Anomaly Detection and Alert System for Facilities and Factories

Dominic Peng
2020/11/30

Traditional Camera Based Surveillance Systems and their Failures

Average cost of surveillance systems
$5,000 - 25,000
per month.

Which can make up
More than 5-20% of
medium to small company's annual expenditure.

Shortcomings

- **High Cost**
  - In a traditional setting, purchasing business security hardware, installation fees, business monitoring by professionals can be of high expenditures
- **Ineffective Security Surveillance**
  - 2021 March, over 200 Tesla factory and warehouse camera hacked
  - 2022 September, Ford lost 20 Mustang GTs near a surveillance guarded storage facility

Our System Makes a Difference

- **Kiana, and Cloud-based RTLS**
  - Kiana's Real Time Location Solutions (RTLS) technology tracks the location of objects or people in real time within a building or other contained area.

- **Our Anomaly Detection and Alert System**
  - With Kiana RTLS technology: track the movement of the devices and collect their MacAddress
  - Conduct unsupervised machine learning analysis to recognize collected data
  - Categorize data into different groupings while monitoring their movements
  - Uses SMS portal authentication to extract user phone numbers, and send notifications messages to relevant personnel when abnormal activities are detected

- **What Our System Brings?**
  - Massive pay off in data security and loss reduction
  - Provide the capabilities of venturing on to Industry 4.0 process
  - Requires no additional software or installation costs

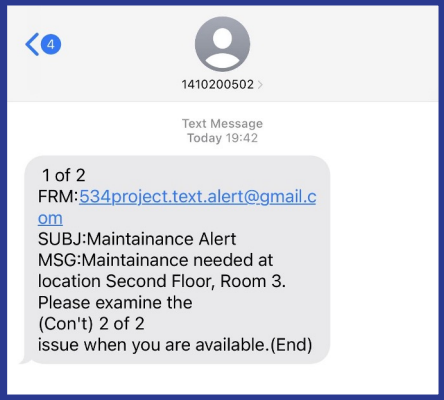
Anomaly Detection and Alert System Performance

Traditional Camera System

- Manually check: Time & Energy Consuming
- High maintenance cost
- Not all places monitored
- Not real time

Anomaly Detection and Alert System

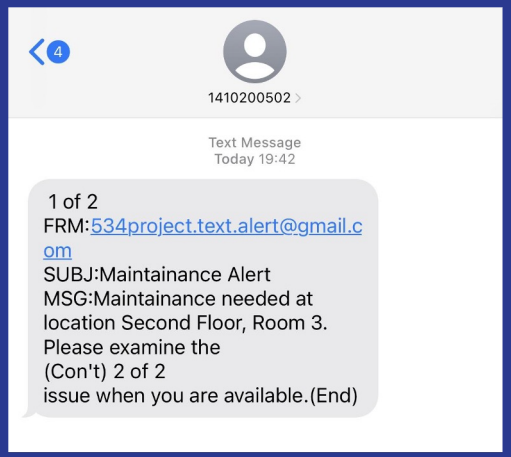
- No additional devices needed
- Low maintenance cost
- All areas covered
- Real time



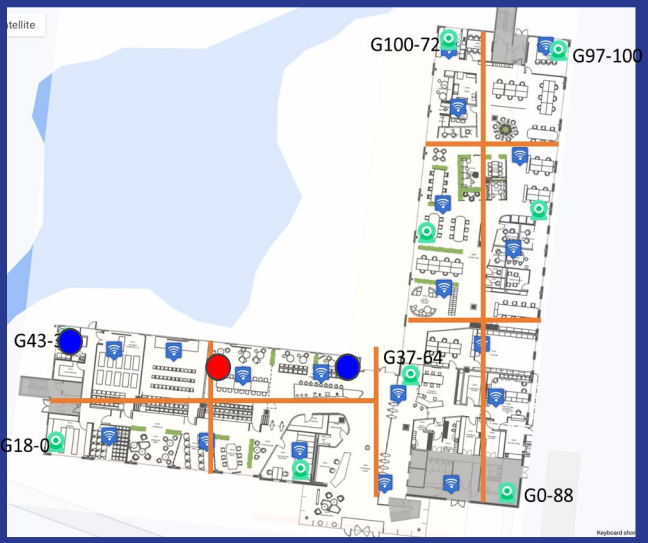
Anomaly Detection and Alert System Performance

