Project InSiN

System-Design

Group-3

Alwin Alwin
Dmytro Gerasymchuk
Evgeny Bardin
Nesrine Doghri

Agenda

1. Requirements Analysis
2. System Specification
3. System-Related Diagrams
4. Implementation Plan
5. Group Organisation

Requirement Analysis

- Identify cyber-attack in a data-set
- Ability to merge identification results with other teams

Agenda

1. Requirements Analysis
2. System Specification
3. System-Related Diagrams
4. Implementation Plan
5. Group Organisation

System Specification

- Build „normal“ data model
- Predict „abnormality“ of new data-points

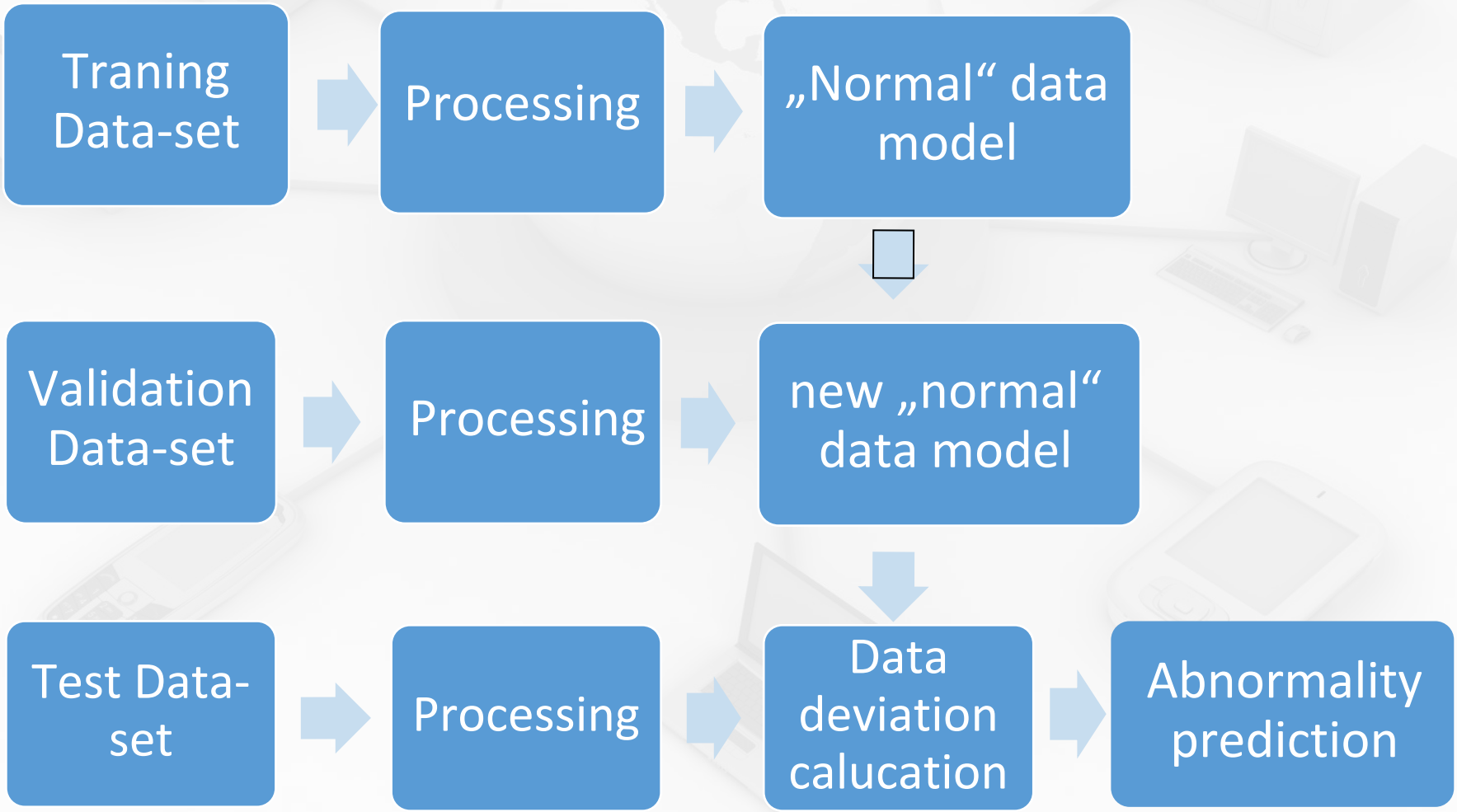
System Specification

A Practical Approach to Anomaly-based Intrusion Detection System by Outlier Mining in Network Traffic

