerabilities in individual IoT devices to target the broader network they are connected to. According to (Da Xu et al., 2014; Goundar et al., 2021) there are reportedly more attack vectors that target IoT devices than traditional ICT systems, highlighting the need to prioritize privacy protection in the IoT environment. The absence of a secure and encrypted network infrastructure could render the adoption of IIoT vulnerable to security threats.

2.3. Cyber-attack in IIoT

The deployment and use of IoT in IIoT settings brings about various security limitations that are dependent on the network infrastructure's features. There are two main reasons why cyberattacks are prevalent in IoT devices:

1) The extensive attack surface that results from the heterogeneity of devices in an IoT environment makes it challenging to implement security mechanisms that apply universally across all devices.
2) The security of IoT is significantly influenced by device computing power limitations, including memory, battery capacity, and radio bandwidth, which render IoT devices incapable of implementing robust security measures.

The presence of a vast array of diverse IoT devices in an the IIoT environment poses a challenge for traditional centralized security solutions. This challenge is heightened when deploying these technologies in trustless environments or interacting with IoT devices installed in such environments.

2.4. Securing IoT devices in Industrial IoT

Numerous studies have explored the security of the Internet of Things (IoT), with researchers focusing on addressing specific security concerns (Ling et al., 2018; Pranata et al., 2012; Ye et al., 2014; Zhao, 2013). However, the heterogeneity of IoT devices present a challenge in implementing uniform security mechanisms. This is because different devices have unique capabilities and constraints, making it difficult to find security mechanisms that are effective for all devices. Furthermore, some security solutions require substantial computation and communication resources, which may not be practical for lightweight, low-cost devices like sensors.

2.5. IoT Hub

An IoT hub is designed to function as a centralized point for managing and communicating with connected devices within an IoT network. As IoT devices typically have limited computing capabilities and are designed for specific functions, such as data collection or device control, the hub acts as a more capable intermediary for processing and storing data, as well as communication. The use of IoT hubs is widespread and can be seen in various applications such as home automation, industrial automation, and transportation. This addresses the second research objective, which is to identify the main challenges associated with using an IDS integrated with an IoT hub and propose solutions to enhance the system's performance in preventing DoS attacks.

IoT hubs serve the following functions:

I. Authentication: The hub confirms the user's identity.
II. Confidentiality: The hub safeguards against unauthorized access to data
III. Access Control: The hub restricts device interactions to specific users and times.
IV. Device Cloaking: The hub conceals IoT devices to make them more difficult for attackers to find.
V. Heterogeneity Awareness: The hub supports different devices from multiple manufacturers.

However, it is important to note that IoT hubs themselves may also be vulnerable to attacks, so it is crucial to ensure their own security. Overall, the use of IoT hubs can be an effective strategy for managing and securing a range of IoT devices, but it is important to carefully consider security implications and take necessary precautions to prevent potential threats. As such it answers the research objective “What are the best practices that can be investigated to optimize the utilization of multiple IoT devices in IoT? “

2.6. Detecting a DoS Attack in Industrial IoT

DoS attacks are one of the most common types of cyber-attacks in the Industrial IoT. A DoS attack involves overwhelming a network or server with a large volume of traffic, rendering it inaccessible to legitimate users. In Industrial IoT, a DoS attack can disrupt the manufacturing process, leading to production downtime, financial loss, and reputational damage. The introduction of a security tool called an Intrusion Detection System (IDS) can aid in detecting potential attacks. An IDS works by analyzing data from IoT devices and other connected devices, looks for patterns or unusual network activity that could indicate an attack.

In the context of Industrial Internet of Things (IIoT) systems, an IDS plays a critical role in securing the network by monitoring the various devices and sensors used in industrial applications. An IoT hub can be used to manage multiple IoT devices on the network and provide a secure access control mechanism, while the IDS can help prevent cyber-attacks by detecting malicious network behavior. This combination of security measures can help protect sensitive data and prevent potentially costly cyber-attacks on industrial systems. This answers our first research objective "What are the best practices that can be investigated to optimize the utilization of multiple IoT devices in IIoT? "

2.7. IDS in Industrial IoT

An Intrusion Detection System (IDS) is a security tool designed to monitor IoT systems for signs of cyber-attacks and alert the network administrator of any suspicious activity, helping prevent network-based attacks before they cause damage. In the context of Industrial Internet of Things (IIoT) systems, an IDS plays a critical role in securing the network by monitoring the various devices and sensors used in industrial applications. An IoT hub serves as a central point for managing and communicating with connected devices in an IIoT network, providing a secure access control mechanism. Combining an IDS with an IoT hub can help prevent potentially costly cyber-attacks on industrial systems by detecting malicious network behavior and protecting sensitive data. Therefore, this combination of security measures can improve the overall security posture of an IIoT system.