	ClientMacAddr	Alarmtime	Floor	Area	Abnormal_type
0	88:66:a5:33:9f:c2	2019-11-28 12:40:45.961 UTC	3	[64, 85]	human_security
1	a4:c3:f0:a1:fc:2a	2019-12-15 08:27:16.863 UTC	2	[63, 90]	human_security
2	9c:da:3e:69:cb:7a	2020-02-12 12:44:63.961 UTC	2	[64, 86]	human_security
3	90:61:ae:25:4b:2b	2020-06-29 17:54:35.473 UTC	0	[58, 85]	machine_maintenance
4	84:9f:b5:e5:4d:8f	2020-07-08 19:44:63.658 UTC	1	[39, 83]	human_security
5	5c:5f:67:8c:17:7f	2020-08-31 03:35:55.43 UTC	3	[87, 92]	human_security

Output of Detected Anomaly Activities



Alarm Message Example
anomaly activities nearby)

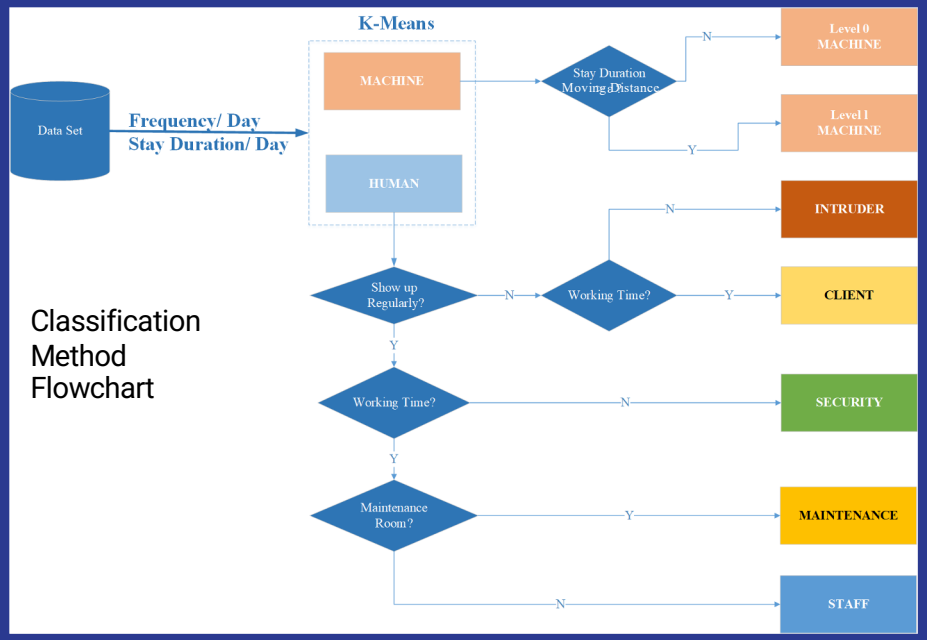


Closest Camera Location (will be activated while

Machine and Personnel Identification

The system uses unsupervised machine learning models to categorize its recorded devices into two large groups: **Machine** and **Human.**

Each of the two groups have their own subgroups.