By

Prajowal Manandhar

System Specification



System Specification (Components & Functions)

- Input data preprocessing
  - Read TCP-dump files
  - TCP/IP packets -> Java-Objects
  - Extract TCP/IP headers
  - Aggregation of TCP/IP packets into TCP sessions

System Specification (Components & Functions)

- Feature vector generation
  - Generate feature vectors
  - Feature vectors -> ARFF
- Features dimension reduction
  - Principal Component Analysis (PCA)

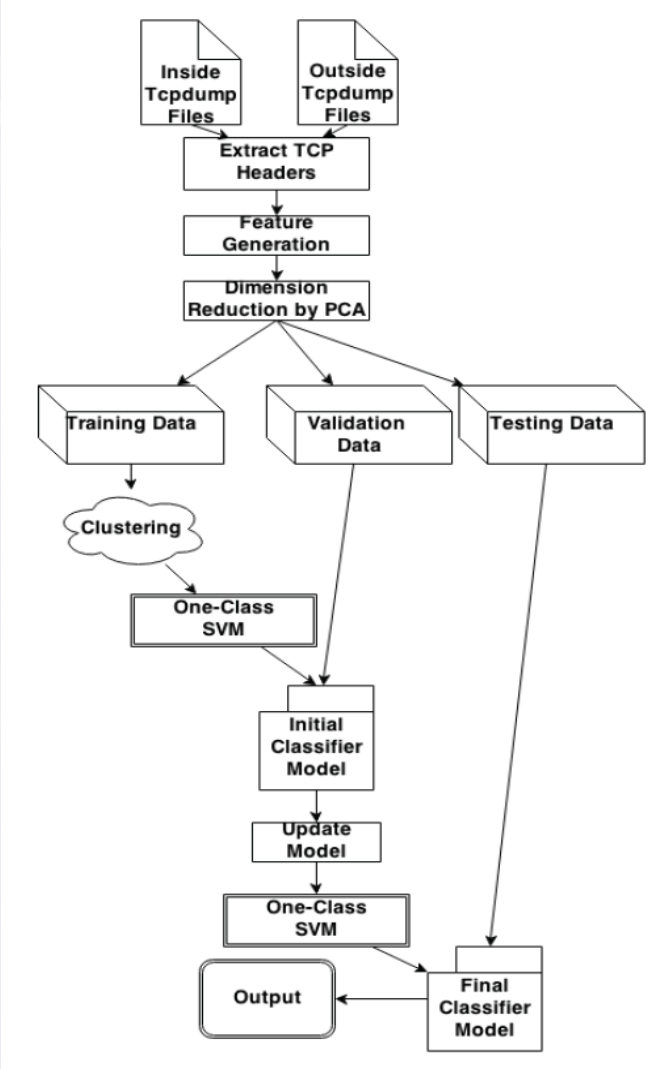
System Specification (Components & Functions)

- Clustering
  - K-means clustering
- One Class SVM
  - Euclidian-distance calculation
  - Hyper-plane function calculation

