**Mini Project Report on**



**Secure Framework for IoT Enabled Applications**



**Submitted in partial fulfillment of the requirement for the award of the degree of**

**BACHELOR OF TECHNOLOGY**

**IN**

**COMPUTER SCIENCE & ENGINEERING**

**Submitted by:**

**Student Name** **University Roll No.**

**Gorisha Babbar 2018812**

***Under the Mentorship of***

**Dr. Neha Garg**

**Professor**



**Department of Computer Science and Engineering**

**Graphic Era (Deemed to be University)**

**Dehradun, Uttarakhand**

**January-2024**

GEU logo

**CANDIDATE’S DECLARATION**

I hereby certify that the work which is being presented in the project report entitled **“Secure Framework for IoT enabled applications”** in partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology in Computer Science and Engineeringof the Graphic Era (Deemed to be University), Dehradun shall be carried out by the under the mentorship of **Dr. Neha Garg, Professor**, Department of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun.

Name : Gorisha Babbar University Roll no: 2018812

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **Chapter No.** | **Description** | **Page No.** |
| Chapter 1 | Introduction | **1** |
| Chapter 2 | Literature Survey | **4** |
| Chapter 3 | Methodology | **6** |
| Chapter 4 | Result and Discussion | **10** |
| Chapter 5 | Conclusion and Future Work | **11** |
|  | References | **12** |

**Chapter 1**

**Introduction**

A security framework, as it pertains to Internet of Things security cameras, is a thorough method of protecting the camera and the data it collects from any attacks. Strong authentication and authorization procedures to manage access, communication channel encryption to safeguard data while it's being transferred, secure boot implementation, and firmware integrity checks to stop unwanted tampering are all included in this framework. A comprehensive approach also incorporates data privacy concerns, industry standard compliance, and network security measures. In order to address potential vulnerabilities and guarantee the confidentiality, integrity, and availability of the device and its data, incident response plans, physical security features, and user education all work together to strengthen the security posture of the security camera. In this project we aim to develop a smart IoT based security framework to detect intrusion.

* 1. **Need for Smart CCTV Cameras**

CCTV cameras nowadays have become a common practice at every store front, home, businesses, in fact, governments around the globe have been implementing more and more surveillance and cameras to detect and prevent crimes as well as be helpful in tracking suspicious activities all around the world. This has led to a increased use of cameras all around the globe

Cameras being electronic devices can be made to include small computers like Raspberry Pi, to enhance their functionality and turning them into fully functional Internet of Things enabled devices. Such a device could prove to be really helpful, rather than a traditional CCTV camera.

Current CCTV cameras are generally useful only after a certain mishap has already happened rather than prevention of such things. Although there are dedicated staff to watch over the live footage from the cameras, human oversight is a common mistake, and it also incurs heavy costs for the businesses to have the appropriate manpower to do something like this.

In this project we will be working with Face Detection models and Utilize it to detect whether a given person on the screen is a known entity or an intruder in real time using Machine Learning Libraries like OpenCV coupled with IoT devices to create a security framework based on IoT.

**1.2 Objective**

By integrating intrusion detection with smart cameras, security surveillance can be improved by utilizing state-of-the-art technology. These smart cameras keep an eye on their surroundings all the time by utilizing cutting-edge technologies like object recognition and motion analysis. The smart cameras immediately send out notifications or initiate automated replies in the event that they discover odd or unlawful activity, such as movements that seem suspicious or unidentified individuals. By utilizing real-time visual analytics and artificial intelligence for improved intrusion detection capabilities, smart cameras become an invaluable asset in protecting a range of environments, from homes to commercial spaces, by enabling a prompt response to potential security threats.

In this project, we will be utilizing a machine learning model, included in the Dlib Library as well as OpenCV library for face recognition and classification purpose. After training the model we have stored the face detection model in a file. Then we have employed a SQLite based database to store the faces of known entities which will be used to provide reference to whether a given person is an intruder or a known entity.

The model is designed to take the image of person and classify the features of the face such as lips, eyes , color, ratios of various parts, into numerical values, which are later used to trace back to the current live feed of what is being shown on camera to determine whether a person on the camera is an intruder or a known entity.

**1.3 Applications**

There are many different industries in which an intrusion detection system with smart cameras is used. By spotting unusual activity and instantly notifying security staff, this device can help reduce theft in retail settings. Smart cameras help ensure worker safety in industrial environments by identifying risky activities or unlawful entry to restricted areas. Furthermore, these frameworks improve public safety in smart cities by promptly identifying possible security concerns in busy areas or vital facilities. This framework's adaptability makes it a useful tool in a variety of settings, where the addition of smart cameras strengthens security protocols and encourages a quicker, more organized response to possible incursions and security problems.

Moreover, integrating smart cameras with intrusion detection systems is essential for enhancing emergency response capabilities. Rapidly identifying suspicious activity can help with prompt reactions to possible security breaches in essential infrastructure, including airports or transportation hubs, reducing risks and guaranteeing public safety. Furthermore, in residential settings, real-time monitoring and alarms provided by smart home security systems outfitted with these frameworks give homeowners peace of mind and improve overall property protection. The significance of employing smart cameras in intrusion detection systems to strengthen security measures and create safer settings in both public and private realms is highlighted by their extensive applicability, particularly as technology advances.

**Chapter 2**

**Literature Survey**

# **Scalable machine learning-based intrusion detection system for IoT-enabled smart cities**

Publication Year: 2019

Author: [Sandeep Pirbhula](https://ieeexplore.ieee.org/author/37085687333)l et al.

