

Securing the MediColBox

a study on how accelerometers can detect intrusion

Å sikre en MediColBox

en studie om hvordan akselerometre kan oppdage innbrudd

Lars Birger Bergmål

321

Bachelor's thesis in Control System Engineering

Faculty of Engineering and Science

Western Norway University of Applied Science

May 6, 2024



Western Norway
University of
Applied Sciences

Abstract

EN - english

This study focuses on the development of a solution to prevent theft and break-ins in medicine collection systems, specifically targeting the MediColBox. The proper disposal of unused and expired medications is crucial for public health, as improper disposal can lead to environmental contamination and potential harm to individuals. The objective of this research is to find methods to detect and deter intrusion attempts in these systems, aiming to minimize the risk of medication loss or theft. A scaled-down prototype utilizing an Inertial Measurement Unit (IMU) is constructed to evaluate different detection and notification methods. The study examines accelerometer data collected during simulated intrusion events, including striking, dropping, sawing, and shaking of the MediColBox. The results demonstrate the effectiveness of the IMU in detecting and capturing accelerative patterns associated with these intrusion scenarios. However, it is noted that the IMU's sensitivity may lead to false alarms, necessitating the exploration of pattern recognition software and machine learning algorithms to enhance the system's accuracy. The study also discusses the potential of combining the accelerometer data with gyroscope data to understand the relationship between acceleration and orientation during intrusion events. The findings strongly support the feasibility of utilizing the IMU as a standalone solution for enhancing the security and protection of the MediColBox. Further research directions include integrating other sensor types, such as the gyroscope, and exploring the applicability of this intrusion detection approach to other systems beyond medicine collection boxes. The outcomes of this study contribute to improving the overall security and integrity of portable storage systems and preventing unauthorized access.

NO - Norsk

Denne studien fokuserer på utviklingen av en løsning for å hindre tyveri og innbrudd i medisinske innsamlingssystemer, spesielt rettet mot MediColBox. Riktig håndtering av ubrukte og utløpte medisiner er avgjørende for folkehelsen, da feilaktig håndtering kan føre til miljøforurensning og potensiell skade på enkeltpersoner. Målet med denne forskningen er å finne metoder for å oppdage og avverge innbruddsforsøk i disse systemene, med sikte på å minimere risikoen for tap eller tyveri av medisiner. En nedskalert prototype som bruker en IMU er konstruert for å evaluere ulike metoder for deteksjon og varsling. Studien undersøker akselerometerdata som er samlet inn under simulerte innbruddshendelser, inkludert slag, dropp, såing og risting av MediColBox. Resultatene viser effektiviteten til IMU i å oppdage og fange opp akselerasjonsmønstre knyttet til disse innbruddsscenarioene. Imidlertid bemerkes det at IMUs følsomhet kan føre til falske alarmer, og det er derfor behov for utforsking av mønstergjenkjenning og maskinlæringsalgoritmer for å forbedre nøyaktigheten til systemet. Studien diskuterer også potensialet for å kombinere akselerometerdata med gyroskopdata for å forstå sammenhengen mellom akselerasjon og orientering under innbruddshendelser. Funnene støtter sterkt muligheten for å bruke IMU som en frittstående løsning for å forbedre sikkerheten og beskyttelsen av MediColBox. Videre forskningsretninger inkluderer integrering av andre sensortyper, som gyroskopet, og utforsking av anvendeligheten av denne innbruddsdeteksjonsmetoden på andre systemer utenfor medisinske innsamlingsskap. Resultatene fra denne studien bidrar til å forbedre den generelle sikkerheten og integriteten til bærbare lagringssystemer og forhindre uautorisert tilgang.

Acknowledgments

I would like to thank the following people for their help and support:

- **Edmundo Villacorta Soriano:** for sharing his vast amount of knowledge and experience in the different fields spanning this thesis, and for spending his even greater patience to guide me away from folly and towards writing a proper report

CONTENTS

Acknowledgments	1
List of Figures	3
List of Tables	3
Glossary	4
I Introduction	4
I-A Background	4
I-B Objectives	5
I-C Limitations	5
I-D Project Stakeholders	5
II Background	5
II-A Definition of the problem	5
III Methodology	7
III-A Phenomenon of Interest	8
III-B Data Collection Methods	8
III-C Prototype Construction	10
III-D Sampling Strategy	11
III-E Data Collection Procedures	11
III-F Ethical Considerations	13
III-G Data Analysis	13
III-H Limitations	14
III-I Tools and Technologies	14
III-J Document Preparation	15
IV Results	15
IV-A Analysis of Accelerometer Data	15
IV-A1 Striking the MediColbox	16
IV-A2 Dropping the MediColbox	18
IV-A3 Sawing on the MediColbox	19
IV-A4 Shaking the MediColbox	20
IV-B Discussion of Findings	21
V Conclusion	22
References	23

LIST OF FIGURES

1	Design of the prototype with the cover on	10
2	Design of the prototype without the cover	10
3	The “wiring diagram” used	12
4	The Sequence diagram used for the program	12
5	Photograph of the prototype	12
6	Accelerometer data during the striking event	16
7	Fourier analysis of accelerometer data during the striking event	17

8	Accelerometer data during the dropping event	18
9	Fourier analysis of accelerometer data during the dropping event	18
10	Accelerometer data during the sawing event	19
11	Fourier analysis of accelerometer data during the sawing event	19
12	Accelerometer data during the shaking event	20
13	Fourier analysis of accelerometer data during the shaking event	20

LIST OF TABLES

I	Types of Intrusion Attempts	6
II	Potential Security Measures for MediColbox	8
III	Potential Data Collection Methods for Intrusion Attempts	9
IV	Possible Data Collection Methods for Intrusion Attempts	13

GLOSSARY

Actuator	Device or mechanism that convert energy into physical motion or force, often used to control or manipulate a system. Examples of actuators include electric motors, solenoids, hydraulic cylinders, and pneumatic actuators. Actuators are commonly used in a wide range of applications, such as robotics, automation, and control systems.
CCU	A component of a system that is responsible for coordinating and managing the activities of other components. In a computer system, the central control unit (CCU) is often the main processor or microcontroller that executes instructions and manages input/output operations.
DSI	Display Serial Interface is a specification used for connecting display panels to electronic devices. It provides a high-speed, serial communication interface for transmitting display data, control signals, and power between devices such as microcontrollers or graphics processing units and display panels.
Exploit	An act of utilizing something to gain a benefit or advantage. The term can be used in various contexts, such as in technology, economics, or social interactions.
HMI	Human-Machine Interface is a system that allows humans to interact with a machine or computer system, often through a graphical user interface or touch screen. The HMI enables the user to control and monitor the machine or system, and provides feedback to the user about its status and performance.
IMU	A device that consists of multiple sensors, such as accelerometers, gyroscopes, and magnetometers, that measures the orientation, velocity, and gravitational forces of an object in motion. IMUs are commonly used in robotics, unmanned vehicles, and virtual reality systems to provide accurate position and motion tracking. They can also be used for stabilization and navigation purposes in aerospace and marine applications.
Intrusion	The act of intruding or the state of being intruded. especially: the act of wrongfully entering upon, seizing, or taking possession of the property of another
MediColBox	The medicine collection part of Medretur's solution for collecting the medicine
RIO	A type of input/output (I/O) system that is located away from the central processing unit (CPU) or main controller, and is connected through a network or communication link. Remote input/output (RIO) systems typically consist of one or more I/O modules that are connected to a communication interface or network adapter.
Sensor card	A printed circuit board (PCB) or electronic module that contains one or more sensors, such as temperature sensors, humidity sensors, pressure sensors, or motion sensors. Sensor cards are often used in electronic systems for data acquisition, monitoring, or control purposes.
Single-board computer	A complete computer system built on a single circuit board, which includes all the basic components of a computer, such as a central processing unit (CPU), memory, input/output (I/O) ports, and storage. SBCs are designed to be compact, low-power, and cost-effective, and are often used for embedded systems, prototyping, and hobbyist projects. They can be used for a wide range of applications, such as robotics, Internet of Things (IoT) devices, and home automation. Examples of popular SBCs include the Raspberry Pi, BeagleBone, and Arduino.
USB	Universal Serial Bus is a common interface that allows communication between computers and peripheral devices. It provides a standardized connection and protocol for connecting devices such as keyboards, mice, printers, and storage devices.