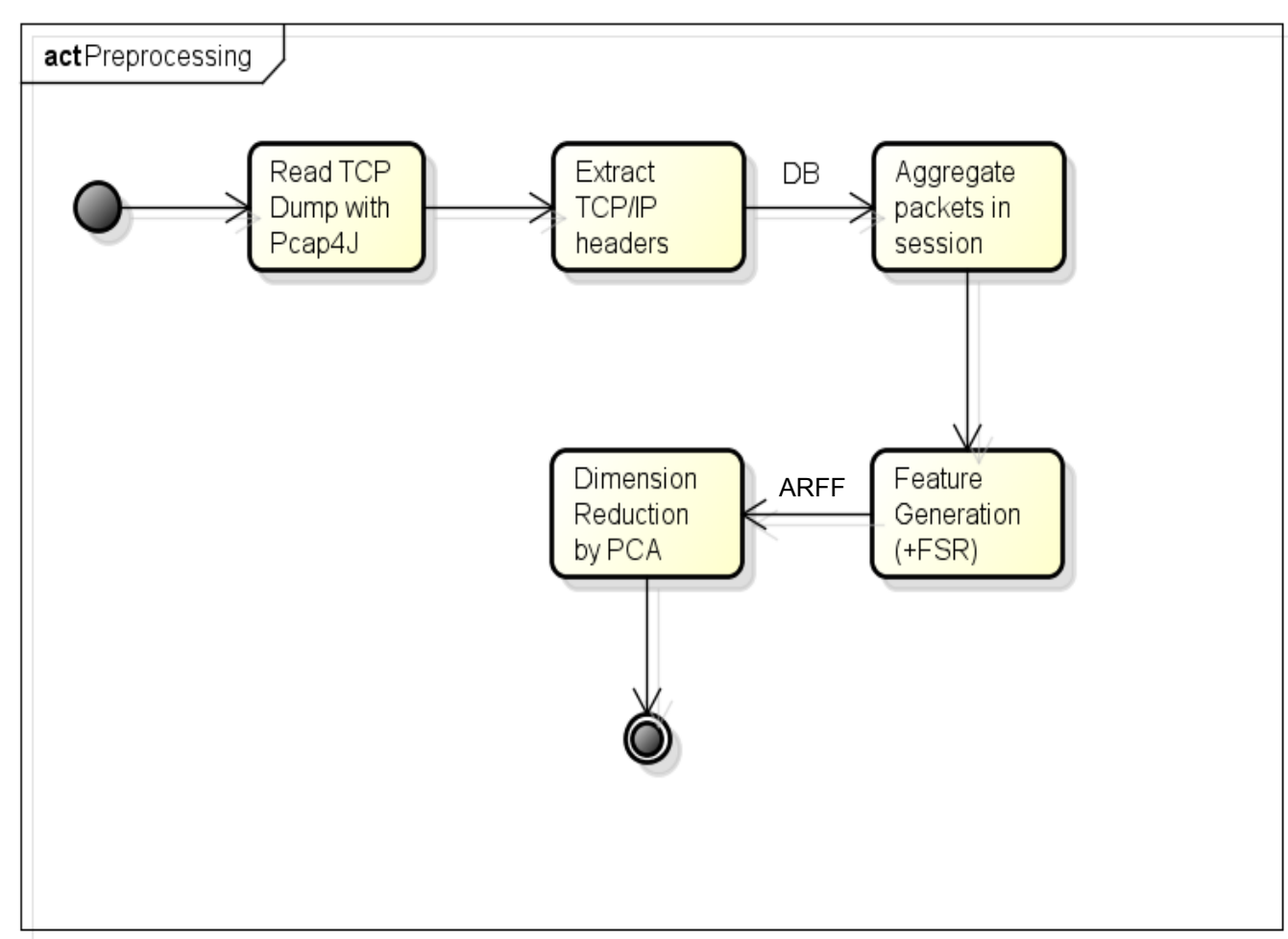
Agenda

1. Requirements Analysis
2. System Specification
3. System-Related Diagrams
4. Implementation Plan
5. Group Organisation

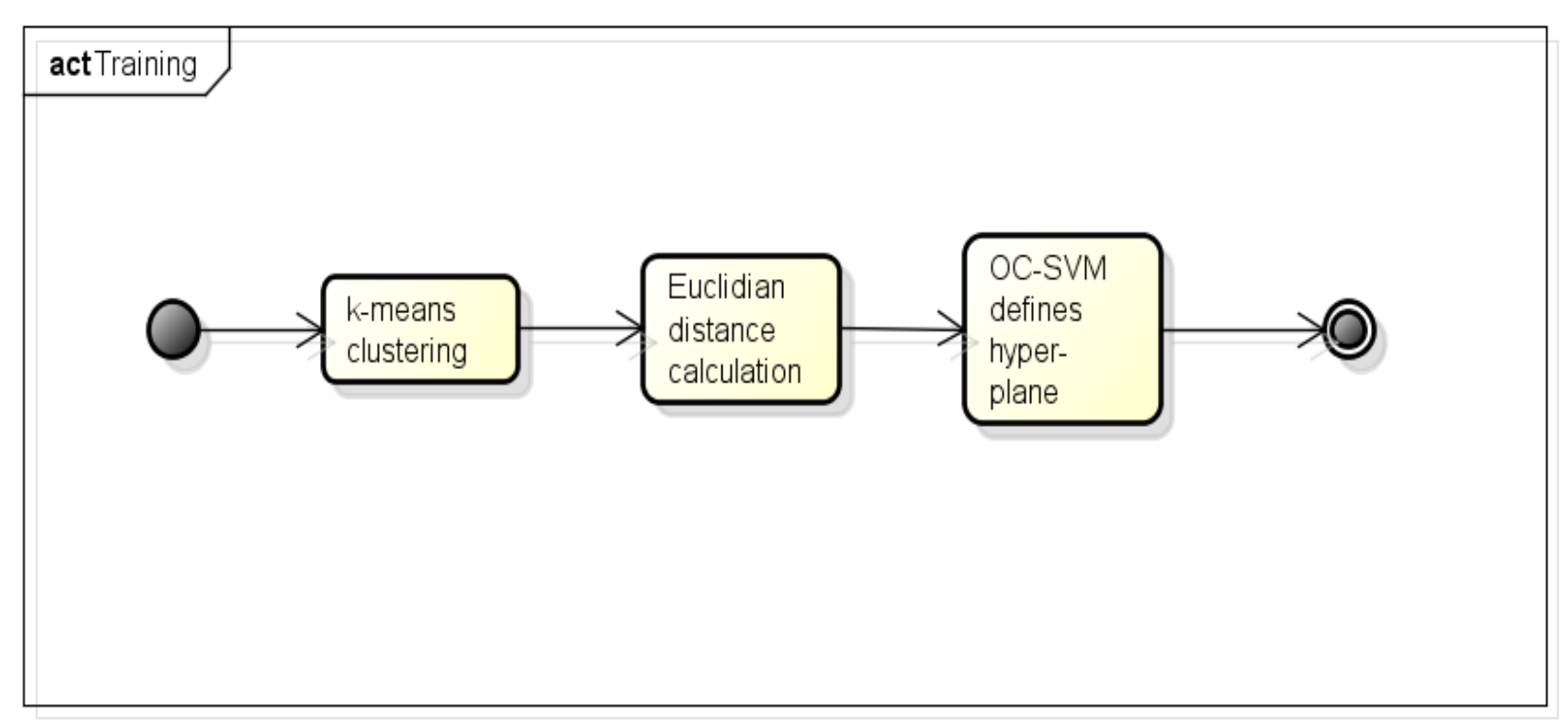
System Architecture



