

AWS Machine Learning Security System

Overview

Developed a real-time intruder detection system using AWS cloud services for video streaming, machine learning-based person detection, data storage, and automated alerts. This system ensures real-time monitoring, and automated security notifications using a serverless architecture.

Tech Stack

- **Video Streaming & Processing:** Laptop Webcam, Amazon Kinesis Video Stream
 - **Compute & Storage:** Amazon EC2, Amazon S3 (for backup & detections)
 - **Machine Learning:** Amazon Rekognition (for person detection)
 - **Database & Notifications:** Amazon DynamoDB, Amazon SNS (for alerts)
 - **Security & IAM:** AWS Identity and Access Management (IAM)
-

Implementation & Responsibilities

1. Real-Time Video Streaming Setup (Producer)

- Configured Amazon Kinesis Video Streams to process a live webcam feed.
- Developed a producer pipeline to **securely** publish video data to Kinesis.
- Created an IAM user with AmazonKinesisVideoStreamFullAccess permissions.
- Utilized GStreamer (gst-launch-1.0) to optimize video encoding & streaming parameters.

bash

```
gst-launch-1.0 v4l2src do-timestamp=TRUE device=/dev/video0 !  
videoconvert !  
video/x-raw,format=I420,width=640,height=480,framerate=30/1 ! x264enc  
bframes=0 key-int-max=45 bitrate=500 !  
video/x-h264,stream-format=avc,alignment=au,profile=baseline !  
kvssink stream-name='Intruder-detection-video-stream'  
storage-size=512 access-key='ACCESS_KEY' secret-key='SECRET_KEY'  
aws-region='us-east-1'
```

AWS Machine Learning Security System

2. Data Backup & Storage (Consumer #1: Backup System)

- Deployed an Amazon EC2 instance (Ubuntu, t2.medium) for processing backups.
 - Set up an S3 bucket (brian-intruder-detection-bucket) to store video frames.
 - Created an IAM role for secure interaction between EC2, Kinesis, and S3.
 - Implemented a Python-based backup solution to store all streamed frames in Amazon S3.
-

3. Intruder Detection & Alerts (Consumer #2: AI-powered Detection System)

- Amazon Rekognition processes video frames for real-time person detection.
- Detection data is stored in Amazon DynamoDB and Amazon S3.
- Configured Amazon SNS to trigger immediate alerts upon intrusion detection.
- S3 event notifications invoke SNS, sending email alerts to the homeowner.

SNS Topic Policy (Example)

json

```
{
  "Version": "2012-10-17",
  "Id": "SNS-Permission",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "s3.amazonaws.com" },
      "Action": [ "SNS:Publish" ],
      "Resource":
"arn:aws:sns:us-east-1:145023139842:intruder-detection-sns",
      "Condition": {
        "ArnLike": { "aws:SourceArn":
"arn:aws:s3:::brian-intruder-detection-bucket" },
        "StringEquals": { "aws:SourceAccount": "145023139842" }
      }
    }
  ]
}
```

AWS Machine Learning Security System

End-to-End System Workflow

- Producer: Streams live video from the webcam to Amazon Kinesis Video Streams.
 - Consumer 1 (Backup): Stores every frame securely in Amazon S3.
 - Consumer 2 (Intruder Detection): Uses Amazon Rekognition to analyze frames, logs detections in DynamoDB & S3, and triggers real-time alerts via Amazon SNS.
-

Key Impact

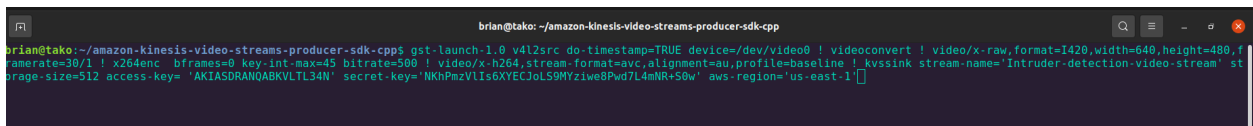
- **Enhanced Security:** Real-time intrusion detection with automated alerts.
 - **Scalable & Serverless:** Leverages AWS managed services to minimize operational overhead.
 - **Data Redundancy:** Ensures backup storage for forensic analysis.
 - **IAM Best Practices:** Secure AWS resource access using least privilege policies.
-

Conclusion

This project showcases cloud security, machine learning, and real-time streaming.

A couple of screenshots to prove it's working!