I. INTRODUCTION

Medretur wants to develop a medicine collection system that automates the process of disposing of medicines. The task of this project is to research and find methods for this system to detect and deter intrusion attempts. This chapter presents background information on the research project, including its objectives and limitations. Information is also provided on the company that commissioned the study.

A. Background

The proper disposal of unused and expired medication is a critical public health issue [1]. Improper disposal of such medicines can lead to contamination of the environment and potential harm to human health [2], [3]. Collection programs for unused medicines have been established to address this issue [4]–[6], but these programs often face challenges in terms of security [7]. This is because these programs deal with sensitive materials that may be valuable to others [8].

B. Objectives

The purpose of this task is to find a solution to prevent theft and break-ins in systems for collecting medicines.

The aim of the proposed solution is to allow such systems to operate without the risk of medications being lost or stolen.

The task aims to evaluate different detection and notification methods and create a scaled-down prototype, and then conclude whether or not this solution works.

C. Limitations

Parts of a control system that use the same components as the existing control system in the MediColBox will be constructed.

The full-scale control system will have the same CCU, HMI, and sensor card, but also remote input/output (RIO) for the actuators.

The prototype that will be assembled is a Single-board computer Raspberry Pi 4B 8GB [9] as CCU, with a 7-inch touchscreen [10] as HMI and a Raspberry Pi Sense Hat v1.0.0 [11] as a sensor card. The purpose of constructing the prototype is to use the IMU in the sensor card.

D. Project Stakeholders

The company **Medretur** is the main target audience. Medretur has a policy to have a long-standing commitment to providing safe and effective waste management solutions to their customers [12]. However, the waste management industry is complex and challenging, and delivering a solution that reliably provides this is not easy. The proposed project seeks to help Medretur navigate this complex landscape by developing a new system that will improve the safety and security of their waste management operations. On a long term basis, there will be developed a system that will help to streamline the waste collection process, reduce the risk of human error, and ensure that all waste is managed in accordance with the current safety and regulatory standards.

By implementing this new system, Medretur will be able to reduce the risk of accidents, errors, and other safety incidents, which will help to protect their employees, customers, and the environment. Overall, the solution proposed by Medretur has the potential to provide significant benefits to Medretur and their customers.

II. BACKGROUND

This chapter presents the definition of the problem, scope of the problem, different solutions related to the problem and why this solution is chosen.

A. Definition of the problem

The problem is intrusion, but is what is intrusion? According to Merriam-Webster, an online English dictionary, intrusion is a noun and is defined in this context as:

“the act of intruding or the state of being intruded” [13]

especially:

“the act of wrongfully entering upon, seizing, or taking possession of the property of another” [13]

In the context of the MediColBox, intrusion refers to attempts to break into the collection system and gain access to the disposed medicines stored inside. The MediColBox contains medications that are expired or no longer needed, which can pose a danger to individuals if they are not disposed of properly [14].

The improper disposal of medications can lead to environmental contamination, harm to human health, and the potential for misuse.

The black market for medications also presents a criminal incentive to break into the collection system and steal the medications for resale. Additionally, there are individuals who may be addicted to certain medications and would seek to gain access to them for personal use.

Therefore, it is crucial to ensure that the MediColBox is secured and protected from intrusion attempts to prevent the tampering or theft of medications.

This requires the implementation of effective detection and deterrent measures to identify and stop intrusion attempts in real-time.

To intrude into the MediColBox in an attempt to get access to the medicines inside, it will be necessary to get through the outer metal shell. The metal shell, in this context, is a type of mechanical barrier, separating the outside from the inside.

Most types of intrusion attempts can be simplified to the contents of (Table I).

TABLE I
TYPES OF INTRUSION ATTEMPTS

Intrusion Attempt	Description
Cutting through the shell	This type of intrusion attempt involves using tools such as saws or angle grinders to physically cut through the outer metal shell of the MediColBox. It is a relatively straightforward method that can be quickly executed if the intruder has the necessary tools and equipment.
Forcing apart the shell	Forcing apart the shell refers to attempts to pry open or force the outer metal shell of the MediColBox using tools such as pry bars or similar implements. This method relies on applying excessive force to separate the components of the shell and gain unauthorized access.
Exploiting the shell	Intruders may attempt to unlock the shell using various exploits, such as lock picking tools, brute force attacks, or electronic hacking techniques. These methods involve manipulating the lock or electronic components of the shell's locking mechanism to gain access without proper authorization.

Cutting through or forcing apart the outer metal shell of the MediColBox are relevant intrusion attempts because they can potentially compromise the security of the contents inside, which are the expired or unused medications. Unauthorized access to these medications can pose a serious risk to public health and safety, as they may be misused, abused, or sold illegally.

Cutting through the shell can be done using power tools such as saws or angle grinders, while forcing apart the shell can be done using a pry bar or a similar tool. These methods of intrusion are relatively easy to carry out and can be completed quickly, especially if the intruder has the necessary tools and equipment.

To prevent cutting or forcing open the shell, physical barriers can be implemented. These can include tamper-proof screws or bolts, reinforced steel plates, or alarm systems. Tamper-proof screws or bolts can be used to secure the outer shell, making it difficult for intruders to unscrew or remove them. Reinforced steel plates can be placed over the shell to increase its strength and make it more difficult to cut or force apart. Alarm systems can be used to alert authorities and deter intruders from attempting to break into the MediColBox.

In addition to physical barriers, other security measures can be employed to prevent intrusion attempts. These can include access control systems such as key card readers or biometric scanners, security cameras to monitor the area around the MediColBox, and regular security patrols or checks.

It is important to note that no security measure is completely foolproof, and determined intruders may still be able to find ways to breach the security of the MediColBox. However, by implementing a combination of physical and electronic security measures, the risk of intrusion can be significantly reduced, and the contents of the MediColBox can be better protected.

Exploit-based intrusion attempts on the MediColBox could involve attempts to bypass or manipulate the locking mechanisms in order to gain unauthorized access to the contents inside. These exploit could include using lock picking tools, “brute force attacks”, or electronic hacking techniques.

Lock picking tools are designed to manipulate the internal workings of locks in order to unlock them without using the key. Brute force attacks involve attempting to force the lock by applying excessive force, such as hitting or kicking the lock or using a tool to pry it open. Electronic hacking techniques may involve attempting to manipulate the electronic components of the lock, such as by intercepting signals sent between the lock and its control system or by exploiting vulnerabilities in the lock’s firmware or software.

Exploit-based intrusion attempts are difficult to detect and prevent because they may not leave physical evidence and may not trigger alarms or other security measures. In addition, these types of attacks may be carried out by individuals with specialized knowledge or equipment, making them more difficult to defend against.

The potential consequences of an exploit-based intrusion attempt on the MediColBox could include unauthorized access to the expired or unused medications inside, which could lead to harm to individuals who consume or misuse them. In addition, successful exploitation of the MediColBox’s security measures could compromise the overall security of the system, potentially leading to further unauthorized access or theft of medications.

To prevent exploit-based intrusion attempts, it is important to implement strong physical and electronic security measures, as well as regular monitoring and maintenance of the security systems. This can include using tamper-proof locks and security cameras, implementing access control systems with strong authentication mechanisms, and regularly updating the firmware and software of the locking mechanisms to address any known vulnerabilities. It is also important to regularly review and update security policies and procedures to ensure that they are up-to-date and effective in addressing new threats and risks.

the last point in the list implies there is something unpredicted and unplanned, so this project will recommend this for future studies instead of covering it in this study.

the project will therefore focus on detecting and deterring cutting and forcing open the shell.

There are several detection and deterrence methods that can be used to prevent cutting and forcing open the shell of the MediColBox as specified (Table II).

Existing technologies that can be adapted for use in the MediColBox include tamper-proof screws or bolts, reinforced steel plates, alarm systems, motion sensors, video cameras, smart locks, and GPS tracking devices. These technologies can be integrated into the overall system by connecting them to a central control system or security platform, which can monitor and manage the various security measures in real-time.

Overall, by implementing a combination of physical and electronic security measures, the risk of cutting and forcing open the shell of the MediColBox can be significantly reduced, and the contents of the box can be better protected.