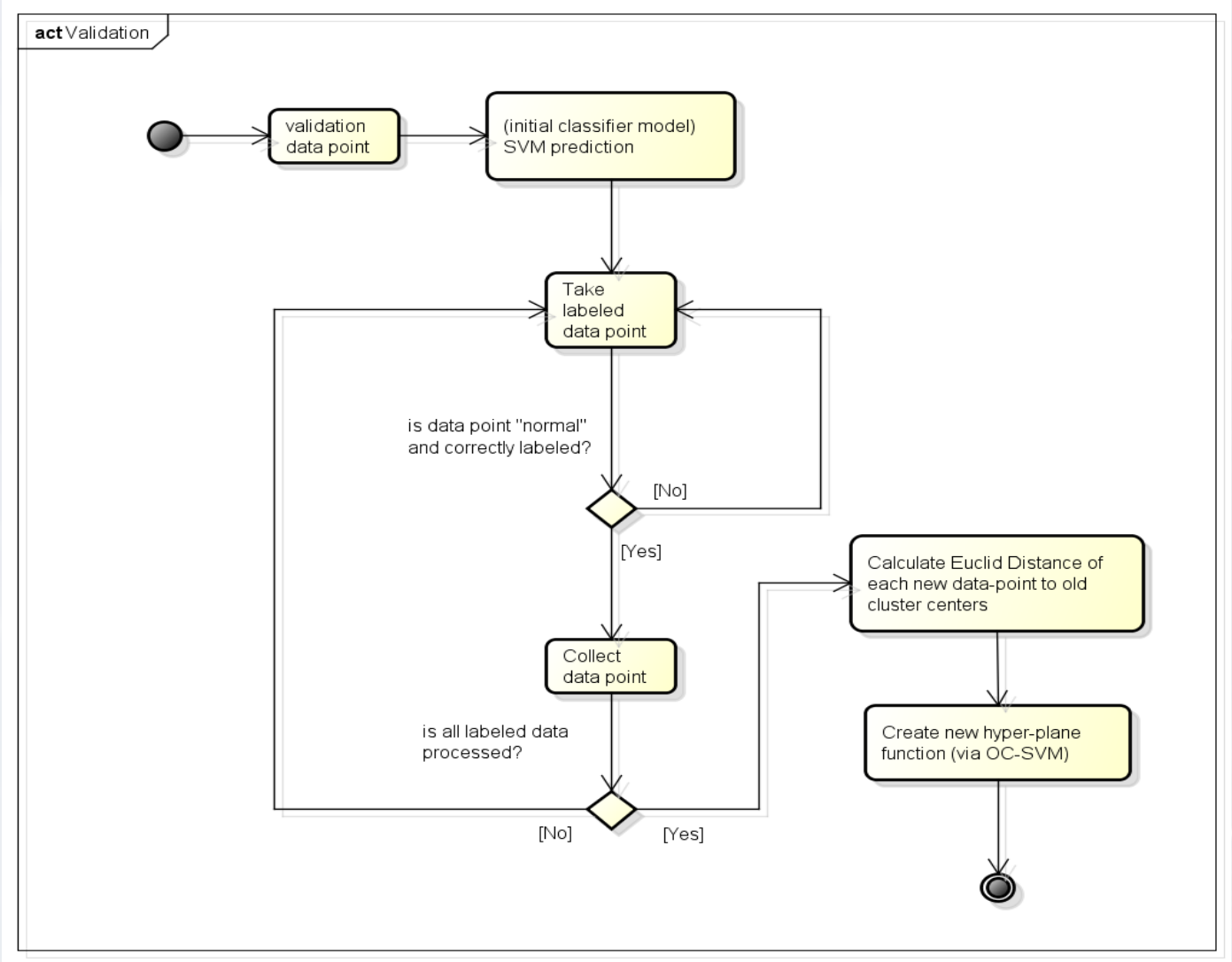
Preprocessing Workflow



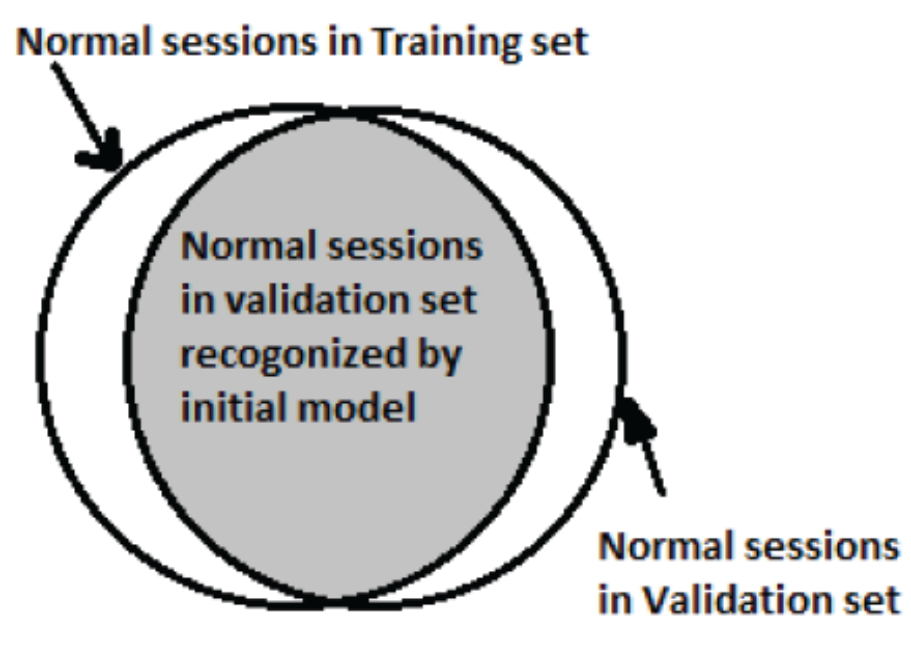
Training Workflow



Validation Workflow



Validation Workflow



Agenda

1. Requirements Analysis
2. System Specification
3. System-Related Diagrams
4. Implementation Plan
5. Group Organisation

Implementation Plan (2nd Milestone)

- Input-data preprocessing *-> 01.06*
- Feature vector generation *-> 08.06*
- Feature demension reduction *-> 08.06*
- Clustering *-> 15.06*

Implementation Plan (3rd Milestone)