Classification Method Flowchart

Machine Classification Groups

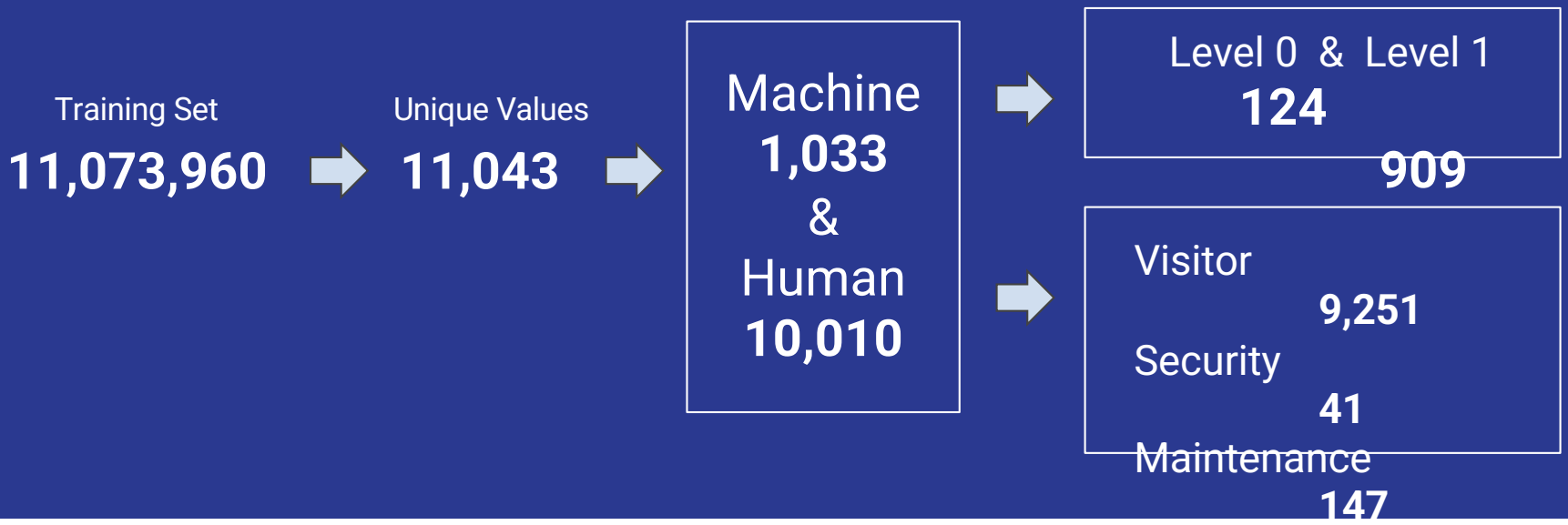
Classification	Description
Level 0 Machine	Machine of great importance, do not usually leave its designated space.
Level 1 Machine	Machine for daily use, can be shifted and moved to other rooms for according to needs.

Human Classification Groups

Classification	Description
Intruder	Unexpected visitors that enters the building during non-working hours.
Client	Visitors that enters the building during normal working hours.
Security	Security personnel that patrol the secured space at non-working hours and stays in the security room during working hours.
Maintenance	Maintenance team that needs to be called to the scene when technical assistance is needed on Level 1 Machines.
Staff	Working staff at the facility, comes to work and leaves office on schedule.

Kiana Data Explorations Overviews

- The original pharmacy dataset has been split into training and testing sets, the training dataset consists 70% of the overall data covering 11,073,960 observations of a pharmacy company from 2019 Aug to 2020 Aug.
- Original dataset consists of the observations of devices in the area, with attributes: unique MacAddress, longitude, latitude, localtime, and floor level.