One study by (Sambangi et al., 2022) proposed a machine learning-based approach to detecting and mitigating DoS attacks in Industrial IoT. The study utilized an ensemble of machine learning algorithms to analyze network traffic and detect DoS attacks. The results showed that the proposed approach was effective in detecting and mitigating DoS attacks in Industrial IoT. A key challenge associated with integrating an IDS with an IoT hub is the high volume and velocity of network traffic generated by IoT devices can cause false positives or false negatives in the detection of DoS attacks (Lawal et al., 2021). This can be addressed by developing machine learning algorithms that are specifically designed to detect DoS attacks in IoT networks and can handle the high volume and velocity of network traffic generated by IoT devices which addresses our third research objective (Gaur & Kumar, 2022).

To address the challenges arising from the diversity of IoT devices, our research proposes the use of IoT hubs, which provide a unified platform for managing and securing a range of devices. These hubs can incorporate extra security features such as authentication, encryption, and access control, which can help minimize the risk of cyber-attacks.

2.8. Support Vector Machine

Support Vector Machine is regarded as one of the best learning algorithms for binary classification and is effective in handling high-dimensional data, which is often the case in IIoT systems that collect large amounts of sensor data (Hsu et al., 2019). SVM works by finding the optimal hyperplane that separates the two classes in a dataset. In the context of detecting attacks in an IIoT infrastructure, SVM can be used to classify network traffic into two classes, normal and anomalous (Boser et al., 1992). This is achieved by training the SVM algorithm on a dataset of normal and attack traffic, and then using it to classify new traffic as either normal or anomalous based on the learned pattern. In the context of IIoT, this means that the SVM algorithm can be trained on data collected from sensors in the IIoT infrastructure to differentiate between normal and abnormal behavior (Hsu et al., 2019; Jha & Ragha, 2013).

2.9. Why NS-3?

As a graduate student in cybersecurity, I conducted extensive research on various network simulators to use in my project. After consulting with some colleagues in the industry and discussing with a recent graduate who had experience in using different network simulators, I decided to use NS-3 for my simulation. I found that NS-3 was highly recommended for its accuracy, flexibility, and the availability of many built-in models and protocols.

The simulator provides a range of pre-built network models, protocols, and devices that can be easily modified and customized to fit the specific requirements of a simulation study. NS-3 has a powerful visualization toolkit called Net Anim, that allows for the display of simulation results in an intuitive and visually appealing manner. This feature is crucial for interpreting and communicating simulation results effectively.

I also found that NS-3 had excellent support for wireless networks and Internet of Things (IoT) simulations, which was highly relevant to my project's focus on evaluating the effectiveness of using machine learning to enhance the performance of an Intrusion Detection System (IDS) integrated with an IoT hub in preventing DDoS attacks.

3. Research Methodology

The objective of this paper is to tackle the security weaknesses of IoT and to provide consumers with the necessary information to make informed decisions about the security of these devices. The goal is to enhance the security of IoT devices against cyber-attacks and improve the detection and mitigation of DoS attacks. The research will use the NSL-KDD dataset and machine learning based on SVM classification, with ethical considerations including data privacy and security metrics. The analysis will be focused on the classification accuracy and performance of our model. Also, the research will involve integrating an IDS with an IoT hub as part of the research design.

