# Software Requirements Specification

# for

# Multimodal Cyberattack

# Detection and

# Classification System

Version 1.0

Prepared by Ishan Surana, Divej Ahuja, Udai Pratap, Piyush Rangdal

Manipal Institute of Technology, Manipal

6th October 2024

Table of Contents

[1. Introduction 1](#_Toc179152841)

[1.1 Purpose 1](#_Toc179152842)

[1.2 Document Conventions 1](#_Toc179152844)

[1.3 Intended Audience and Reading Suggestions 1](#_Toc179152845)

[1.4 Product Scope 1](#_Toc179152846)

[1.5 References 2](#_Toc179152847)

[2. Overall Description 2](#_Toc179152848)

[2.1 Product Perspective 2](#_Toc179152849)

[2.2 Product Functions 2](#_Toc179152850)

[2.3 User Classes and Characteristics 2](#_Toc179152851)

[2.4 Operating Environment 2](#_Toc179152852)

[2.5 Design and Implementation Constraints 2](#_Toc179152853)

[2.6 User Documentation 3](#_Toc179152854)

[2.7 Assumptions and Dependencies 3](#_Toc179152855)

[3. External Interface Requirements 3](#_Toc179152856)

[3.1 User Interfaces 3](#_Toc179152857)

[3.2 Hardware Interfaces 3](#_Toc179152858)

[3.3 Software Interfaces 3](#_Toc179152859)

[3.4 Communications Interfaces 3](#_Toc179152860)

[4. System Features 4](#_Toc179152861)

[4.1 Multimodal Data Collection 4](#_Toc179152862)

[4.2 Cyberattack Detection 4](#_Toc179152863)

[5. Other Nonfunctional Requirements 4](#_Toc179152864)

[5.1 Performance Requirements 4](#_Toc179152865)

[5.2 Safety Requirements 4](#_Toc179152866)

[5.3 Security Requirements 5](#_Toc179152867)

[5.4 Software Quality Attributes 5](#_Toc179152868)

[5.5 Business Rules 5](#_Toc179152869)

[6. Other Requirements 5](#_Toc179152870)

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Date** | **Reason For Changes** | **Version** |
|  |  |  |  |
|  |  |  |  |

# Introduction

## Purpose

This Software Requirements Specification (SRS) document outlines the requirements for the Multimodal Cyberattack Detection and Classification System (Version 1.0). The product aims to detect and classify cyberattacks through the integration of various data modalities, decentralized federated learning, blockchain technology, and feedback mechanisms for continuous improvement. This SRS covers the entire system, focusing on the multimodal detection model, federated learning framework, blockchain integration, and centralized analysis and coordination components.

## Document Conventions

The document follows the conventions of specifying requirements as clear and unambiguous statements. Requirements are prioritized as High, Medium, or Low, with a unique identifier assigned to each. Higher-level requirements are assumed to be inherited by detailed requirements unless otherwise specified.

## Intended Audience and Reading Suggestions

This document is intended for various stakeholders:

* **Developers**: Technical details on system architecture and requirements.
* **Project Managers**: Overview of project scope and objectives.
* **Marketing Staff**: Understanding of product features and benefits.
* **Users and Testers**: Insight into system functionality and user interactions.
* **Documentation Writers**: Guidelines for user manuals and help documentation.

It is recommended to start with the overview sections and then proceed to sections relevant to each stakeholder’s role.

## Product Scope

The Multimodal Cyberattack Detection and Classification System serves to enhance cybersecurity measures by detecting and classifying various types of cyberattacks using real-time data collection and advanced machine learning techniques. Its goals include improved detection accuracy, data privacy through federated learning, and secure result storage on the blockchain, aligning with corporate strategies of adopting cutting-edge cybersecurity technologies.

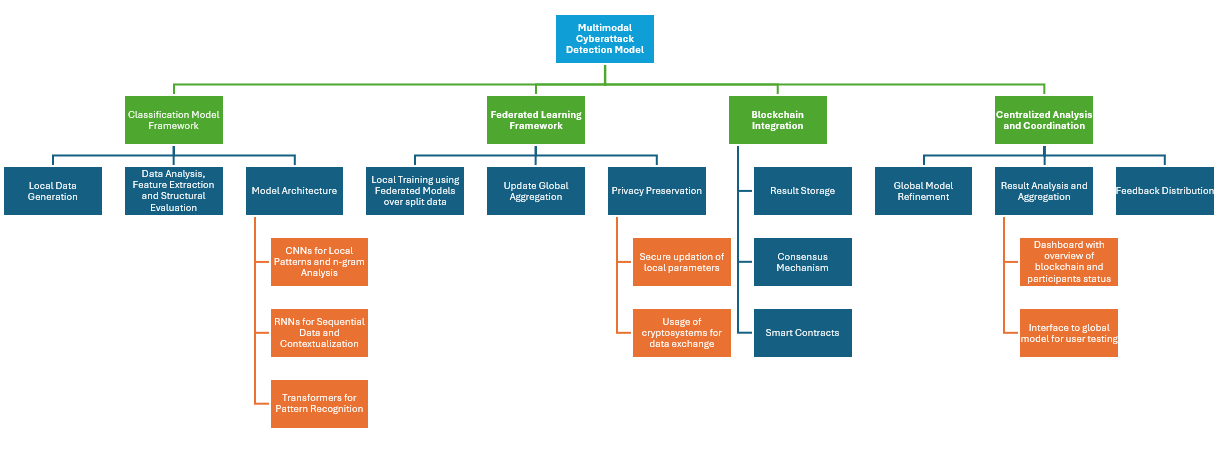
## References

https://www.mdpi.com/2504-4990/5/3/58#B27-make-05-00058

# Overall Description

## Product Perspective

This system is a self-contained product that builds upon existing cybersecurity technologies and integrates novel approaches like federated learning and blockchain. It will interface with various hardware devices for data collection and communicate with a central server for model updates. The following diagram illustrates the system's major components and their interconnections.