III. METHODOLOGY

In this section, the methodology for observing and analyzing intrusion attempts on the MediColBox will be outlined. A description of the phenomenon of interest, data collection methods, sampling strategy, data

TABLE II
POTENTIAL SECURITY MEASURES FOR MEDICOLBOX

Security Measure	Description
Physical Barriers	As mentioned earlier, physical barriers such as tamper-proof screws, reinforced steel plates, or alarm systems can be used to prevent unauthorized access to the MediColBox. These barriers can deter intruders from attempting to break into the box and can also alert authorities to any intrusion attempts.
Inertial Measurements	Utilizing an IMU in the sensor card to detect any changes in the box's orientation or movement, providing additional data for intrusion detection and prevention.
Motion Sensors	Motion sensors can be placed around the MediColBox to detect any movement or activity in the surrounding area. If an intruder attempts to cut or force open the shell, the motion sensors will detect their movement and trigger an alarm, alerting authorities to the intrusion attempt.
Video Surveillance	Video cameras can be installed around the MediColBox to monitor any activity in the surrounding area. The footage can be monitored in real-time by security personnel, who can alert authorities to any intrusion attempts.
Smart Locks	Smart locks can be used to secure the MediColBox, using electronic authentication mechanisms such as biometric scanners, keycard readers, or passwords. These locks can be integrated with other security measures, such as motion sensors or video surveillance, to provide additional layers of security.
GPS Tracking	GPS tracking technology can be used to monitor the location of the MediColBox and track any unauthorized movement or tampering. This can help to deter theft or unauthorized access to the box.

collection procedures, ethical considerations, data analysis approach, validity and reliability measures, and limitations of the study will be provided.

A. Phenomenon of Interest

The phenomenon of interest in this study is intrusion attempts on the MediColBox. The various aspects of intrusion, including the methods employed by intruders, their motivations behind the attempts, and the potential consequences of successful intrusions, will be investigated. By understanding these aspects, the project aims to enhance the security and protection of the MediColBox and the medications it contains.

B. Data Collection Methods

To collect data on intrusion attempts, the project will primarily utilize the Inertial Measurement Unit (IMU) as the main data collection method for detecting intrusion attempts on the MediColBox. This choice allows for a more focused investigation into the effectiveness of the IMU in identifying unauthorized access.

The IMU, with its capability to capture physical movements, vibrations, and orientation changes of the MediColBox, provides valuable data for intrusion detection and analysis. By relying on the IMU alone, the project aims to determine if it can effectively detect and alert on intrusion attempts without the need for additional systems.

This approach also enables the project to address the feasibility of implementing other data collection methods mentioned earlier, such as motion sensors, video surveillance, access logs, incident reports, and interviews. By evaluating the standalone performance of the IMU, the project can assess its potential to serve as a cost-effective and efficient solution for intrusion detection on the MediColBox.

The investigation will involve testing and analysis of the IMU data collected during simulated intrusion attempts. This evaluation will focus on assessing the accuracy, reliability, and timeliness of the IMU in detecting and alerting on unauthorized movements or tampering.

By dedicating the study to evaluating the IMU's effectiveness as a standalone solution, the project aims to determine if the implementation of additional data collection methods is necessary for robust intrusion

detection. The results will provide insights into the suitability and viability of relying solely on the IMU for enhancing the security and protection of the MediColBox and its contents.

(Table III) presents potential data collection methods for intrusion attempts.

TABLE III
POTENTIAL DATA COLLECTION METHODS FOR INTRUSION ATTEMPTS

Data Collection Method	Description
Motion Sensors	Implementing motion sensors that can detect unauthorized movements near the MediColBox.
Inertial Measurements (IMU)	Utilizing an Inertial Measurement Unit (IMU) to detect any changes in the orientation or movement of the MediColBox, providing data for intrusion detection and analysis.
Video Surveillance	Installing surveillance cameras around the MediColBox to capture intrusion attempts visually.
Access Logs	Maintaining detailed logs of access attempts and recording any suspicious activities.
Incident Reports	Gathering information from incident reports filed by security personnel or individuals who have witnessed intrusion attempts.
Interviews	Conducting interviews with security personnel to gain insights into their experiences and observations regarding intrusion attempts.

The IMU, with its capability to capture physical movements, vibrations, and orientation changes of the MediColBox, provides valuable data for intrusion detection and analysis. By relying on the IMU alone, the project aims to determine if it can effectively detect and alert on intrusion attempts without the need for additional systems.

This approach also enables the project to address the feasibility of implementing the other data collection methods mentioned earlier, such as motion sensors, video surveillance, access logs, incident reports, and interviews. By evaluating the standalone performance of the IMU, the project can assess its potential to serve as a cost-effective and efficient solution for intrusion detection on the MediColBox.

The investigation will involve comprehensive testing and analysis of the IMU data collected during simulated intrusion attempts. This evaluation will focus on assessing the accuracy, reliability, and timeliness of the IMU in detecting and alerting on unauthorized movements or tampering.

By dedicating the study to evaluating the IMU's effectiveness as a standalone solution, the project aims to determine if the implementation of additional data collection methods is necessary for robust intrusion detection. The results will provide insights into the suitability and viability of relying solely on the IMU for enhancing the security and protection of the MediColBox and its contents.

C. Prototype Construction

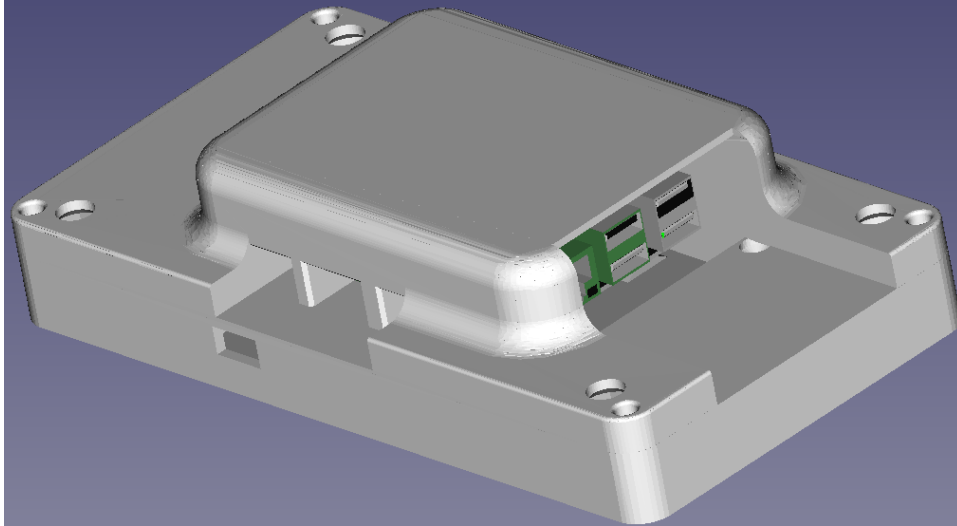


Fig. 1. Design of the prototype with the cover on

The prototype control system is constructed using the following components:

- 1× Single-board computer: Raspberry Pi 4B 8 GB [9] as the CCU
- 1× Human-Machine Interface (HMI): 7-inch touchscreen [10]
- 1× Sensor Card: Raspberry Pi Sense Hat v1.0.0 [11] with an integrated IMU
- 4× M3 8 mm long threaded screws
- 8× M3 8 mm long spacers with 8 mm threaded rods on one side
- 1× 22-pin 0.5 mm pitch cable for the DSI connectors
- 1× USB type A to USB type micro B cable for power and GND between HMI and Raspberry Pi
- 1× USB type A to USB type C cable for power
- 1× 230 V AC to USB type A power adapter
- 1× Custom-designed cover to protect the electronics during testing
- 4× M3.5 8 mm long screws
- 4× M4 10 mm long screws

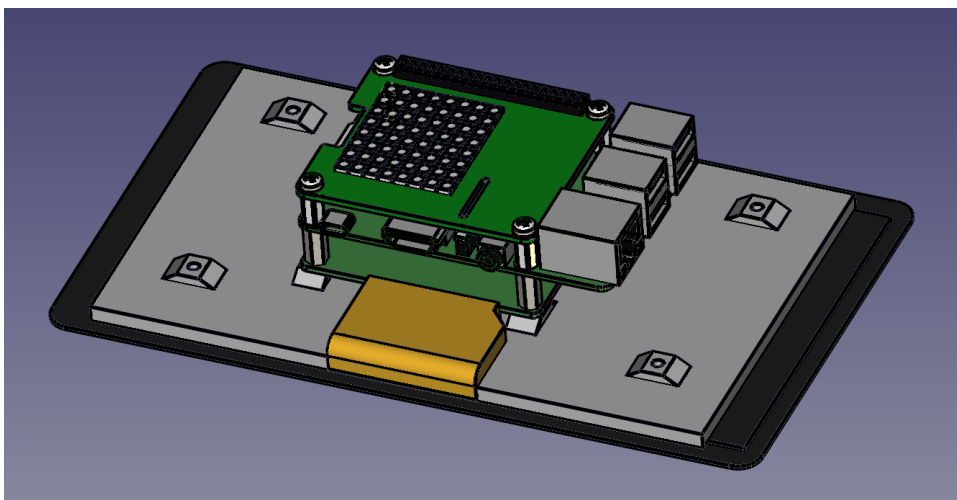


Fig. 2. Design of the prototype without the cover

The construction process involves the following steps:

- 1) Assemble the prototype:
 - a) Mount the Raspberry Pi 4B on the 7-inch touchscreen by using the threaded spacers.
 - b) Mount the Raspberry Pi Sense Hat on the Raspberry Pi 4B by attaching it to the 2×20 pin.
- 2) Connect the components according to the wiring diagram (Figure 3):
 - a) Connect the DSI output from the Raspberry Pi to the DSI input on the 7-inch touchscreen using a suitable ribbon cable.
 - b) Connect the display's USB type micro B power connector input to one of the USB type A connectors on the Raspberry Pi (it does not matter which one).
- 3) Enclose the electronics with the custom-designed cover.
 - a) Attach the screen to the first part of the casing using the M3.5 screws.
 - b) Attach the second part of the casing to the first part of the casing using the M4 screws.
- 4) Configure the software environment for the Raspberry Pi 4B and install the necessary libraries and drivers.
 - a) Open Raspberry Pi Imager. Install it if you don't already have.
 - b) Insert the micro SD card into your computer. You can use an adapter if needed.
 - c) On Raspberry Pi Imager, select the storage device to install the operating system. Select the micro SD card.
 - d) On Raspberry Pi Imager, select operating system to install. Select Raspberry Pi OS.
 - e) Click "write" and wait till complete.
 - f) Remove the micro SD card and insert it into the Raspberry Pi.
 - g) start the Raspberry Pi, open terminal and type the code:


```
sudo raspi-config
```
 - h) Select "Interfacing Options"
 - i) Select the "I2C" option
 - j) Select "<Yes>"
 - k) Select "<Ok>"
 - l) Select "<Yes>"
- 5) Establish communication between the CCU, HMI, and the sensor card by setting up appropriate interfaces and protocols.
 - a) implement software that follows this sequence (Figure 4)

D. Sampling Strategy

For our study, we define a sampling strategy to ensure the representation of different scenarios and potential risks associated with intrusion attempts on the MediColBox. Our sample may include specific locations where the MediColBox is deployed, instances of reported intrusion attempts, or a combination of both. We strive to select a diverse sample that covers a range of demographic and environmental factors to enhance the generalizability of our findings.

E. Data Collection Procedures

To collect data on intrusion attempts, we follow specific procedures to ensure accuracy and completeness. These procedures involve implementing the following data collection methods (Table IV):

These procedures help us capture the necessary data for analysis and provide a comprehensive understanding of intrusion attempts on the MediColBox.

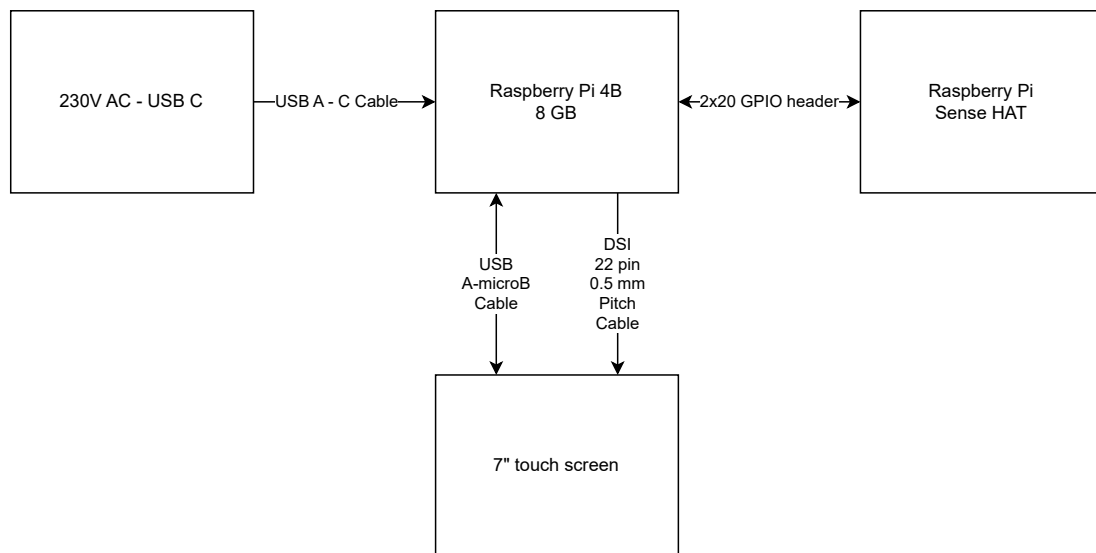


Fig. 3. The “wiring diagram” used

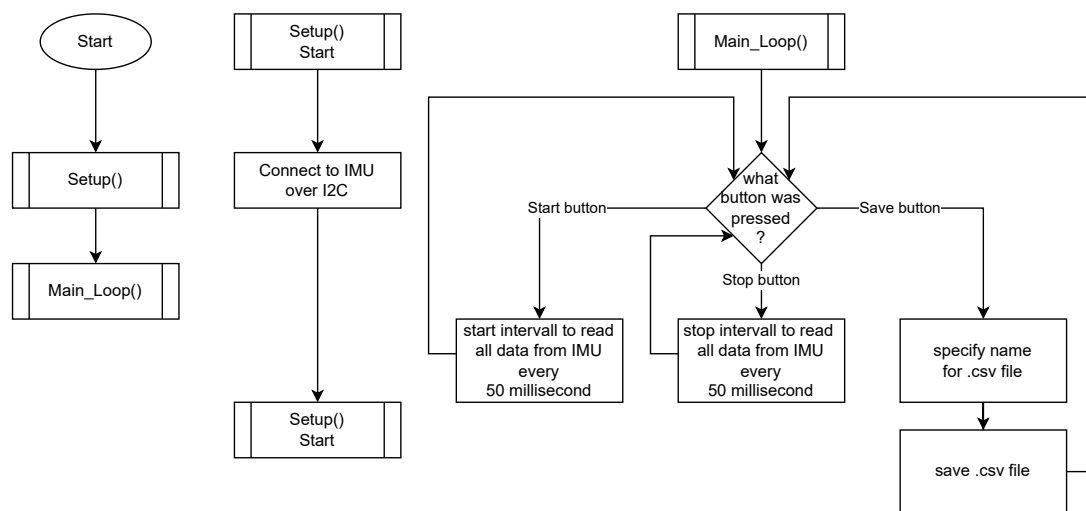


Fig. 4. The Sequence diagram used for the program

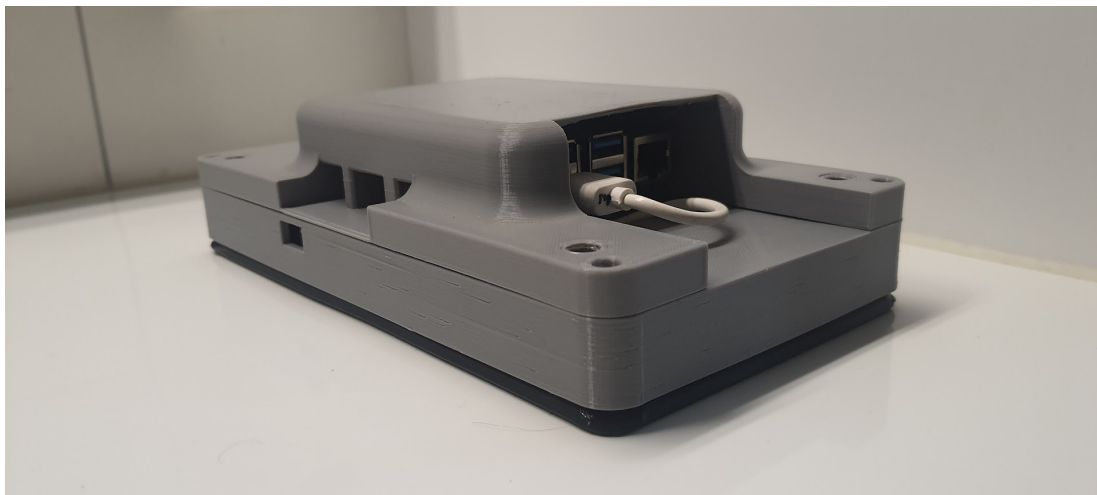


Fig. 5. Photograph of the prototype

TABLE IV
POSSIBLE DATA COLLECTION METHODS FOR INTRUSION ATTEMPTS

Data Collection Method	Description
Installing Surveillance Cameras and Motion Sensors	Installing surveillance cameras and motion sensors at strategic locations around the MediColBox.
Implementing Protocols for Incident Documentation	Implementing protocols for documenting and reporting intrusion incidents, including recording timestamps, descriptions of the events, and any available contextual information.
Reviewing Video Footage, Access Logs, and Incident Reports	Regularly reviewing video footage, access logs, incident reports, and conducting interviews to gather relevant data.
Ensuring Equipment Functionality and Maintenance	Ensuring the proper functioning and maintenance of surveillance equipment and data storage systems.