Machine and Personnel Identification

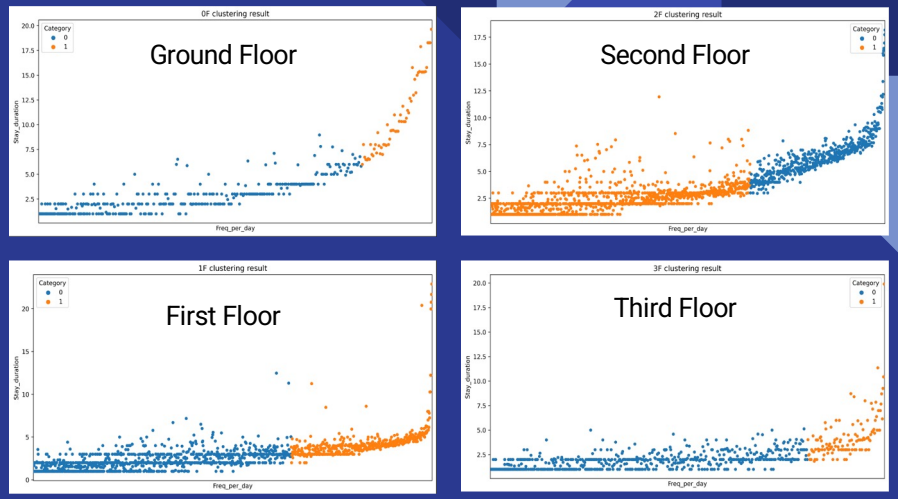
Human V.S. Machine

- We conducted a general human/machine splitting using K-means clustering method.
- The model examines
  - **signal frequency per day**
  - **online duration per day**
  - **most commonly appeared location**

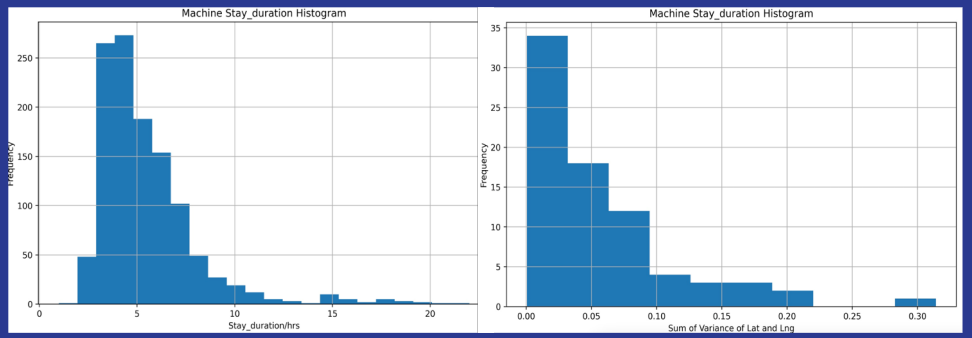
Level 0 Machine V.S. Level 1 Machine

- Further classify machines into high significance machine and regularly used workplace machines.
- The two are separated by
  - **duration of a machine staying in the same spot**
  - **sum of variance of moving distance**