1. Research Design:

   The research design for this study is experimental. Experimental research design is the best approach to investigate the effectiveness of different models, algorithms, and techniques in detecting, preventing, and mitigating DoS attacks in IoT. The use of experimental research design will allow the researcher to control the variables and establish cause-effect relationships between the dependent and independent variables. The study will involve setting up a simulated Industrial IoT network, which will be used to test the effectiveness of various DoS attack detection and mitigation techniques. The experiments will be designed to evaluate the performance of an IDS integrated with an IoT hub.
2. Data Methods:

   Data set used will be gotten from the Canadian Institute for Cybersecurity called the NSL-KDD. It will be modified to fit our scenario, adjusting to detect several forms of cyber-attack.
3. Experimental Procedure:

   The experiment will involve the following steps:

- Setting up a simulated Industrial IoT network, consisting of thirty IoT devices, an IoT hub, and an attacker node.
- Configuring the IoT hub to receive and transmit data from the devices in the network.
- Integrating an IDS with the IoT hub and configuring it to detect and mitigate DoS attacks.
- IDS in the hub analyzes traffic from many connected devices based on the patterns in our dataset, using SVM Classifier and identifies signs of an attack.
- Conducting simulated DoS attacks on the network, with varying parameters Measuring the effectiveness of the IDS in detecting and mitigating DoS attacks
- Perform the mitigation process based on SVM classification.

4. Ethical Considerations:

   We will ensure that ethical considerations are observed during the study. The informed consent of the participants will be obtained, and their confidentiality will be guaranteed.

5. Limitations:

   Studying has some limitations. First, the study will be conducted in a simulated environment, which may not reflect the real-world scenarios. Second, the study will be conducted with a small dataset and thus may limit the generalizability of the study results.

6. Significance of the Study:

   The study's significance is in developing an effective system for detecting and mitigating DoS attacks in IoT environments. The study's results will provide insights into the effectiveness of the proposed system and inform the development of better security measures for IoT systems.

4. Design Specifications

We utilized a virtual machine running Ubuntu 14.04 and installed Network Simulator 3.26 (NS-3). The program simulates an intrusion detection system for a DoS attack on an Internet of Things (IoT) network. 30 devices are included in the simulation, along with a hub that serves as a server and archives the data. The hub interacts with the IoT devices and uses Support Vector Machine

(SVM) classifier to analyze the traffic to look out for potential attacks. The code is written in C++ using the Ns-3 network simulator library.

5. Implementation

The simulation makes use of the NS-3 network simulator and has modules for the core, network, mobility, configuration storage, Wi-Fi, internet, flow monitoring, and IoT. Using UDP sockets and the GenerateTraffic function, the simulation produces traffic and mimics packet transmission. SVM is also used in the simulation to categorize traffic and spot attacks. The main function loads the simulation parameters and configures the network architecture, which is made up of three node containers: IoTNodes, AttackerNode, and IoTHub_Node. Figure 1 shows the diagrammatic representation of the proposed system.