F. Ethical Considerations

We recognize and address ethical considerations related to our study. This includes:

- Adhering to relevant data protection regulations and guidelines.
- Anonymizing data during the analysis phase to protect the identities of individuals involved.

By considering these ethical considerations, we aim to conduct our study with integrity and respect for individuals' privacy.

G. Data Analysis

The collected data from the IMU is analyzed using a systematic approach. Since there is no video footage or access logs available, our analysis focuses solely on the data captured by the IMU. The analysis process includes the following steps:

- Data preprocessing: The collected IMU data is preprocessed to ensure its quality and suitability for analysis. This may involve removing any noise or outliers, normalizing the data, and performing any necessary transformations to prepare it for further analysis.
- Exploratory data analysis: We conduct exploratory data analysis to gain a better understanding of the IMU data. This involves visualizing the data, examining summary statistics, and identifying any patterns or trends that may be present. Exploratory analysis helps in identifying initial insights and forming hypotheses for further investigation.
- intrusion detection algorithm: We develop or utilize an intrusion detection algorithm that can process the IMU data and identify potential intrusion attempts. This algorithm is trained and validated using a suitable methodology to ensure its effectiveness in detecting unauthorized access based on the IMU readings.
- Statistical analysis: If applicable, statistical analysis techniques can be employed to analyze the IMU data further. This may include identifying correlations between different variables or conducting hypothesis testing to validate any observed patterns or relationships.
- Data visualization: Data visualization techniques, such as plots, charts, or graphs, can be employed to present the analyzed IMU data effectively. Visualizations can help in understanding the patterns, trends, and anomalies in the data, making it easier to interpret and communicate the findings.

By conducting an analysis of the anonymized IMU data, we aim to gain insights into the effectiveness of the IMU in detecting intrusion attempts on the MediColBox. This analysis will contribute to the assessment of the IMU as a standalone solution for enhancing the security and protection of the MediColBox and its contents.

H. Limitations

It is essential to acknowledge the limitations inherent in studying intrusion attempts on the MediColBox. These limitations may include:

- **Availability of intrusion data:** The limited availability of documented intrusion attempts may impact the sample size and the generalizability of the findings.
- **Challenges in capturing all intrusion attempts:** Some intrusion attempts may go undetected or unreported, leading to potential underrepresentation in the collected data.
- **Generalizability of findings:** The context of the MediColBox and the specific locations where it is deployed may influence the generalizability of the findings to other similar systems.

We address these limitations by maximizing the available data, selecting a diverse sample, and providing contextual information to aid in the interpretation and application of our findings.

By incorporating these elaborations into the methodology section, we can effectively observe and analyze intrusion attempts on the MediColBox, gaining insights into the methods, motivations, and potential vulnerabilities associated with these attempts.

I. Tools and Technologies

During the course of this study, the following tools and technologies were utilized:

- **LaTeX:** LaTeX, a typesetting system widely used in academia and scientific research, was used for document preparation. It provided powerful tools for creating professional-looking documents, including support for mathematical equations, figures, tables, and bibliographic references.
- **Visual Studio Code (VSCode):** VSCode, a versatile text editor, served as the primary tool for writing code, editing documents, and managing project files. It provided a user-friendly interface, syntax highlighting, code completion, and integration with version control systems like Git.
- **FreeCAD:** FreeCAD, an open-source computer-aided design (CAD) software, was utilized for designing and creating 3D models of the prototype. It enabled precise modeling and visualization of the physical components, ensuring accurate representation and construction.
- **GitHub:** GitHub, an open-source web-based platform for version control and collaboration, was used to track changes, collaborate with team members, and maintain the integrity and availability of project files. It provided a centralized repository for source code and project documentation.
- **Programming Languages:** The primary programming languages used in this study were Python and JavaScript. Python, an open-source language, was employed for data analysis, algorithm development, and system control, while JavaScript, also open-source, was utilized for web development and implementing the human-machine interface (HMI) functionality.
- **Electron:** Electron, an open-source framework for building cross-platform desktop applications, was utilized for developing the HMI. It enabled the integration of open-source web technologies (HTML, CSS, and JavaScript) into a standalone application, providing a responsive and user-friendly interface.

These open-source tools and technologies played a crucial role in streamlining the research process, facilitating data analysis, and developing a functional prototype that aligns with the research objectives. By prioritizing open-source solutions, the study fostered collaboration, transparency, and accessibility, promoting the advancement of knowledge and encouraging community contributions.

J. Document Preparation

The document was prepared using LaTeX, an open-source typesetting system widely used in academia and scientific research. LaTeX provided powerful tools for creating professional-looking documents, including support for mathematical equations, figures, tables, and bibliographic references.

To facilitate the writing process, Visual Studio Code (VSCode), an open-source text editor, was utilized as the primary tool. VSCode offered a range of features and extensions that enhanced productivity and provided a seamless writing experience. It enabled efficient collaboration, syntax highlighting, code completion, and integration with version control, ensuring the integrity and consistency of the document.

By leveraging open-source tools like LaTeX and VSCode, the study embraced the principles of openness, collaboration, and knowledge sharing, fostering innovation and contributing to the open-source community.

IV. RESULTS

The results' section presents the findings from the analysis of the accelerometer data collected during the simulated intrusion attempts on the MediColbox. The accelerometer data provides insights into the physical movements and vibrations experienced by the MediColbox during these intrusion scenarios.

A. Analysis of Accelerometer Data

The accelerometer data captured the acceleration patterns resulting from different simulated intrusion attempts, including striking, dropping, sawing, and shaking the MediColbox. The data analysis focused specifically on the accelerometer readings to evaluate the sensitivity and effectiveness of the IMU in detecting unauthorized access.

1) *Striking the MediColbox*: Figure 6 presents the accelerometer data recorded when the MediColbox was struck with a fist. The accelerometer readings showed a sharp increase in acceleration followed by a swift, but gradual decrease as the impact dissipated. The peak acceleration value reached during the strike was measured at $X = 5[m/s^2]$, $Y = -31[m/s^2]$, $Z = -55[m/s^2]$ and occurred at $t = 0.8[s]$. The analysis of the data indicates that the IMU successfully detected and recorded the impact caused by the striking event.