- One Class SVM *-> 22.06*
- Tests *-> 06.07*

Agenda

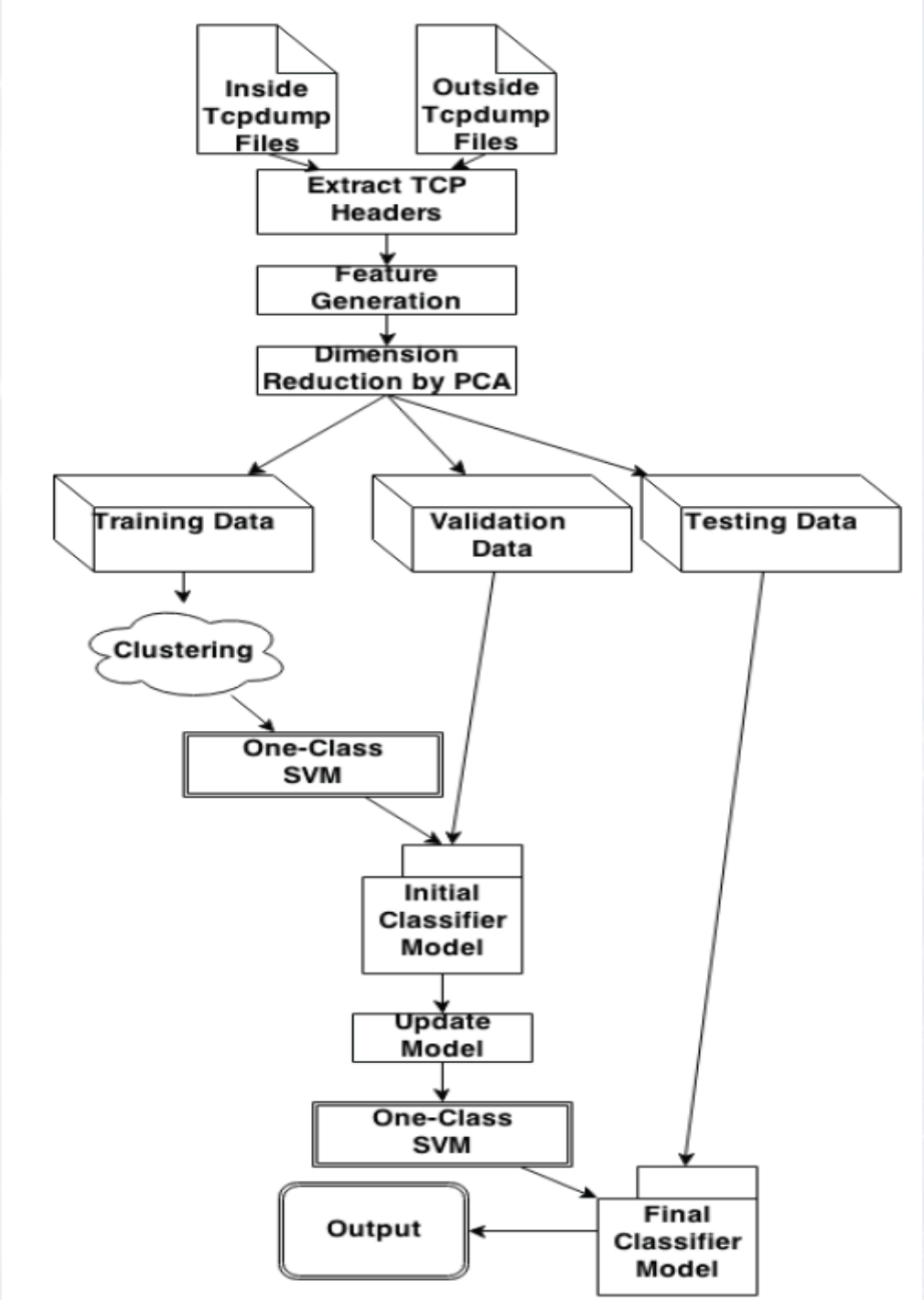
1. Requirements Analysis
2. System Specification
3. System-Related Diagrams
4. Implementation Plan
5. Group Organisation

Group Organisation

- Development enviroment:
  - Java
  - Weka
  - Maven
  - Pcap4J
  - LibSVM
  - MySQL

Group Organisation

- Organisation enviroment:
  - SVN
  - WIKI (Redmine)


Inside Tcpdump Files
Outside Tcpdump Files
Extract TCP Headers
Feature Generation
Dimension Reduction by PCA
Training Data
Validation Data
Testing Data
Clustering
One-Class SVM
Initial Classifier Model
Update Model
One-Class SVM
Output
Final Classifier Model