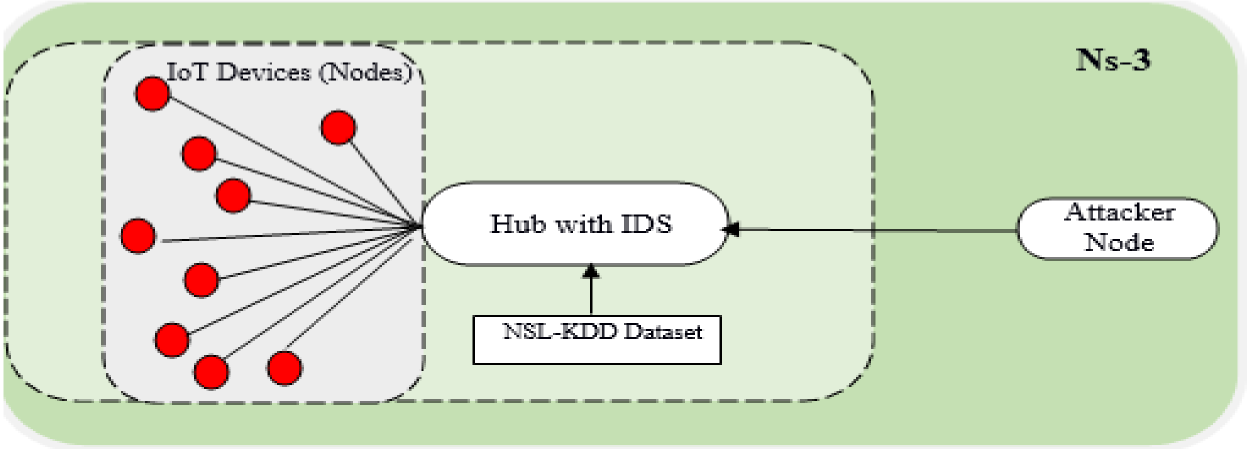


Figure 1: Diagrammatic Representation of Ns-3

6. Evaluation

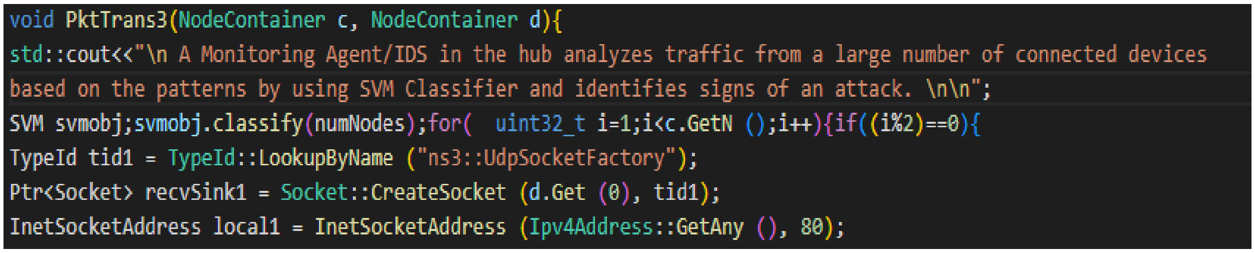
Our simulation focused on developing an efficient IDS to detect a DOS attack in an IoT environment. The system consists of a network comprising of 30 IoT devices, an attacker node, and an IoT hub with a monitoring agent. The IoT devices undergo a registration process with several unique metrics such as the Id, PUF, IMEI, and MAC address. The devices communicated sensed data with the IoT hub which acts as a central server and stores the data. The Monitoring agent (IDS) in the hub analyses the traffic from the connected devices and using our SVM classifier dataset detects unusual traffic which are potential signs of attack.

6.1. Discussion

The code can be broken down into four distinct functions that mimic DOS attack detection by an IDS in the hub and communication between IoT devices and an IoT hub. The primary function accepts as inputs, among other things, the number of nodes, the size of the packet, and the separation between nodes. The simulation process involved the following steps:

1. Main: This function configures the simulation environment by defining node containers for IoT devices, the attacker node, and the IoT Hub node. It also configures simulation parameters such as node distance, packet size, and node count.
2. Data Transmission: The PktTrans1 and PktTrans2 are functions that establish communication between the IoT devices and the IoT hub nodes using UDP sockets and generate traffic at fixed intervals and packet sizes. The hub acts as a server and stores the data.
3. Analyzing the traffic: The PktTrans3 function analyses the incoming traffic based on the SVM classifier and identifies signs of attacks.

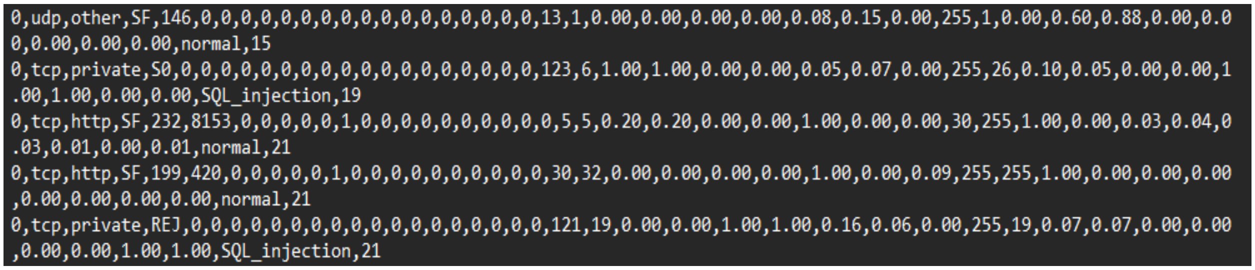
The training and testing results were generated by combining data in the dataset and configuring the model to look out for the pattern categorized as malicious. The categorization used in our program is shown in Figure 2.



```
void PktTrans3(NodeContainer c, NodeContainer d){
std::cout<<"\n A Monitoring Agent/IDS in the hub analyzes traffic from a large number of connected devices
based on the patterns by using SVM Classifier and identifies signs of an attack. \n\n";
SVM svmobj;svmobj.classify(numNodes);for(  uint32_t i=1;i<c.GetN ();i++){if((i%2)==0){
TypeId tid1 = TypeId::LookupByName ("ns3::UdpSocketFactory");
Ptr<Socket> recvSink1 = Socket::CreateSocket (d.Get (0), tid1);
InetSocketAddress local1 = InetSocketAddress (Ipv4Address::GetAny (), 80);
```