K-means Cluster Analysis on Different Floors

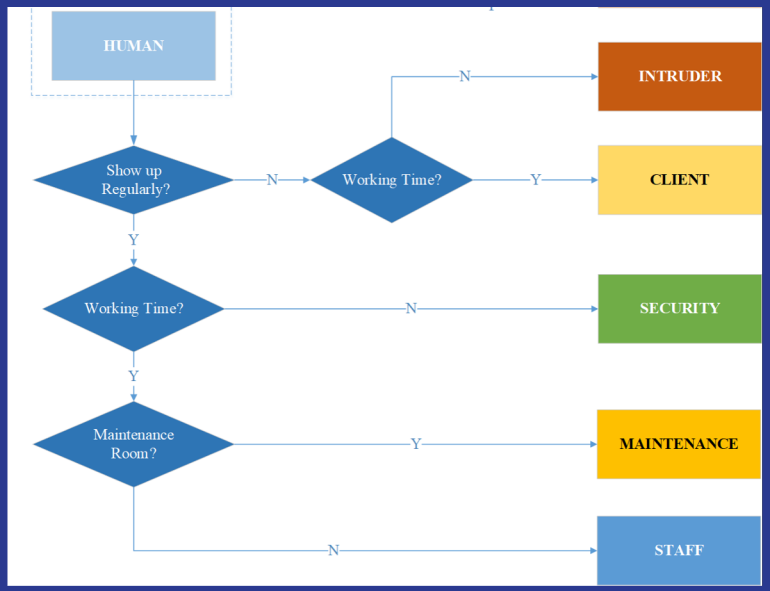


Histogram for Stay Duration and Moving Distance



Further Personnel Identification

Flowchart for Personnel Separation



Human V.S. Human

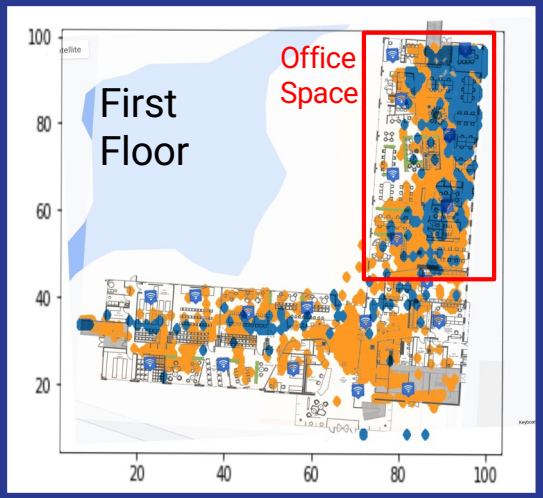
Based on time of appearance, stay duration, and commonly stayed area, the system further divided humans into **security personnel**, **maintenance team**, **working staff**, **client** and **intruder**.

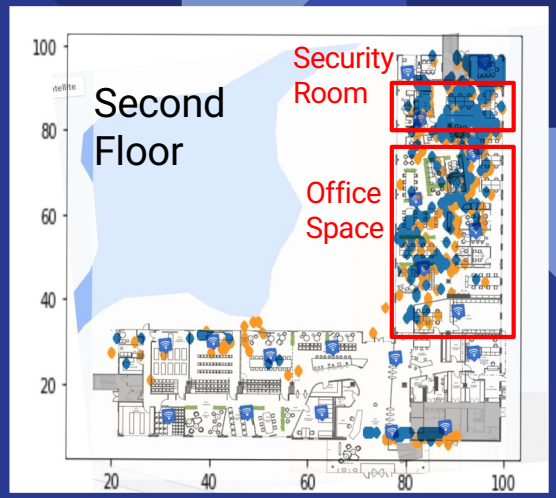
- **Time of Presence**
  - Security, maintenance and staff usually have a fixed schedule of presence
  - Client and intruder visits at random
- **Overall Stay Duration**
  - Maintenance and staff usually have a fixed working hours
  - Security personnel stays in the facility longer
- **Commonly Stayed Area**
  - Security, maintenance and staff have their designated working area
  - Client and intruder do not

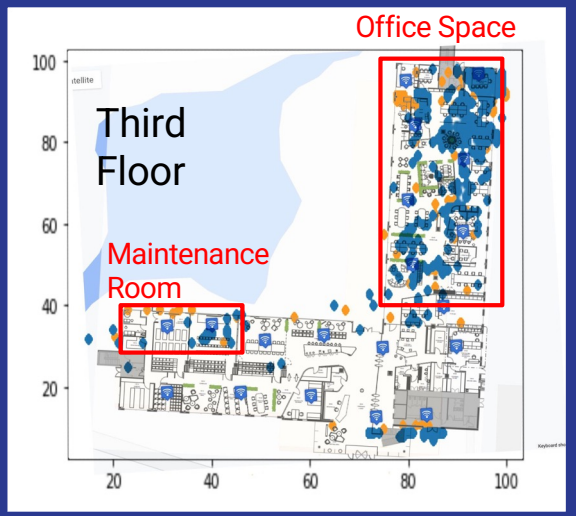
Further Personnel Identification

1) Gridding System that divide floor map into 100 x 100 grids.