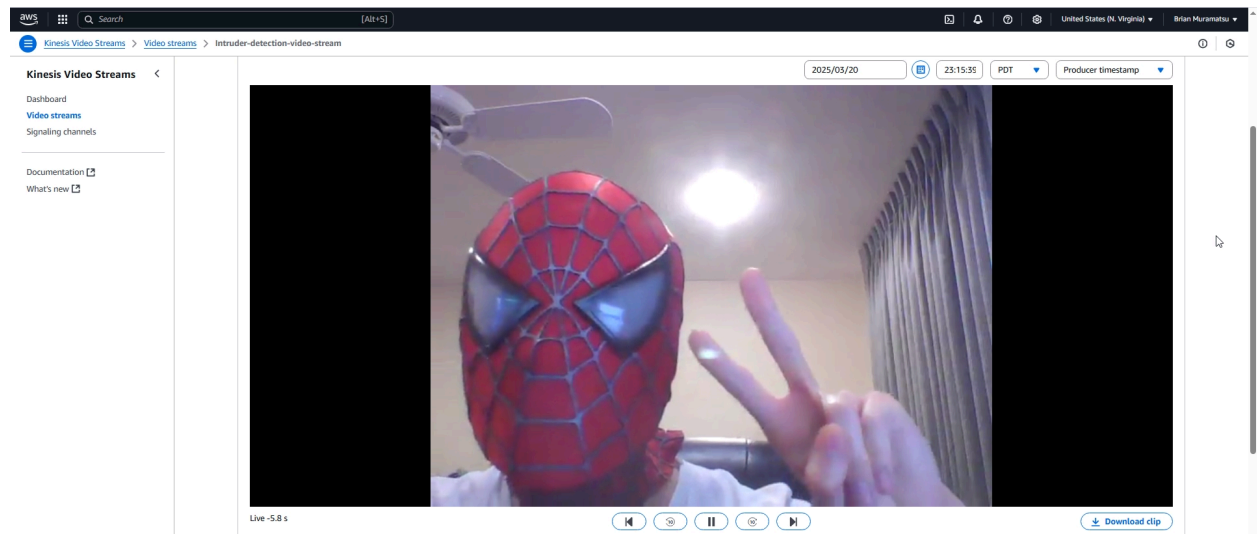
Starting the video stream:



```
brian@tako: ~/amazon-kinesis-video-streams-producer-sdk-cpp
brian@tako:~/amazon-kinesis-video-streams-producer-sdk-cpp$ gst-launch-1.0 v4l2src do-timestamp=TRUE device=/dev/video0 ! videoconvert ! video/x-raw,format=i420,width=640,height=480,framerate=30/1 ! x264enc bframes=0 key-int-max=45 bitrate=300 ! video/x-h264,stream-format=avc,alignment=au,profile=baseline ! kvssink stream-name='intruder-detection-video-stream' st
orage-size=512 access-key='AKIASDRANQABKVLTL34N' secret-key='NKhPmzVLI6XYECJolS9MYziwe8Pw7L4mNR+S9w' aws-region='us-east-1'
```

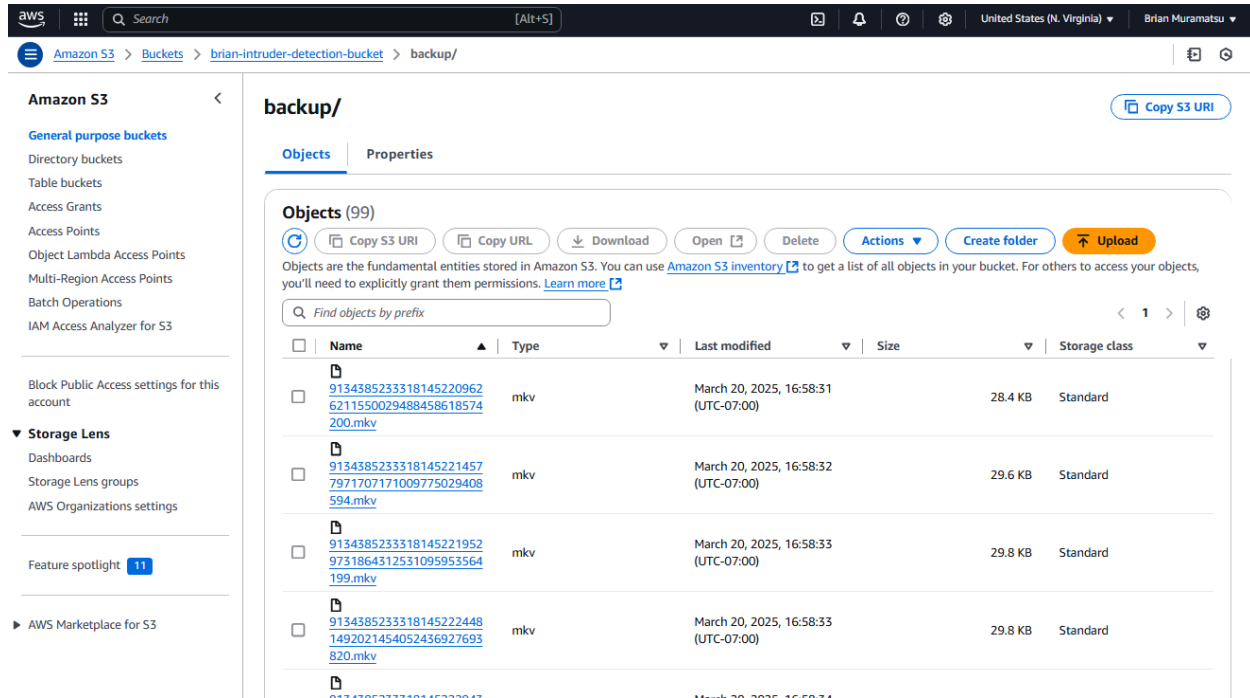
AWS Machine Learning Security System

Real time detection using AWS Kinesis Video Streams:

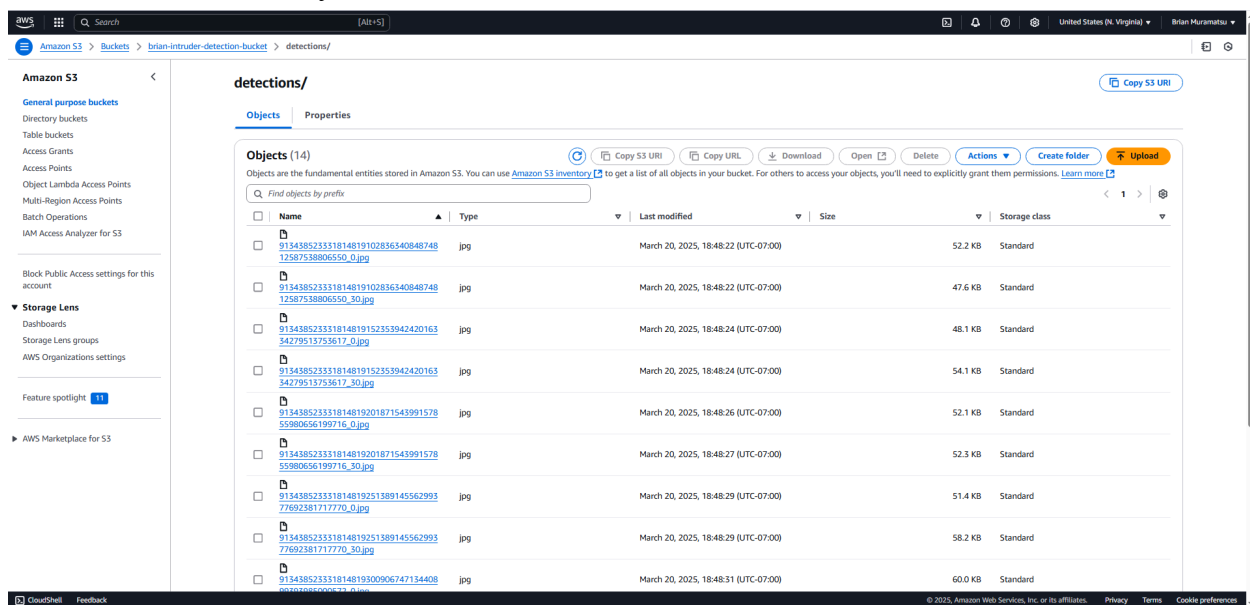


AWS Machine Learning Security System

AWS detection backup folder for backing up all the information from the producer:

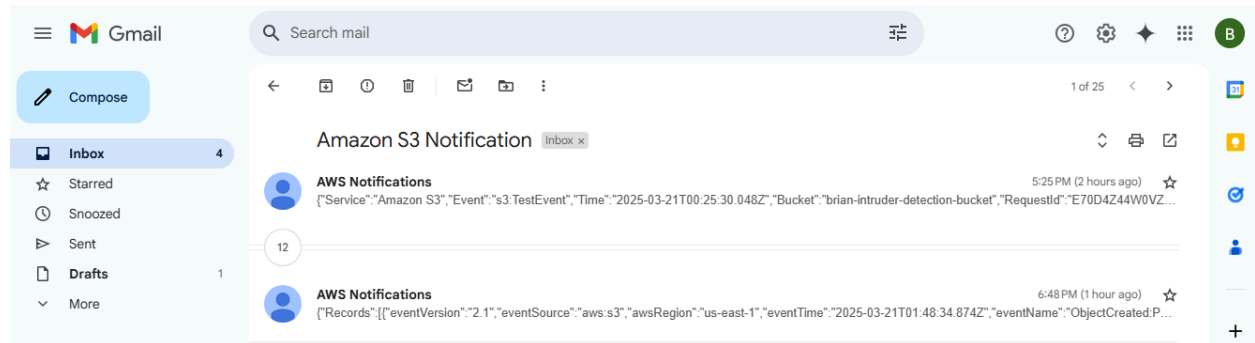


Detections folder actually deal with the intrusion detection:



AWS Machine Learning Security System

Real time notifications from Amazon S3:



Conclusion:

It works!

REFERENCES:

[amazon-kinesis-video-streams-producer-sdk-cpp](#)

[What is Amazon Kinesis Video Streams?](#)

[What is Amazon SNS?](#)

[What is Amazon Rekognition?](#)

[Security best practices in IAM](#)