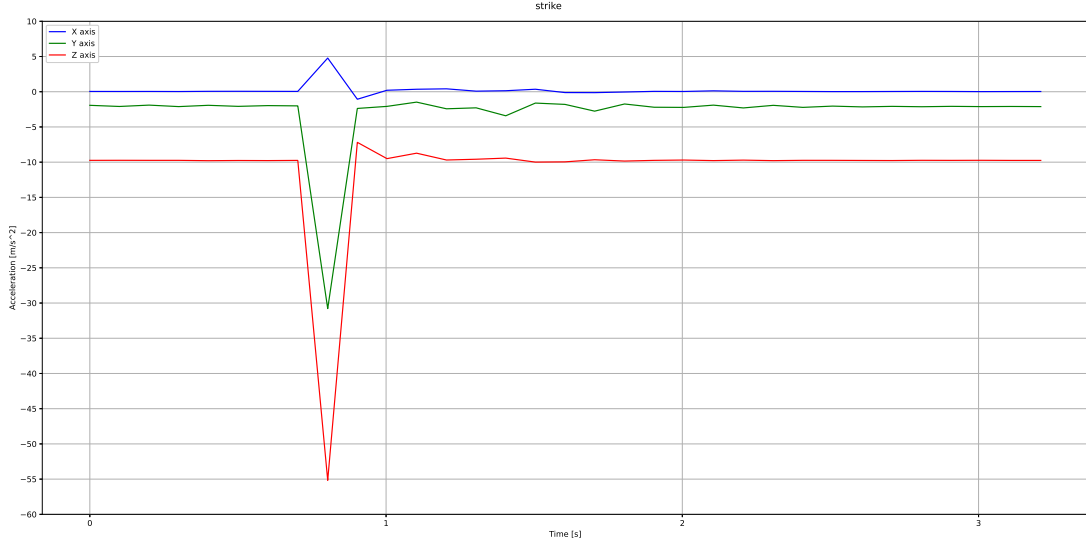


Fig. 6. Accelerometer data during the striking event

Looking at the data we can clearly see the peak acceleration and how it stands out from the rest of the data visualized. However, how do we set criteria so that we can automatically claim an acceleration like this is an attempt of intrusion and not just a random event? A way we, during the data gathering, could reason for, was to find the force needed to break the box and estimate from the weight of the box how much acceleration would be close to breaking the box open. In this case the data gathering "Prototype" is $0.645[kg]$. With the measured acceleration in X , Y and Z direction results in a combined acceleration of $|\vec{a}| = \sqrt{5^2 + (-32)^2 + (-55)^2}[m/s^2] \approx 63.332[m/s^2]$. If a box is designed to handle an impact large enough to momentarily expose it to $63.332[m/s^2]$ multiplied by a given safety factor, then it would be viable to account for sensor error margins and say that any acceleration above $60[m/s^2]$ should immediately trigger an alarm.

Another method could be to assume that if somebody wanted to break the box, they would either break the box in one strike, or try to hit the box repeatedly with strikes that individually might not break the box but that combined might manage to break the box due to material fatigue. If we divide the strike force that would immediately trigger an alarm (in this case $60[m/s^2]$), by the estimated resistance to fatigue in a scale from 0 to 1 and raise it to the number of strikes you assume you would need to break the box using the assumed amount of needed repeated strikes. An example of this could be to do the calculation:

$$a_{trigger} * \rho_{fatigue}^{n_{strikes}} \rightarrow 60[m/s^2] * 0.9^5 \approx 35.43[m/s^2]$$

In this example then 5 repeated strikes of approximately $35.43[m/s^2]$ will also trigger an alarm.

If we continue to analyze the data, we can try using frequency analysis on the striking event hoping to find information not revealed by just graphing the data. One way to find the frequency values of the data to analyze is using Fourier analysis. Herein this figure 7. The Fourier analysis reveals to us the frequency

components present in the accelerometer readings. This could provide insights into the characteristics of the impact and resulting vibrations.

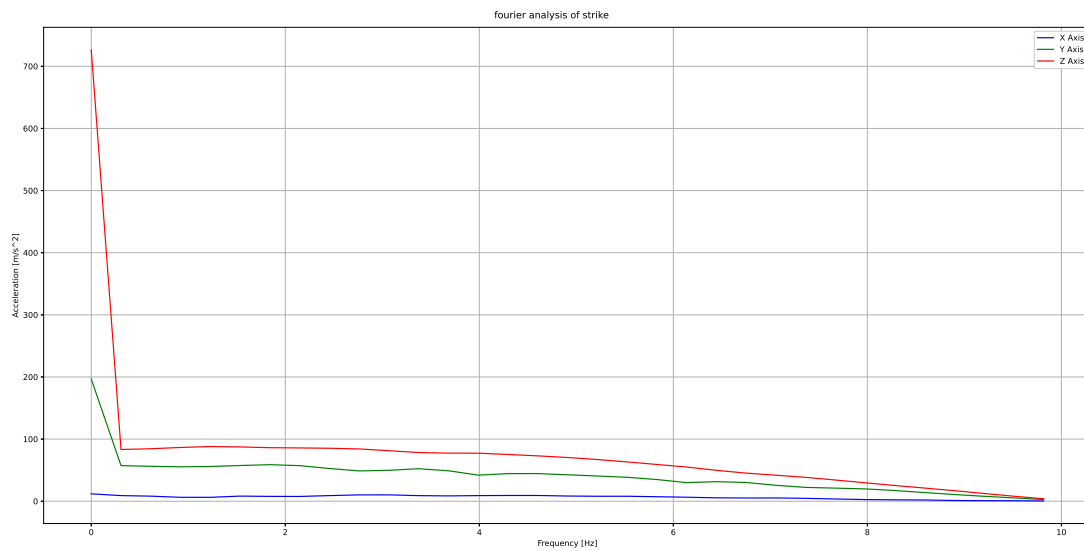


Fig. 7. Fourier analysis of accelerometer data during the striking event

Looking at the Fourier transformed data no additional information could be extrapolated from the data, that wasn't already discussed from the untransformed data.

2) *Dropping the MediColbox*: The accelerometer data collected when the MediColbox was dropped from a table is presented in Figure 8. The data showed a sudden increase in acceleration when the MediColbox was released, followed by a deceleration as it came into contact with the surface. The maximum acceleration value recorded during the drop was $X = -7.7[m/s^2]$, $Y = 35[m/s^2]$, $Z = -50.7[m/s^2]$, which occurred at $t = 5.1[s]$. The analysis confirms that the IMU effectively captured the acceleration changes associated with the dropping event.

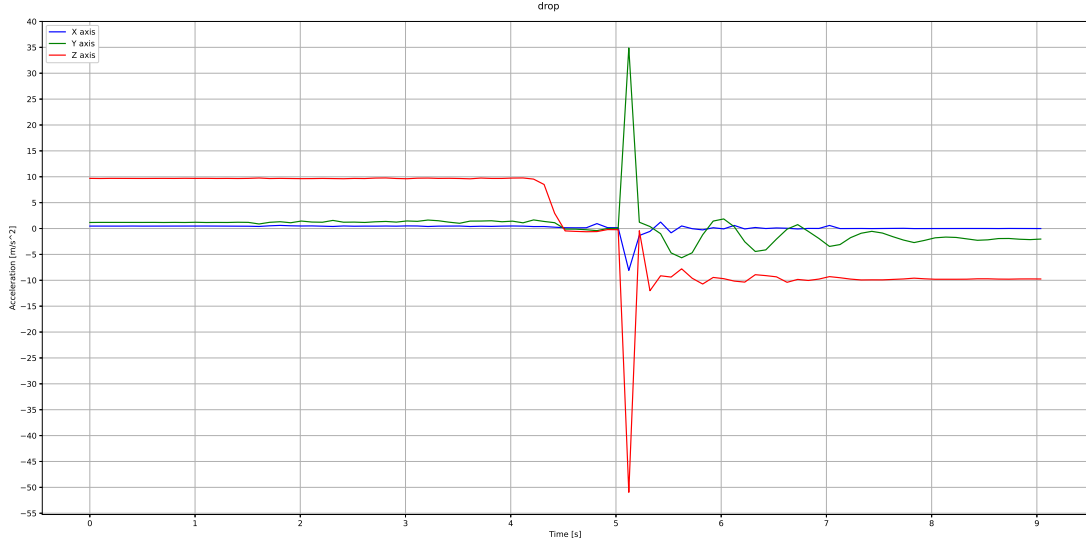


Fig. 8. Accelerometer data during the dropping event

analyzing the data similarly to how we did at the striking event we find that in this case we have a total peak acceleration of $|\vec{a}| \approx 62[m/s^2]$

The Fourier analysis of the accelerometer data during the dropping event is shown in Figure 9. The Fourier analysis allows us to examine the frequency components present in the accelerometer readings and provides insights into the characteristics of the drop and resulting vibrations.