Figure 2: Using SVM Model to Analyze Network Traffic.

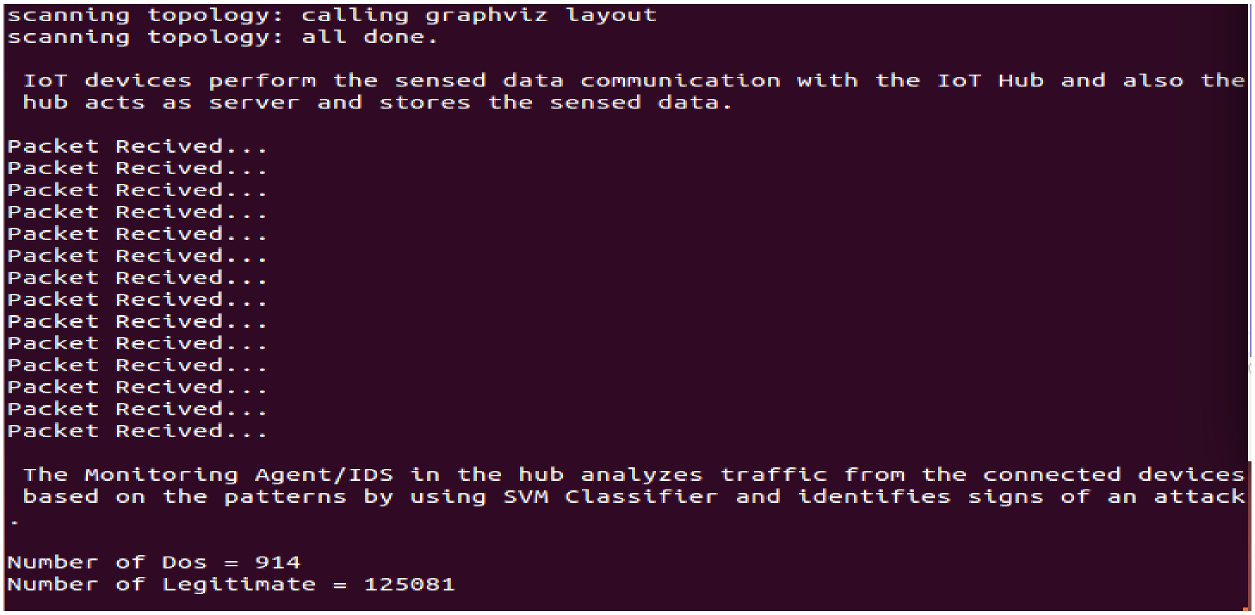
The program can now identify odd traffic based on the datasets provided, but no specific safeguards are in place to guard against any malicious assault harming the network. An example of traffic data is showed in Figure 3.



```
0,udp,other,SF,146,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,13,1,0.00,0.00,0.00,0.00,0.08,0.15,0.00,255,1,0.00,0.60,0.88,0.00,0.0
0,0.00,0.00,0.00,normal,15
0,tcp,private,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,123,6,1.00,1.00,0.00,0.00,0.05,0.07,0.00,255,26,0.10,0.05,0.00,0.00,1
.00,1.00,0.00,0.00,SQL_injection,19
0,tcp,http,SF,232,8153,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,5,5,0.20,0.20,0.00,0.00,1.00,0.00,0.00,30,255,1.00,0.00,0.03,0.04,0
.03,0.01,0.00,0.01,normal,21
0,tcp,http,SF,199,420,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,30,32,0.00,0.00,0.00,0.00,1.00,0.00,0.09,255,255,1.00,0.00,0.00,0.00
,0.00,0.00,0.00,0.00,normal,21
0,tcp,private,REJ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,121,19,0.00,0.00,1.00,1.00,0.16,0.06,0.00,255,19,0.07,0.07,0.00,0.00
,0.00,0.00,1.00,1.00,SQL_injection,21
```