2) Assigned Floor Map for First Floor and Second Floor

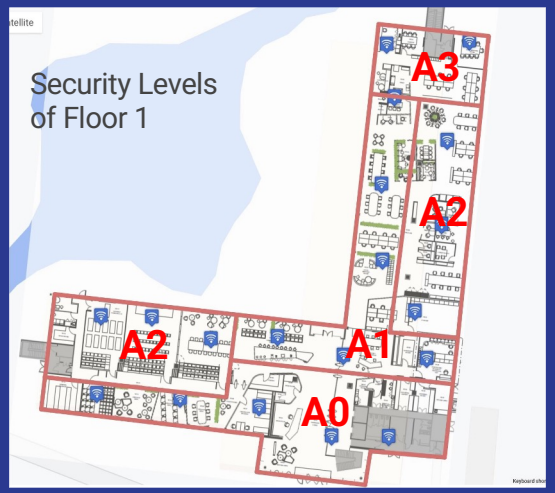


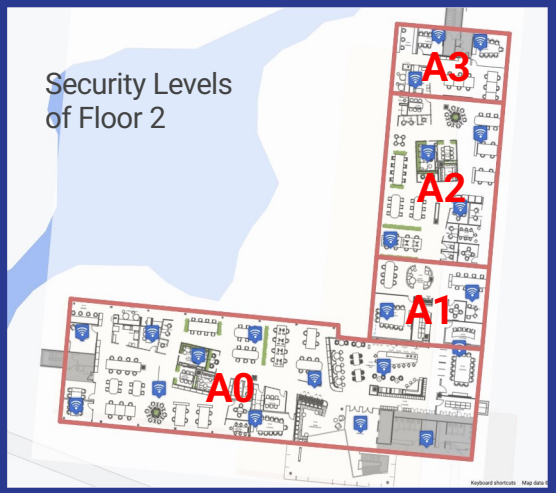




- A gridding system is created to simplify computation.
- We used grids to assign different rooms for convenience of personnel recognition and dividing security levels.
- The rooms are appointed with our conjectures. Rooms can be easily modified by changing the assigned grids.

Abnormal Activity Detection: Levels of Floors and Humans





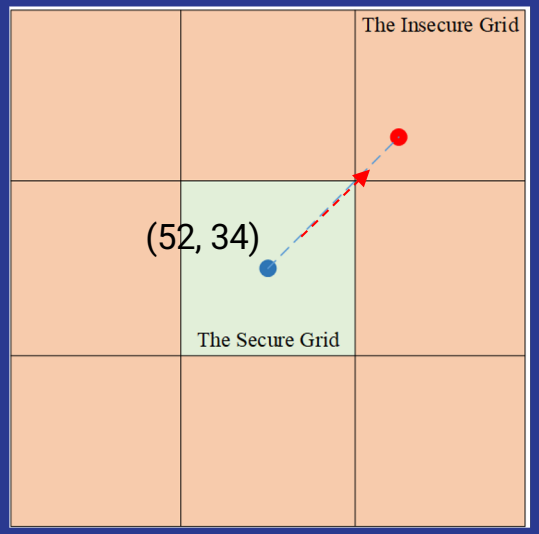
Classification	Security Level	Regional Level	Areas allowed to enter
Security	3	3	Area 0, Area 1, Area 2, Area 3
Maintenance and High level Staff	2	2	Area 0, Area 1, Area 2
Low level Staff	1	1	Area 0, Area 1
Visitor	0	0	Area 0

Classification Groups and their Assigned Security Levels

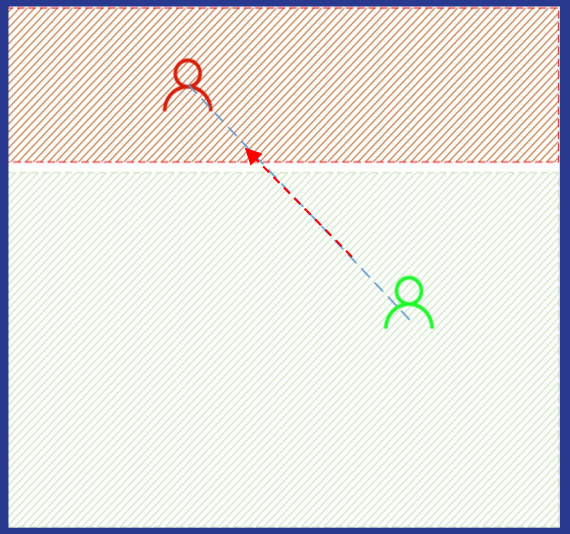
- 4 Levels: 0, 1, 2, 3
- Assigned levels based on cumulative population density: the higher the density, the higher the security level

Replicable :)

Abnormal Activity Detection: Levels of Machines and Humans



Security area for machines (10x10 surrounding grids)