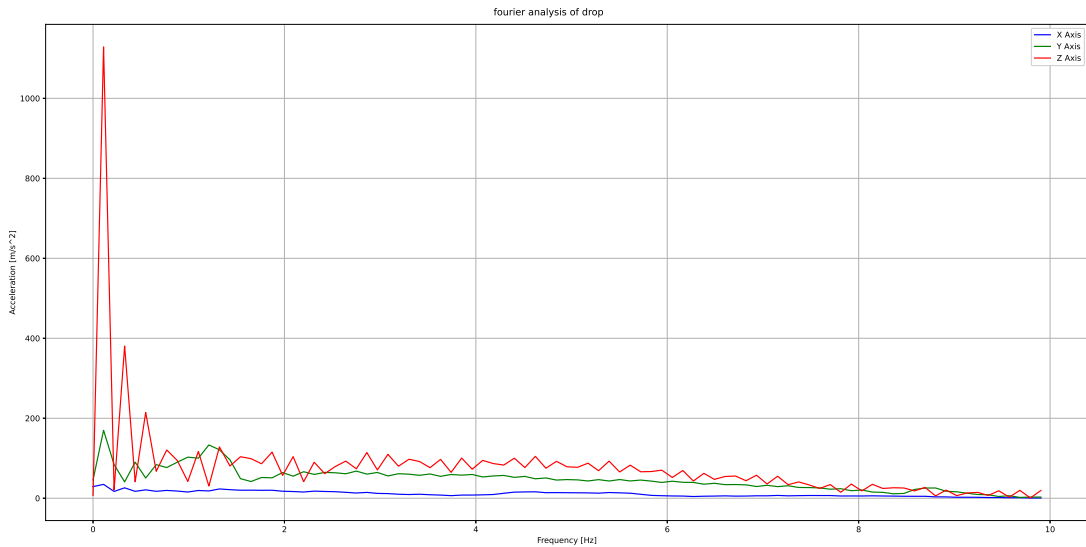


Fig. 9. Fourier analysis of accelerometer data during the dropping event

3) *Sawing on the MediColbox:* Figure 10 illustrates the accelerometer data recorded while sawing on the MediColbox using a metal cutting saw. The data exhibited periodic variations in acceleration corresponding to the back-and-forth sawing motion. The analysis of the data indicated a consistent pattern of acceleration changes during the sawing event. This suggests that the IMU was able to capture the vibrations and oscillations caused by the sawing action.

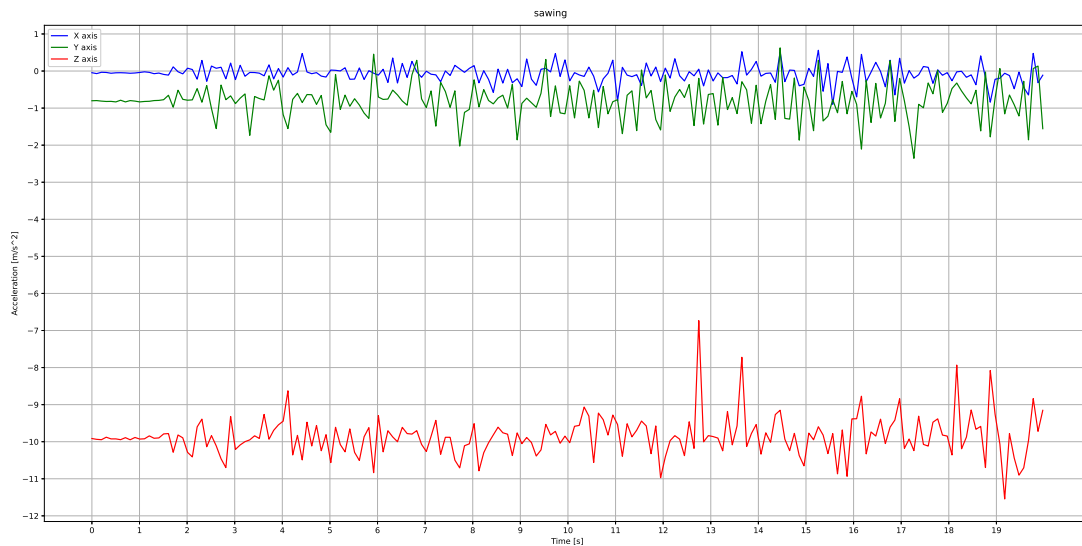


Fig. 10. Accelerometer data during the sawing event

The Fourier analysis of the accelerometer data during the sawing event is shown in Figure 11. The Fourier analysis allows us to examine the frequency components present in the accelerometer readings and provides insights into the characteristics of the sawing action. By analyzing the frequency distribution and identifying prominent peaks or patterns in the frequency domain, we can gain a deeper understanding of the dynamic response of the MediColbox to the sawing forces.

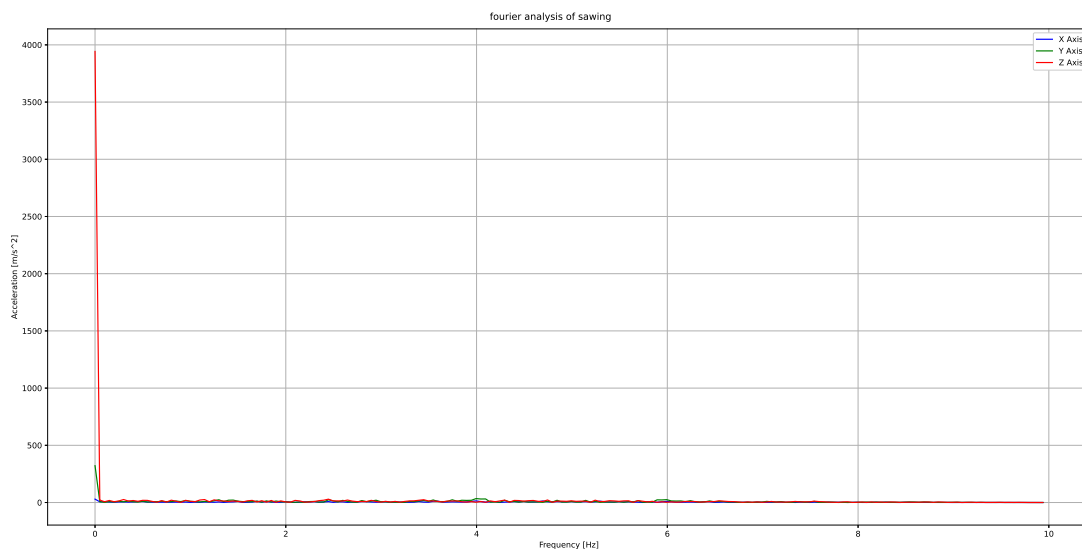


Fig. 11. Fourier analysis of accelerometer data during the sawing event

4) *Shaking the MediColbox:* The accelerometer data obtained while shaking the MediColbox on a sifter, simulating cutting it with an angle grinder, is presented in Figure 12. The data exhibited irregular and rapid fluctuations in acceleration due to the shaking motion. The analysis of the data demonstrated that the IMU was sensitive enough to detect and record these rapid changes in acceleration, indicating its potential for detecting unauthorized access attempts involving similar movements.

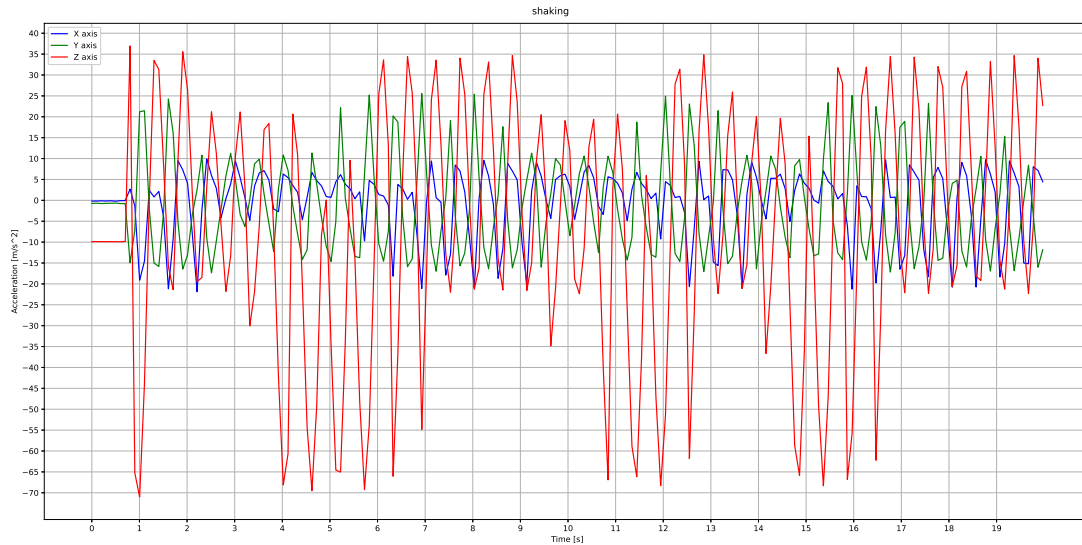


Fig. 12. Accelerometer data during the shaking event

The Fourier analysis of the accelerometer data during the shaking event is shown in Figure 13. The Fourier analysis allows us to examine the frequency components present in the accelerometer readings and provides insights into the characteristics of the shaking motion. By analyzing the frequency distribution and identifying prominent peaks or patterns in the frequency domain, we can gain a deeper understanding of the dynamic response of the MediColbox to the shaking forces.