Figure 3: Dataset Image Showing Various Types of Traffic

Following the execution of the simulation, based on the dataset used, malicious traffic is detected. The result is seen in Figure 4 showing the total number of malicious traffic and legitimate traffic



```
scanning topology: calling graphviz layout
scanning topology: all done.

 IoT devices perform the sensed data communication with the IoT Hub and also the
 hub acts as server and stores the sensed data.

Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...

 The Monitoring Agent/IDS in the hub analyzes traffic from the connected devices
 based on the patterns by using SVM Classifier and identifies signs of an attack
.

Number of Dos = 914
Number of Legitimate = 125081
```

Figure 4: Result from the Simulation Attack Based on Dataset.

To effectively mitigate the attack, it is advised to put additional precautions in place, such as firewalls to block the detected traffic and the usage of IPS to stop the traffic from getting to the network and impacting it.

7. Conclusion and Future Work

In conclusion, this study highlights the importance of implementing an Intrusion Detection System (IDS) in an IoT network to enhance security and improve network performance. The simulation results showed that the IDS agent was highly effective in detecting potential attacks.

Future work can focus on evaluating the performance of the network under different attack scenarios and comparing the effectiveness of different IDS algorithms. There is still room for improvement in terms of implementing the SVM, making the simulation more flexible, and including performance metrics and analysis of the results. Overall, the study highlights the need for a more secure and reliable IoT network infrastructure and the importance of using simulations to evaluate and improve these systems.

8. Reference

Abdullah, A., Kaur, H., & Biswas, R. (2020). Universal Layers of IoT Architecture and Its Security Analysis. In *New Paradigm in Decision Science and Management* (pp. 293–302). Springer.

Agarwal, M., Sarkhel, D., & Samanta, D. (2018). An Overview: Security Issue in IoT Network. *Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018*, 491–494. https://doi.org/10.1109/ICISC.2018.8399121

Ahamed, J., & Rajan, A. V. (2017, January 13). Internet of Things (IoT): Application systems and security vulnerabilities. *International Conference on Electronic Devices, Systems, and Applications*. https://doi.org/10.1109/ICEDSA.2016.7818534

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC)*, 180–187.

Asemani, M., Jabbari, F., Abdollahei, F., & Bellavista, P. (2019). A comprehensive fog-enabled architecture for iot platforms. *International Congress on High-Performance Computing and Big Data Analysis*, 177–190.

Boser, B. E., Guyon, I. M., & Vapnik, V. N. (1992). A training algorithm for optimal margin classifiers. *Proceedings of the Fifth Annual Workshop on Computational Learning Theory*, 144–152.

Chandra Priya, J., Puvaneswari, S., & Raju, S. (2021). BIIoT: Provenance of Industrial IoT Data with Blockchain Technology. *International Journal of Engineering Research & Technology (IJERT). ICRADL*. www.ijert.org

Chawdhry, A., Paullet, K., & Pinchot, J. (2022). Internet of things: Measuring data privacy concerns of users. *Issues in Information Systems*, *23*(4).

Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics*, *10*(4), 2233–2243.

Gaur, V., & Kumar, R. (2022). Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices. *Arabian Journal for Science and Engineering*, *47*(2), 1353–1374. https://doi.org/10.1007/s13369-021-05947-3

Goundar, S., Bhardwaj, A., Nur, S. S., Kumar, S. S., & Harish, R. (2021). Industrial Internet of Things: Benefit, Applications, and Challenges. *Innovations in the Industrial Internet of Things (IIoT) and Smart Factory*, 133–148.

Gresak, E., & Voznak, M. (2020). Protecting Gateway from ABP Replay Attack on LoRaWAN. In P. and T. D. T. and H. D. V. and K. S. B. Zelinka Ivan and Brandstetter (Ed.), *AETA 2018 - Recent Advances in Electrical Engineering and Related Sciences: Theory and Application* (pp. 400–408). Springer International Publishing.

