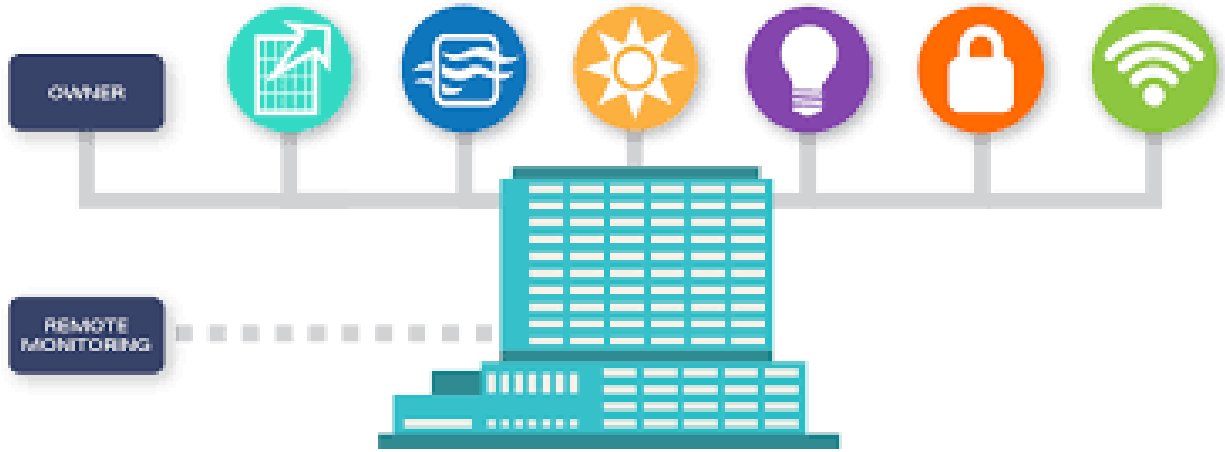
Anomaly Detection in Building Automation Control Networks (BACnet)

Team:
Sofian Ghazali,
Muhammad Zahid Kamil,
Rahul Balamurugan

Mentors:
Dr. Hussein Al Nuweiri
Mr. Salah Hessein

Introduction

- *BMS* - Building Management Systems



[1]

- *BACnet* - Building Automation Control Network Protocol

[2]

Problem Statement

- Current Number of exposed BAS devices: 48,112 [3]
- Ukraine power outage, Dec 2015: Affected 230,000 people [4]

=>Need for greater threat detection/prevention measures in BMS

Our Solution

- Robust Intrusion Detection Algorithm
- Capture potential breaches
- Alert users in the building facility