## Product Functions

The product will perform the following key functions:

* Local data collection for model training.
* Cyberattack detection and classification using deep learning models.
* Federated learning for decentralized model training and updates.
* Blockchain storage of model updates and metadata.
* Centralized analysis of aggregated results for model refinement.

## User Classes and Characteristics

* **Security Analysts**: High technical expertise; require detailed analysis and reporting features.
* **Developers**: Medium technical expertise; need access to system APIs and technical documentation.
* **End Users**: Low technical expertise; require a simple interface for viewing detected threats.

## Operating Environment

The software will operate on a variety of hardware platforms, including personal computers and servers, and will be compatible with Linux and Windows operating systems. The system will also interface with various data sources and APIs for real-time data collection.

## Design and Implementation Constraints

The project must adhere to corporate security policies and privacy regulations (e.g., GDPR). The use of specific technologies such as TensorFlow for machine learning and Ethereum for blockchain implementation will also guide design choices. Hardware constraints include ensuring compatibility with IoT devices for data collection.

## User Documentation

User manuals, online help, and tutorials will be provided in both printed and electronic formats.

## Assumptions and Dependencies

* Availability of reliable network connectivity for data transmission.
* Access to secure cryptographic libraries for encryption.
* Requirements to be installed with the specific versions as described in documentation.
* Assumption of user compliance with privacy guidelines.

# External Interface Requirements

## User Interfaces

The user interface will be designed with the following characteristics:

* Intuitive layout for ease of navigation.
* Standard buttons for actions like 'Refresh,' 'Analyze,' and 'Report.'
* Error messages will follow a consistent format for user feedback.

## Hardware Interfaces

The system will interface with:

* Various sensors and devices for data collection.
* Secure communication protocols such as HTTPS for data transfer between devices.

## Software Interfaces

The system will interact with:

* TensorFlow (version 2.0 or higher) for model training.
* Ethereum (version 1.0 or higher) for blockchain functionalities.
* Other libraries for data preprocessing and analysis (e.g., Pandas, NumPy).

## Communications Interfaces

Communications will utilize:

* HTTPS and WebSocket protocols for data transmission.
* Encryption standards (e.g., AES, BB84) for secure data exchange and updates.
* RESTful API for interaction with the central server and user inte

# System Features

## Multimodal Data Collection

4.1.1 Description and Priority

* This feature involves the collection of real-time data from various devices, prioritized as **High**.

4.1.2 Stimulus/Response Sequences

* User Action: Initiate data collection.
* System Response: Begin real-time data collection and display status updates.

4.1.3 Functional Requirements

* + REQ-1: The system shall collect data from specified sensors.
  + REQ-2: The system shall provide a status update on data collection progress.

## Cyberattack Detection and Classification

4.2.1 Description and Priority

* This feature involves analyzing collected data to detect cyberattacks, prioritized as **High**.

4.2.2 Stimulus/Response Sequences

* User Action: Requests cyberattack analysis.
* System Response: Analyze data and return classification results.

4.2.3 Functional Requirements

* + REQ-3: The system shall classify detected threats into predefined categories.
  + REQ-4: The system shall alert users to detected threats in real-time.

## Blockchain Integration

4.3.1 Description and Priority

* This feature involves the secure storage of model updates and results on the blockchain, prioritized as **High**.

4.3.2 Stimulus/Response Sequences

* User Action: Initiates the process of recording updates to the blockchain.
* System Response: Encrypts and stores model updates on the blockchain and confirms successful storage.

4.3.3 Functional Requirements

* REQ-5: The system shall securely record model updates on the blockchain.
* REQ-6: The system shall ensure immutability of stored updates through blockchain technology.
* REQ-7: The system shall validate updates using a consensus mechanism.

## Centralized Analysis and Coordination

4.4.1 Description and Priority

* This feature involves the aggregation of model updates and analysis of results to enhance the global model, prioritized as **High**.

4.4.2 Stimulus/Response Sequences

* User Action: Requests global model refinement based on collected updates.
* System Response: Aggregates updates, refines the model, and distributes improved parameters back to devices.

4.4.3 Functional Requirements

* REQ-8: The system shall aggregate model updates from the blockchain to refine the global model.
* REQ-9: The system shall analyze aggregated results to improve detection accuracy.
* REQ-10: The system shall distribute updated model parameters back to individual devices.

# Other Nonfunctional Requirements

## Performance Requirements

The system shall process incoming data with a maximum latency of 200 ms and achieve a detection accuracy of 95%.

## Safety Requirements

The system must ensure data integrity during transmission and have rollback capabilities in case of failed updates.

## Security Requirements

The system shall implement user authentication protocols and encrypt sensitive data both in transit and at rest. It shall also adapt regular system checks and safety auditing.

## Software Quality Attributes

The system shall exhibit:

* **Reliability**: 99% uptime during operational hours.
* **Maintainability**: Code should adhere to best practices to facilitate future updates.

## Business Rules

Only authorized personnel can access sensitive components of the system.

# Other Requirements

The system must comply with relevant legal and regulatory requirements for data privacy and cybersecurity.

Appendix A: Glossary

* **CNN**: Convolutional Neural Network
* **RNN**: Recurrent Neural Network
* **NLP**: Natural Language Processing
* **IoT**: Internet of Things

Appendix B: Analysis Models

High-level architecture diagrams will be included to depict system components and interactions.

Appendix C: To Be Determined List

* TBD on specific APIs to be used for data collection and model training.
* TBD on additional data sources and formats for input data.