Security area for humans

Level 1 Machines

- Leave secure grid —> Level 3 alarm (Security)
- Signal disappears —> Level 3 alarm (Security)

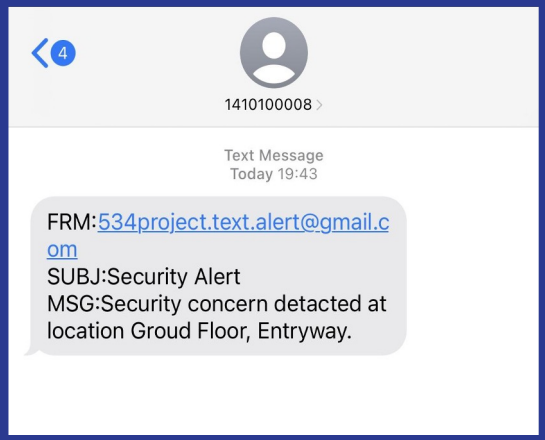
Level 0 Machines

- Leave company building —> Level 3 alarm (Security)
- Signal disappears —> Level 1 alarm (Maintenance)

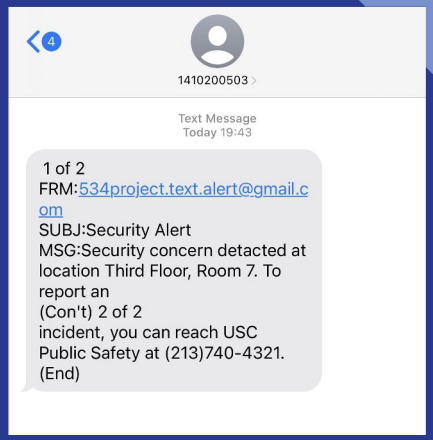
- Enter unpermitted area —> level 3 alarm (Security)

Abnormal Activity Detection: Anomaly Alert

Level 1 alert messages



Level 2 alert messages



Level 3 alert messages

- Connect to WIFI —> obtain phone number through SMS Portal authentication
- Security & maintenance are responsible for different areas
- Notify type & location of incidents
- System connects to security cameras
- Our testing model sent alert messages through the built-in python package smtplib, for communication on an enterprise scale, there are other platforms, e.g., Twilio, to provide APIs programmable communication tools

Abnormal Activity Detection: Third Party Connections

Cooperating Security Cameras

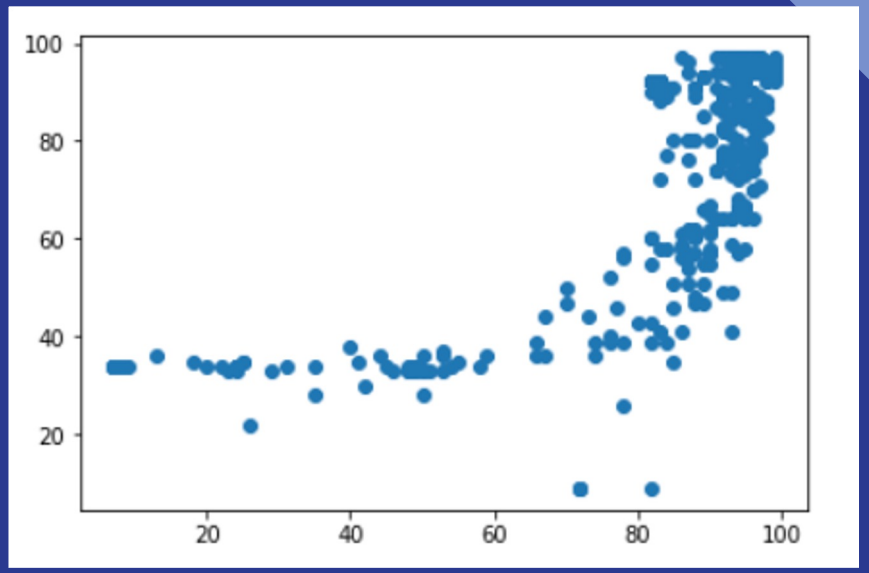
- Each security camera is responsible for specific grids
- System connects to security cameras
- Send video, type and location of the incidents as needed

Thank you for listening!