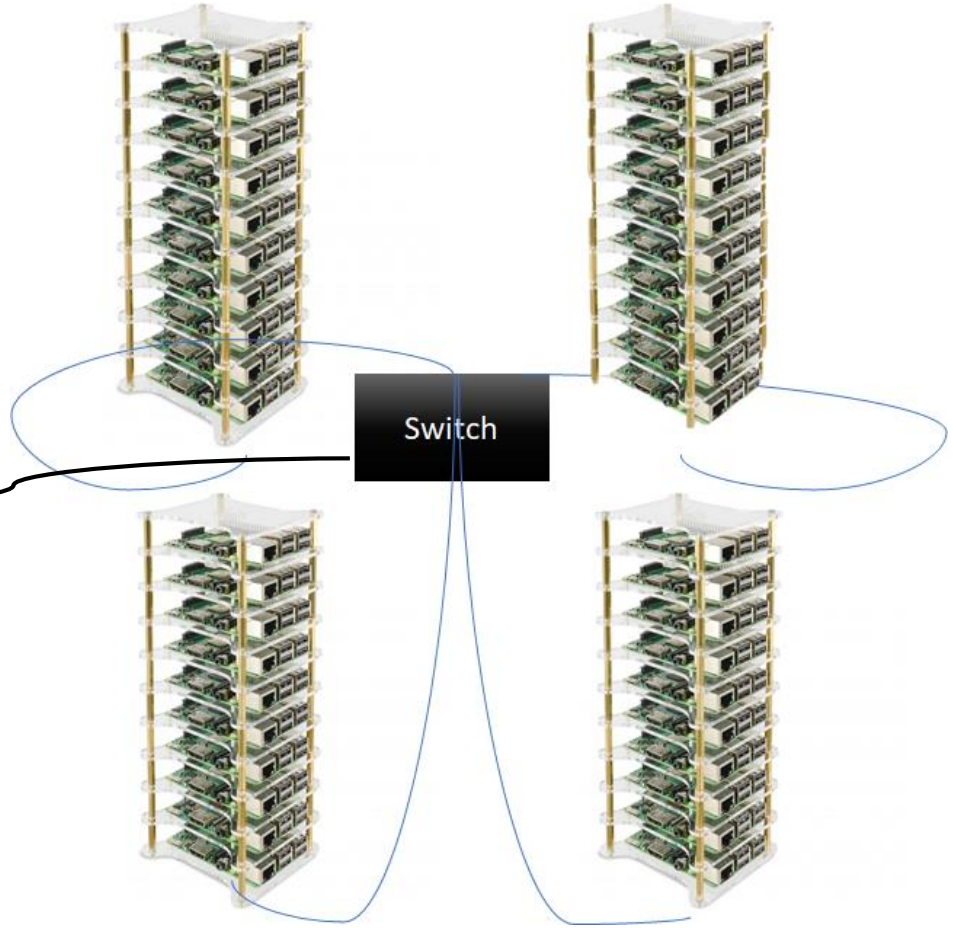
Design & Software

[6]

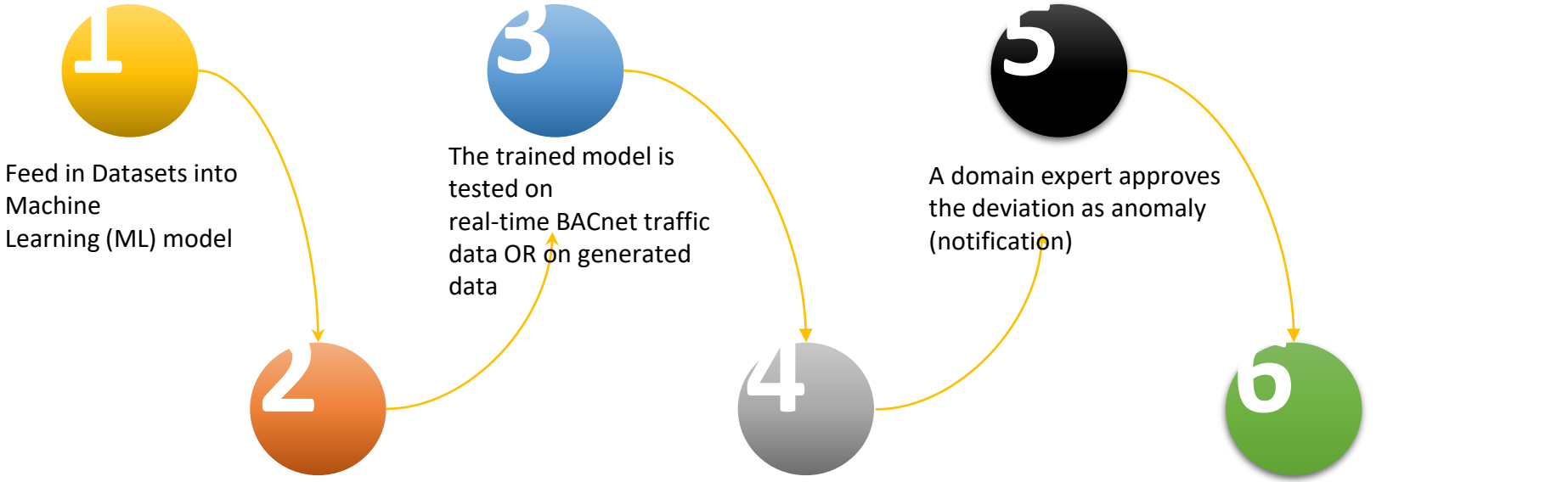
[7]

[8]

[5]