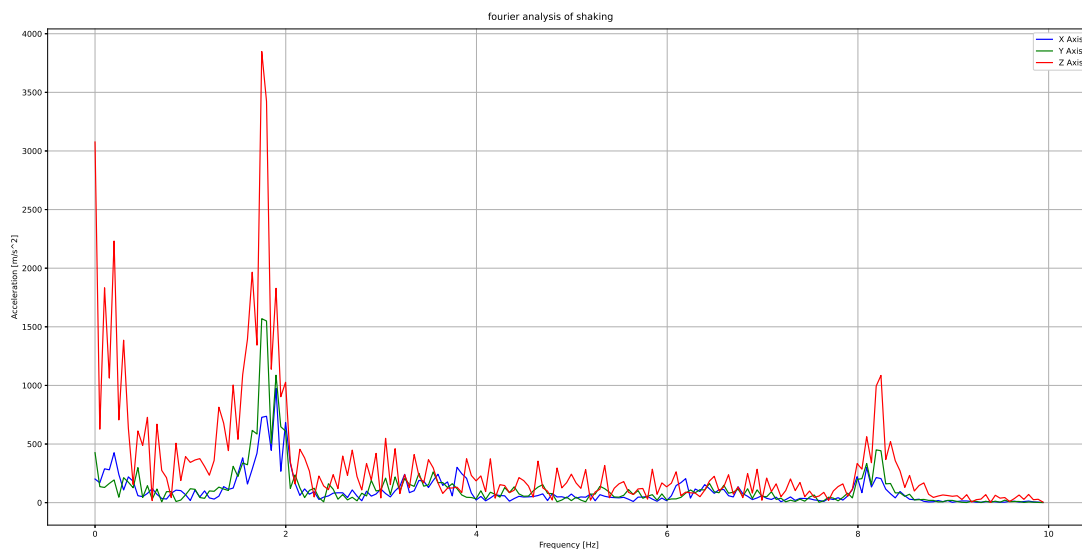


Fig. 13. Fourier analysis of accelerometer data during the shaking event

B. Discussion of Findings

The analysis of the accelerometer data during the simulated intrusion attempts provides valuable insights into the IMU's ability to detect and capture unauthorized access events. The results demonstrate that the accelerometer readings accurately captured the accelerative patterns associated with striking, dropping, sawing, and shaking the MediColbox.

The findings suggest that the IMU is a reliable and effective sensor for detecting physical movements and vibrations, which are indicative of intrusion attempts. The accelerometer data recorded during the simulated scenarios showcased the IMU's sensitivity to changes in acceleration, enabling it to capture both high-impact events and subtle vibrations.

However, it is important to note that the analysis focused solely on the accelerometer data, and other data collected by the IMU, such as gyroscope or magnetometer readings, were not considered in this study. Further research could explore the integration of multiple sensor data to enhance the accuracy and robustness of intrusion detection.

Overall, the results indicate the potential of the IMU as a standalone solution for intrusion detection on the MediColbox. The findings support the feasibility of utilizing the IMU to enhance the security and protection of the MediColbox by effectively detecting and alerting on unauthorized access attempts.

V. CONCLUSION

The analysis of the accelerometer data during the simulated intrusion attempts on the MediColbox revealed several key findings. Firstly, the IMU demonstrated remarkable sensitivity to changes in acceleration, successfully capturing both high-impact events and subtle vibrations. The accelerometer readings accurately detected the accelerative patterns associated with striking, dropping, sawing, and shaking the MediColbox, indicating the effectiveness of the IMU in detecting and capturing different intrusion scenarios.

However, it was observed that the IMU's high sensitivity also led to the detection of movements from nearby individuals, which may result in false alarms. To address this limitation, further research is recommended to explore the implementation of pattern recognition software, such as machine learning algorithms, to filter out false alarms and improve the accuracy of intrusion detection.

Additionally, the analysis highlighted the potential of combining the accelerometer data with other sensor types, such as gyroscope data, to gain a comprehensive understanding of both acceleration and orientation during intrusion events. This integration could enhance the overall security and integrity of the MediColbox system by providing a more holistic approach to intrusion detection.

The feasibility of utilizing the IMU as a standalone solution for enhancing the security and protection of the MediColbox is strongly supported by the study's findings. However, it is important to address the challenges associated with false alarms and explore the potential of integrating multiple sensor types to further improve the intrusion detection capabilities.

The implications of this study's findings extend beyond the MediColbox system. The successful application of the IMU in detecting intrusion attempts suggests its potential use in other portable storage systems or similar applications that require intrusion prevention. Future research should investigate the adaptability of this intrusion detection approach to different contexts and explore its broader implications.

In conclusion, the analysis of the accelerometer data during the simulated intrusion attempts provides valuable insights into the effectiveness of the IMU in detecting unauthorized access. The study lays the foundation for further research in the field of intrusion detection, including the development of more advanced algorithms and the exploration of potential applications beyond the MediColbox system. By improving the security and integrity of portable storage systems, these findings contribute to the protection of sensitive information and resources.

REFERENCES

- [1] D. C. Throckmorton, “Fda stresses critical importance of safe disposal of medications,” *U.S. Food and Drug Administration*, Apr 2021. [Online]. Available: <https://www.fda.gov/news-events/fda-voices/fda-stresses-critical-importance-safe-disposal-medications-ahead-national-prescription-drug-take>
- [2] A. B. Boxall, “The environmental side effects of medication,” *EMBO reports*, Dec 2004. [Online]. Available: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1299201/>
- [3] OECD, *Management of Pharmaceutical Household Waste*, 2022. [Online]. Available: <https://www.oecd-ilibrary.org/content/publication/3854026c-en>
- [4] *Apotek 1*, Jan 2023. [Online]. Available: <https://www.apotek1.no/bruk-av-legemidler/retur-og-destruksjon-av-legemidler>
- [5] O. o. t. Commissioner, “Whereand how to dispose of unused medicines,” *U.S. Food and Drug Administration*, Apr 2021. [Online]. Available: <https://www.fda.gov/consumers/consumer-updates/where-and-how-dispose-unused-medicines>
- [6] *Helsenorge*, Sep 2019. [Online]. Available: <https://www.helsenorge.no/medisiner/medisiner-holdbarhet-og-oppbevaring/>
- [7] A. Lutro, “Medisintyveri kan ende i tragedie,” *Nettavisen*, Nov 2005. [Online]. Available: <https://www.nettavisen.no/artikkel/medisintyveri-kan-ende-i-tragedie/s/12-95-495291>
- [8] U. Nations, “Drug trafficking,” *United Nations : Office on Drugs and Crime*, May 2023. [Online]. Available: <https://www.unodc.org/unodc/en/drug-trafficking/index.html>
- [9] R. Pi, “Buy a raspberry pi 4 model b,” *Raspberry Pi*. [Online]. Available: <https://www.raspberrypi.com/products/raspberry-pi-4-model-b/?variant=raspberry-pi-4-model-b-8gb>
- [10] —, “Buy a raspberry pi touch display,” *Raspberry Pi*. [Online]. Available: <https://www.raspberrypi.com/products/raspberry-pi-touch-display/>
- [11] —, “Buy a sense hat,” *Raspberry Pi*. [Online]. Available: <https://www.raspberrypi.com/products/sense-hat/>
- [12] M. AS, “Vår visjon,” *Medretur*. [Online]. Available: <https://www.medretur.no/vår-visjon>
- [13] “Intrusion definition and meaning,” *Merriam-Webster*. [Online]. Available: <https://www.merriam-webster.com/dictionary/intrusion>
- [14] M. C. Lovegrove, N. J. Weidle, and D. S. Budnitz, “Trends in Emergency Department Visits for Unsupervised Pediatric Medication Exposures, 2004–2013,” *Pediatrics*, vol. 136, no. 4, pp. e821–e829, 10 2015. [Online]. Available: <https://doi.org/10.1542/peds.2015-2092>