Appendix

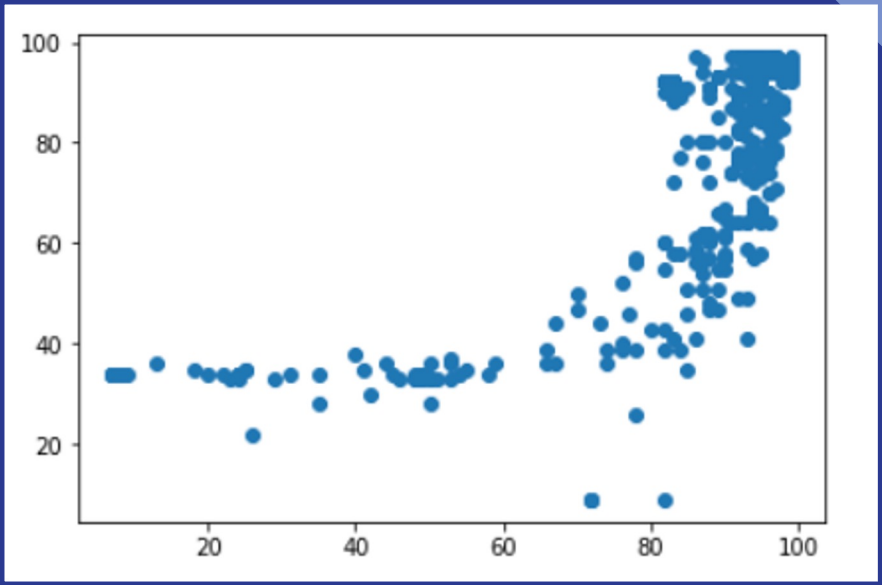
The Cost of Cyber Attacks on Businesses. https://www.solvereone.com/cost-of-cyber-attacks-on-businesses/

Appendix: Levels of Floors and Distributions of Level 0 Machines



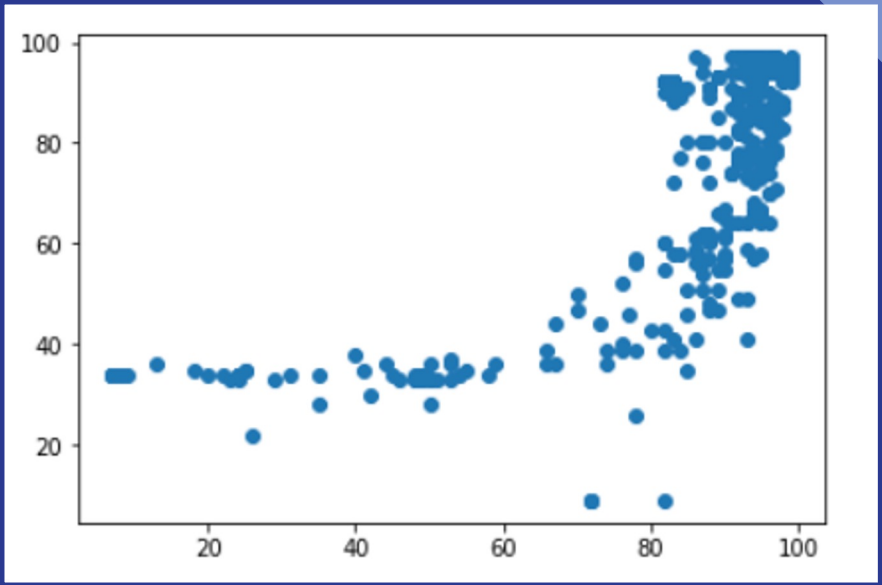
Distribution of level 0 machines on floor 1

Appendix: Levels of Floors and Distributions of Level 0 Machines



Distribution of level 0 machines on floor 2

Appendix: Levels of Floors and Distributions of Level 0 Machines



Distribution of level 0 machines on floor 3