General Overview



Standards

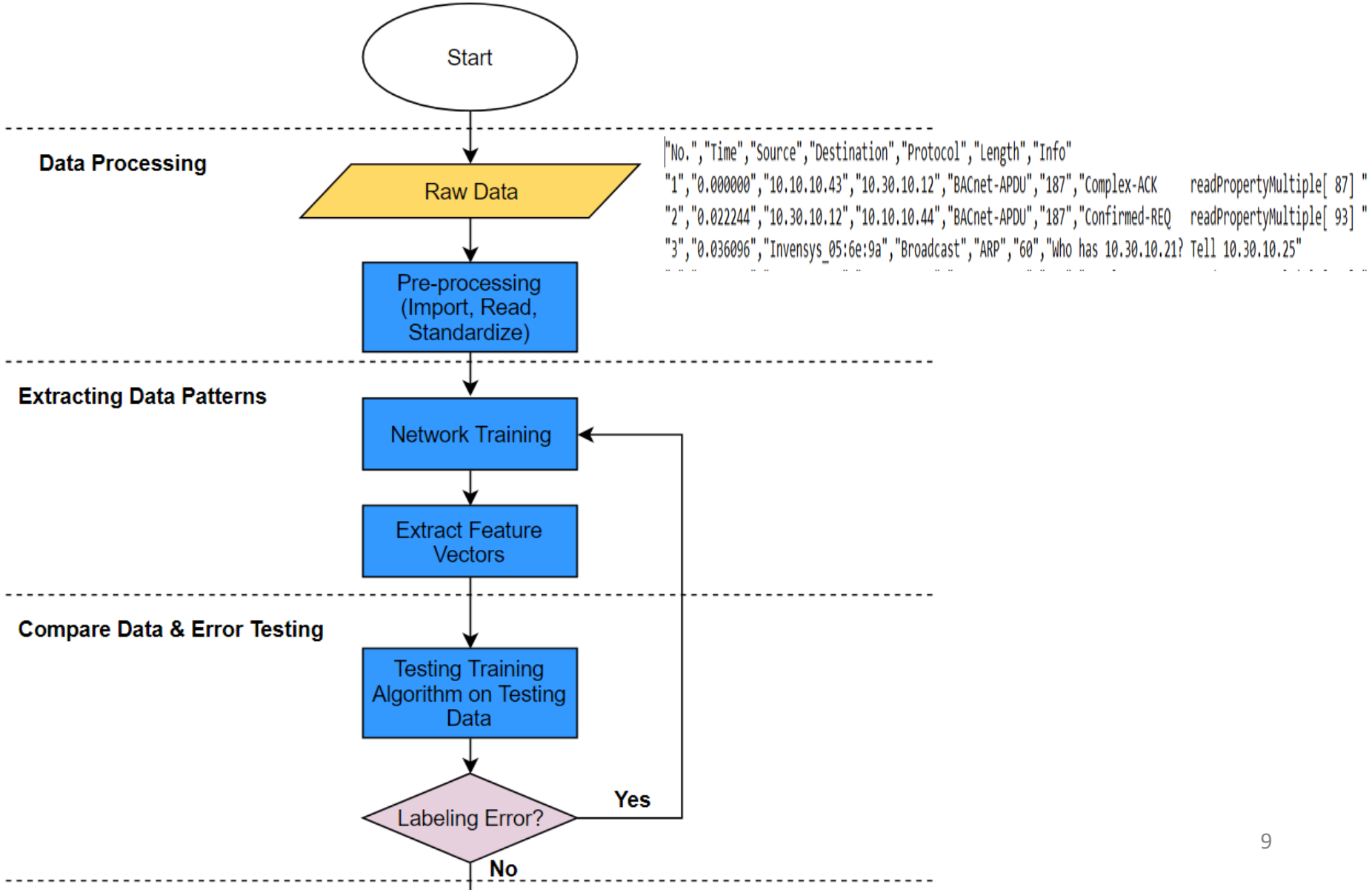
- ANSI-ASHRAE 135-2016 [9]:
  - Defines procedure and message syntax
  - Details third party connections to existing BACnet