Hsu, H.-T., Jong, G.-J., Chen, J.-H., & Jhe, C.-G. (2019). Improve Iot Security System Of Smart-Home by Using Support Vector Machine. *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, 674–677. https://doi.org/10.1109/CCOMS.2019.8821678

Iansiti, M., West, J., & Horii, D. ilustraciones. (1997). *Technology integration: Turning great research into great products*. Harvard Business School.

Jesús, R.-L. J., Cristhian, P.-V. O., René, R.-G. M., & Heberto, F.-M. (2019). How to improve the iot security implementing ids/ips tool using raspberry pi 3b. *Editorial Preface from the Desk of Managing Editor*, *10*(9).

Jha, J., & Ragha, L. (2013). Intrusion detection system using support vector machine. *International Journal of Applied Information Systems (IJAIS)*, *3*, 25–30.

Lawal, M. A., Shaikh, R. A., & Hassan, S. R. (2021). A DDoS attack mitigation framework for IoT networks using fog computing. *Procedia Computer Science*, *182*, 13–20.

Ling, Z., Liu, K., Xu, Y., Gao, C., Jin, Y., Zou, C., Fu, X., & Zhao, W. (2018). *IoT Security: An End-to-End View and Case Study*. http://arxiv.org/abs/1805.05853

Mohamed, A., Wang, F., Butun, I., Qadir, J., Lagerström, R., Gastaldo, P., & Caviglia, D. D. (2022). Enhancing Cyber Security of LoRaWAN Gateways under Adversarial Attacks. *Sensors*, *22*(9). https://doi.org/10.3390/s22093498

Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieta, A. (2020). Securing IIoT using defence-in-depth: towards an end-to-end secure industry 4.0. *Journal of Manufacturing Systems*, *57*, 367–378.

Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors*, *20*(13), 3625.

Pongle, P., & Chavan, G. (2015). Real time intrusion and wormhole attack detection in internet of things. *International Journal of Computer Applications*, *121*(9).

Pranata, H., Athauda, R., & Skinner, G. (2012). Securing and governing access in ad-hoc networks of internet of things. *Proceedings of the IASTED International Conference on Engineering and Applied Science, EAS*, 84–90.

Rizvi, S., Kurtz, A., Pfeffer, J., & Rizvi, M. (2018). Securing the internet of things (IoT): A security taxonomy for IoT. *2018 17th IEEE International Conference on Trust, Security and Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 163–168.

Saini, M. K., & Saini, R. K. (2019). Internet of Things (IoT) Applications and Security Challenges: A Review. *International Journal of Engineering Research & Technology (IJERT). NCRIETS.* www.ijert.org

Sambangi, S., Gondi, L., & Aljawarneh, S. (2022). A feature similarity machine learning model for ddos attack detection in modern network environments for industry 4.0. *Computers and Electrical Engineering*, *100*, 107955.

Shah, Y., & Sengupta, S. (2020). A survey on Classification of Cyber-attacks on IoT and IIoT devices. *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 406–413.

Shukla, P. (2017). ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things. *2017 Intelligent Systems Conference (IntelliSys)*, 234–240.

Simpson, A. K., Roesner, F., & Kohno, T. (2017). Securing vulnerable home IoT devices with an in-hub security manager. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 551–556.

Sofia Anthi, E. (2022). *Detecting and Defending against Cyber Attacks in a Smart Home Internet of Things Ecosystem*.

Talwana, J. C., & Hua, H. J. (2017). Smart World of Internet of Things (IoT) and its Security Concerns. *Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, IThings-GreenCom-CPSCom-Smart Data 2016*, 240–245. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.64

Vorakulpipat, C., Rattanalerdnusorn, E., Thaenkaew, P., & Dang Hai, H. (2018). Recent challenges, trends, and concerns related to IoT security: An evolutionary study. *International Conference on Advanced Communication Technology, ICACT*, *2018-February*, 405–410. https://doi.org/10.23919/ICACT.2018.8323774

Ye, N., Zhu, Y., Wang, R., Malekian, R., & Lin, Q. (2014). *An efficient authentication and access control scheme for perception layer of internet of things*.

Zhao, Y. L. (2013). Research on data security technology in internet of things. *Applied Mechanics and Materials*, *433*, 1752–1755.