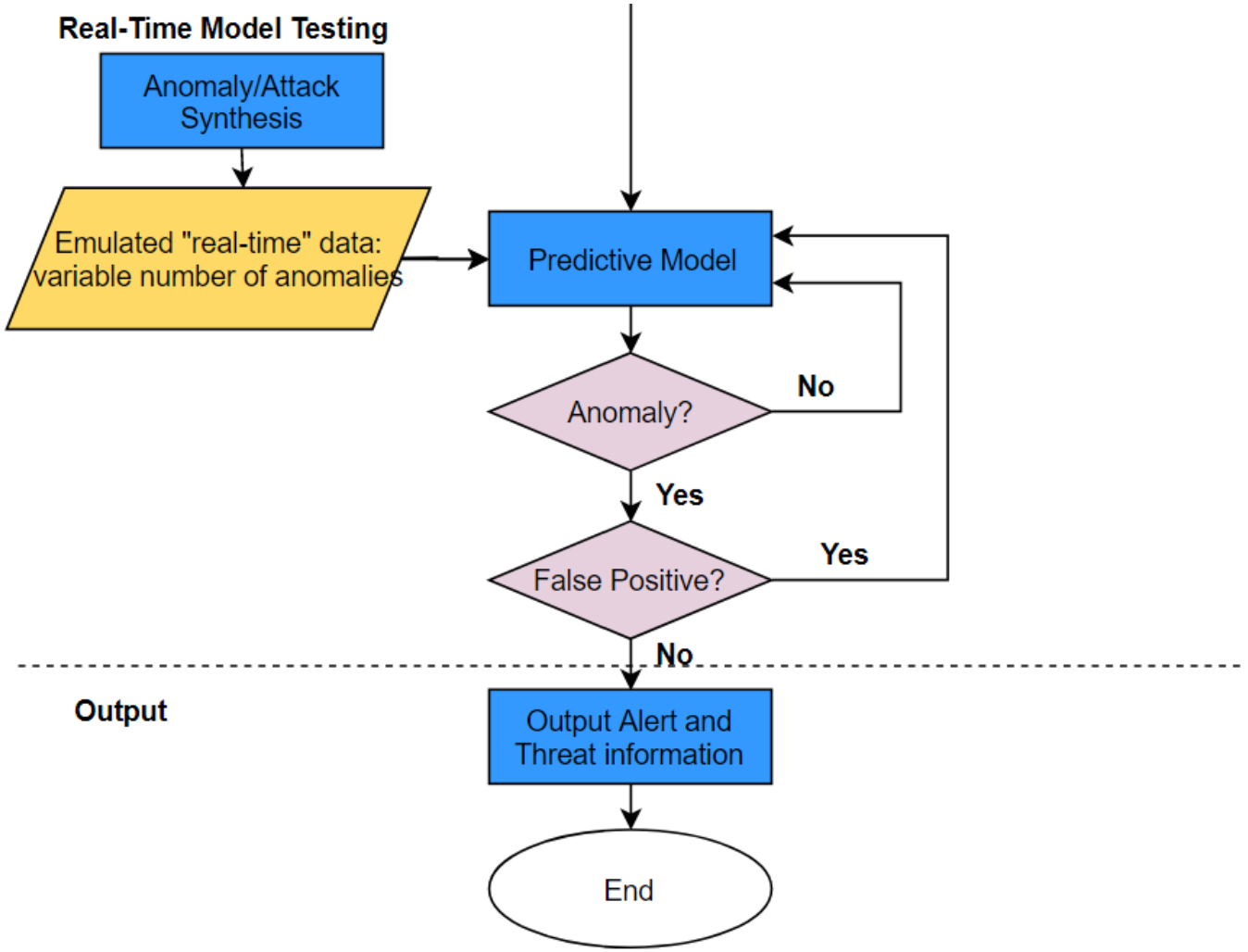
- Standards compliant hardware (Ethernet connection, IPv4 Network Protocol)

Constraints

- Lack of real BACnet data
  - Difficult to get from IT due to security reasons
- Cannot test cyber attacks on real BMS
- Solution: Emulate BACnet devices and generate data

Program Flow




Real-Time Model Testing
Anomaly/Attack Synthesis
Emulated "real-time" data: variable number of anomalies
Predictive Model
Anomaly?
No
Yes
False Positive?
Yes
No
Output
Output Alert and Threat information
End

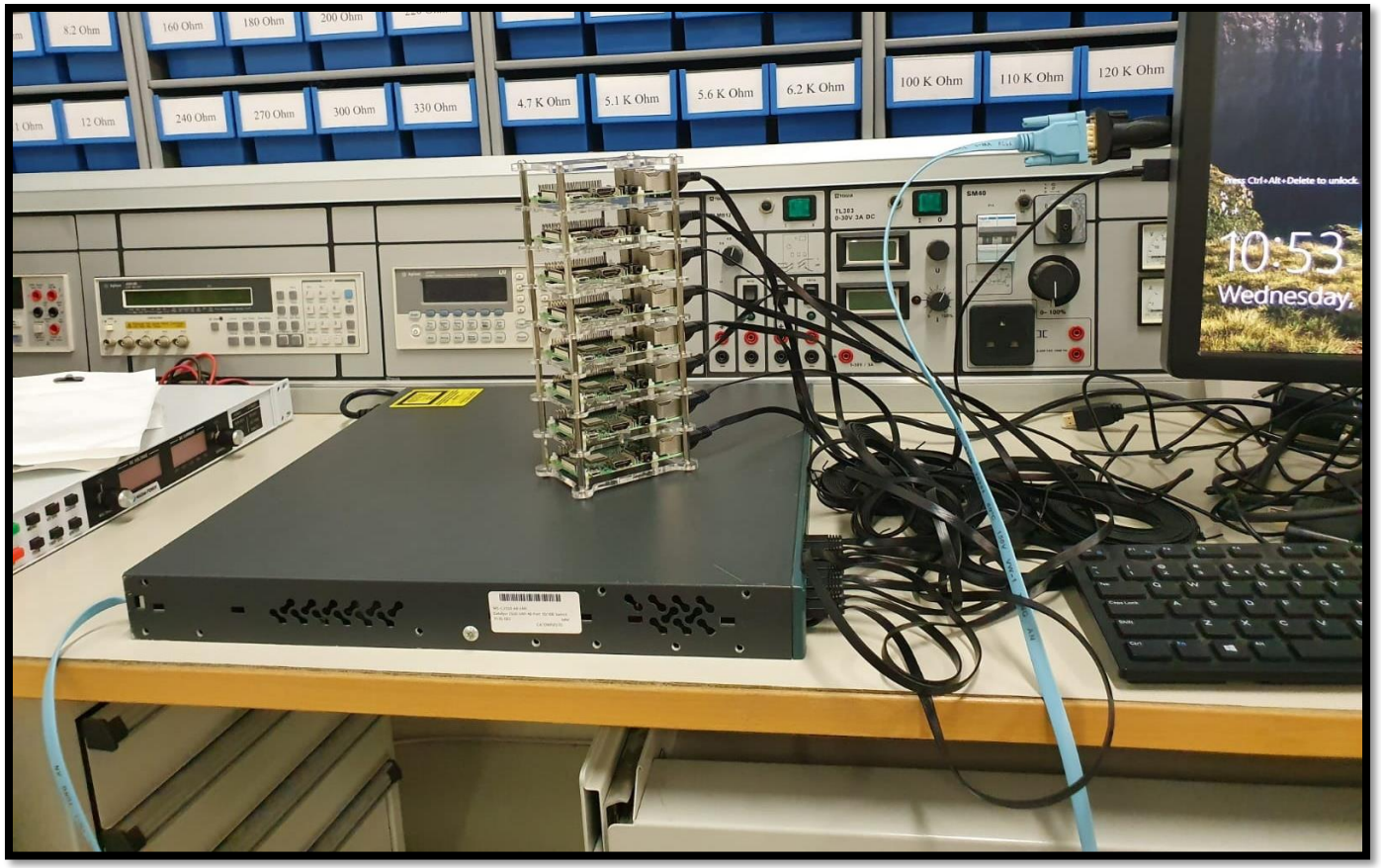
Performance Criteria

Criteria	Our Solution
Public Safety	Possibly threat in case of failure or breach
Responsiveness	Highly responsive due to unsupervised learning capabilities
Adaptability	Needs human input to adapt to new patterns, but easily does so
Comprehensiveness	Accounts for a wide range of threats as it only learns normal patterns
Fail-Proof Measures	None for the time-being except for human observation
Economics	Could be cheap or costly depending on method of implementation
Global	Can be implemented in any BACnet network across the globe
Cultural	Regular data collection could offend certain cultural sensibilities
Public Health	Malicious triggering of alarms could cause panic
Social	Help better the wellbeing of building users by protecting them from cyber criminals
Environmental	The project has negligible impact on the environment

Product Analysis

	Password Protection	AC2000 Interface [11]	THE-Driven Anomaly Detector [12]	Our Solution
Accuracy	Not Applicable	Information Not Available	~96%	-Can't be measured-
Limitations	Limited to passive protection	Manual configuration required	Constrained by flexibility of frequency analysis techniques	Impossible to have a 0% false positive rate
Pros	Easy to implement, most cost-effective	User-friendly, can be used across all common BMS protocols	Efficient data classification, high accuracy and sensitivity;	Highly adaptive and comprehensive
Cons	Easily bypassed	Not open to novel detection mechanisms	Not dynamic	Problems due to mistraining

Current Progress



Project Milestones

September 2019
Project Proposal

November 2019
Initial Design finalized

December 2019
Set-up Test rack

Stage 1

Worked on program flow, customer needs analysis and benchmarking

Stage 2

Implement hardware design, set-up Local Network and prepare Raspberry Pi stack for data generation

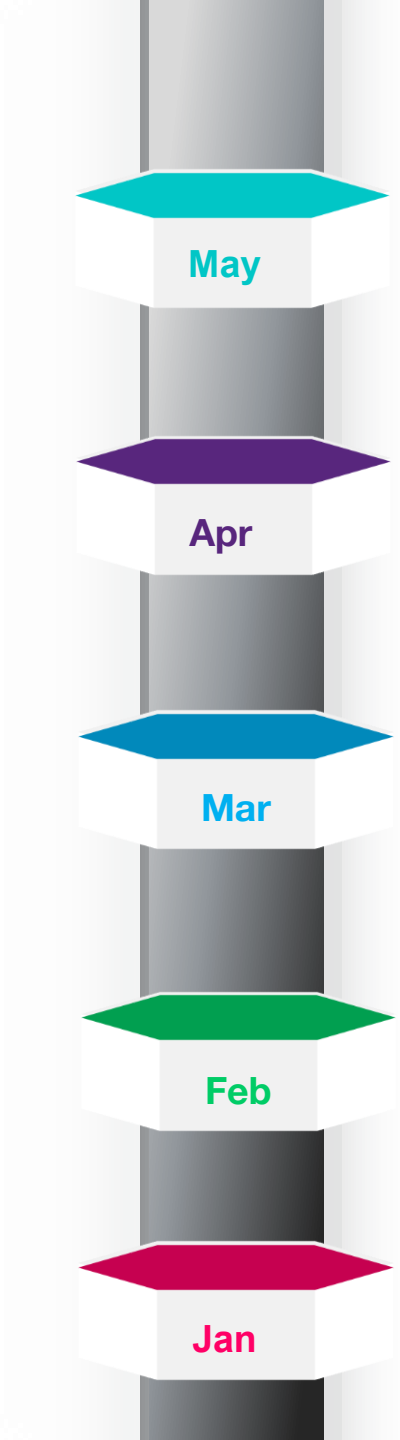
Our Beginning

Deciding problem statement, analyzing project feasibility and brainstorming

Next Semester

Work on the machine learning algorithms and implement software

Timeline



May 2020
Graduation

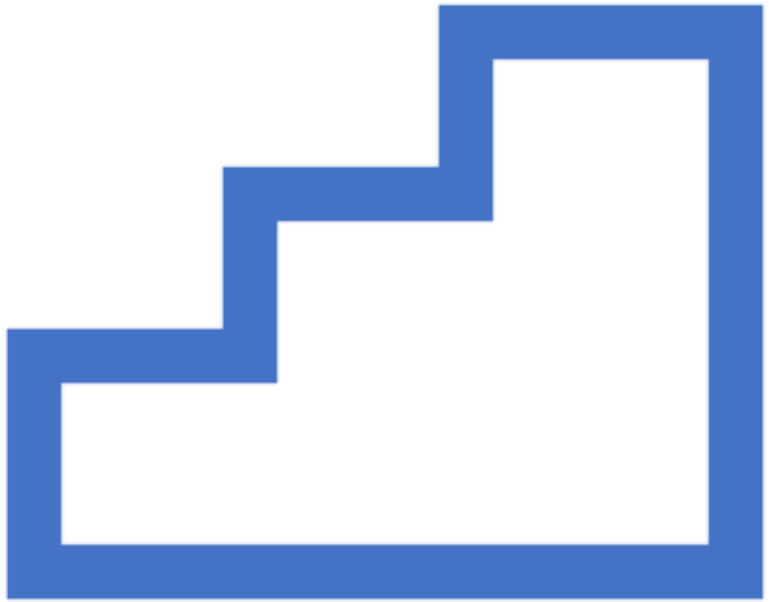
April 2020
Prepare for demo day

March 2020
Start network training, Test anomaly detector and continue network training

February 2020
Implement and adapt the machine learning algorithm, debug software

January 2020
Generate datasets, finalize machine learning techniques

Future Steps



- Possibly create an app for remote alerts
- Consider cost mechanics of embedded detector
- Implement predictive threat detection mechanism in a real-time BACnet system

References

1. MLN Company. (2019). *Building Management Systems - MLN Company*. [online] Available at: http://www.mlncompany.com/what-we-do/building-management-systems/ [Accessed 4 Dec. 2019].
2. Dms.hvacpartners.com. (2019). Bacnet Basics User's Guide. [online] Available at: https://dms.hvacpartners.com/docs/1000/Public/04/11-808-417-01.pdf [Accessed 3 Sep. 2019].
3. Metadata, https://censys.io/ipv4/metadata?q=bacnet&
4. Pavel et al, “Ukraine's power outage was a cyber attack: Ukrenergo”, Reuters, Jan 18,2017. Accessed 16 Sep 2019
5. Google Search. [Online]. Available: https://www.google.com/search?q=laptop&sxsrf=ACYBGNTFECOoj5LsWVDNZAtvfmGRDvmjTg:1575445883360&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiG_vWhwZvmAhXFqlkKHUNgD4QQ_AUoAXoECA8QAw&biw=1536&bih=722#imgrc=kte5opKgrQ4V2M: [Accessed: 04-Dec-2019].
6. Google.com. (2019). [online] Available at: https://www.google.com/search?biw=1536&bih=722&tbm=isch&sxsrf=ACYBGNS8tUPvlhPpovtFekzpGNjoJJSAQw%3A1575445890149&sa=1&ei=gmXnXdvkCKHH_Qb-uYGgCA&q=python+logo&oq=python+logo&gs_l=img.3..0i67l6j0l4.172058.173659..173854...1.0..0.263.1954.2-8.....0....1..gws-wiz-img.....10..35i39j35i362i39j0i131.gFK6bEnemfw&ved=0ahUKEwjbrZSlwZvmAhWhY98KHf5cAlQQ4dUDCAc&uact=5#imgrc=0-lAWpuQBjsPGM: [Accessed 4 Dec. 2019].
7. “Download,” *Wireshark · Go Deep.* [Online]. Available: https://www.wireshark.org/. [Accessed: 04-Dec-2019].
8. https://www.google.com/search?biw=1536&bih=722&tbm=isch&sxsrf=ACYBGNQ-tVlGHIieP1T0np9TKirjY3qQ9w%3A1575446119500&sa=1&ei=Z2bnXYuQHu2c_Qbfj7XoAw&q=vnc+viewer+logo&oq=vnc+viewer+logo&gs_l=img.3..0.10232.10815..11082...0.0..0.241.1666.2-7.....0....1..gws-wiz-img.....35i39j0i24.BsssxU3wkTM&ved=0ahUKEwjL38KSwpvmAhVtTt8KHd9HDT0Q4dUDCAc&uact=5#imgrc=sk6RIltid5PenM:
9. Ashrae.org. (2019). *Standard 135-2016, BACnet™ -- A Data Communication Protocol for Building Automation and Control Networks*. [online] Available at: https://www.ashrae.org/technical-resources/standards-and-guidelines/standards-addenda/standard-135-2016-bacnet-a-data-communication-protocol-for-building-automation-and-control-networks [Accessed 4 Dec. 2019].
10. “AC2000,” AC2000 Access Control & Security Management | CEM Systems. [Online]. Available: https://www.cemsys.com/products/access-control-systems/ac2000/ . [Accessed: 06-Nov-2019].
11. Z. Zheng and A. Reddy, “Safeguarding Building Automation Networks: THE-Driven Anomaly Detector Based on Traffic Analysis,” 2017. [Online]. Available: http://cesg.tamu.edu/wpcontent/uploads/2018/01/ICCCN-Zhiyuan-Zheng-Paper-2017-July-1.pdf

Thank You!