Journal Name: [2019 13th International Conference on Sensing Technology (ICST)](https://ieeexplore.ieee.org/xpl/conhome/9039856/proceeding)

Summary: The paper [1] explores innovative approaches to enhance security in urban environments. The focus is on leveraging machine learning techniques to detect and prevent intrusions effectively. The research, presented at the 2019 13th International Conference on Sensing Technology (ICST), emphasizes the importance of scalable solutions for the evolving challenges of securing interconnected IoT devices in smart cities.

# **Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System**

Publication Year: 2022

Author: Mohd Husanain, et al.

Journal Name: Security and Privacy of sensor and actuator network

Summary: This Journal [2] addresses the prevention of MQTT vulnerabilities through an IoT-enabled intrusion detection system. Focused on the security and privacy of sensor and actuator networks, the paper emphasizes the importance of safeguarding MQTT (Message Queuing Telemetry Transport) protocols in the context of IoT. The authors propose strategies to mitigate vulnerabilities and enhance the overall security of IoT systems, highlighting the significance of proactive measures against potential threats in sensor and actuator networks.

# **Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks**

Publication Year: 2022

Author: Rajasekhar Chaganti et.al

Journal Name: Enhanced Cyber-Physical Security in IoT

Summary: The journal[3] discusses a deep learning approach for an SDN (Software-Defined Networking)-enabled intrusion detection system in IoT networks. Focused on enhancing cyber-physical security in IoT, the paper explores the application of deep learning techniques to strengthen intrusion detection capabilities. The authors emphasize the integration of SDN principles to improve the efficiency and adaptability of the intrusion detection system within IoT networks. The research contributes to the ongoing efforts to bolster cybersecurity measures in the rapidly evolving landscape of IoT-enabled systems.

**Summary of Literature Survey:**

All together, these evaluations of the literature explore state-of-the-art developments in intrusion detection systems in the context of IoT-enabled environments. In order to secure smart cities, they concentrate on scalable machine learning approaches, highlighting the necessity of flexible solutions in the face of changing IoT problems. In order to address the vulnerabilities in MQTT, the second review suggests an intrusion detection system that is enabled by the Internet of Things. This emphasizes how important it is to protect communication protocols in sensor and actuator networks. The third review, which concludes, investigates a deep learning strategy for intrusion detection in Internet of Things networks that is combined with Software-Defined Networking (SDN). This study highlights the use of cutting-edge technology to strengthen intrusion detection capabilities and improve overall cybersecurity measures in the dynamic IoT-enabled ecosystem, adding to the larger picture of increased cyber-physical security in IoT.

**Chapter 3**

**Methodology**

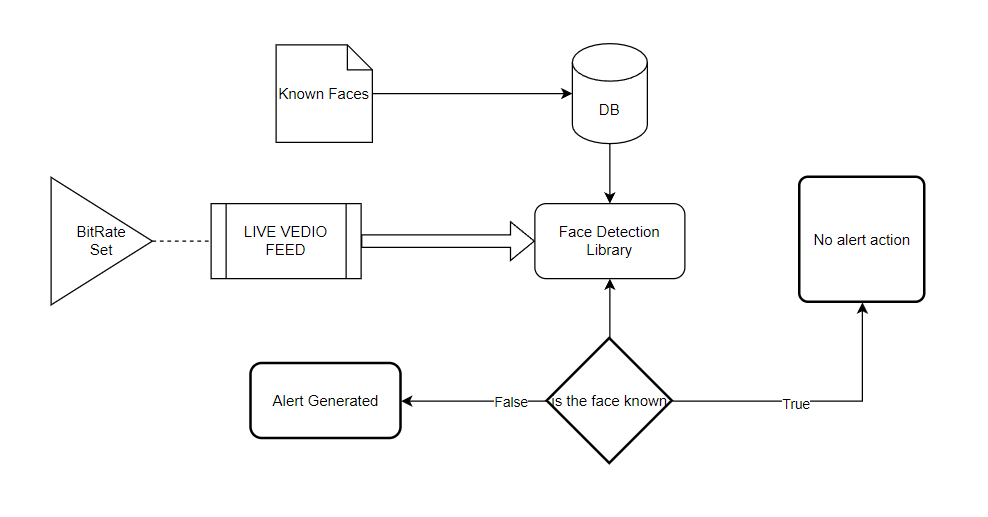
**3.1 Tools and Technologies Used**

**Python :** Python is the language being used for this project. This is due to its many community-based characteristics, such as the fact that it has a wealth of potent tools available for scientific computing packages. Pandas and NumPy are two well-known and free software packages. These packages will drastically reduce and vary the amount of code required to create a certain program. Repetition becomes quick and effective as a result. The code written is shorter and easy to write. Hence Python was best suited for the project.

**Jupyter Notebook :** Users can create and share documents with live code, equations, visualizations, and narrative text using the interactive computing environment of Jupyter Notebook[5]. Its ability to handle many programming languages makes it a flexible tool for scientific research, machine learning, data analysis, and visualization. Users may describe their workflow, analyze data, and run code cells in real-time. Data scientists, academics, and educators choose Jupyter Notebook because it combines explanatory text with code to encourage repeatability and cooperation. It is an indispensable tool for data exploration and experimentation due to its intuitive interface and broad library support.

**OpenCV :** A popular open-source computer vision and machine learning library in the domains of robotics, image processing, and computer vision is called OpenCV (Open Source Computer Vision). Designed in C++, OpenCV offers a wide range of tools and features for real-time computer vision applications, with interfaces available for Python and other programming languages.

**3.2 Proposed Workflow**

****

**Figure 3.2.1** Proposed System Architecture and Workflow

The Proposed workflow of the Model can be divided into two parts : -

1. Adding Known Faces to the DataBase for Later Recognition
2. Utilizing the Database for application to live intrusion detection

The system presented here composes of five modules:-

1. Live Video Feed

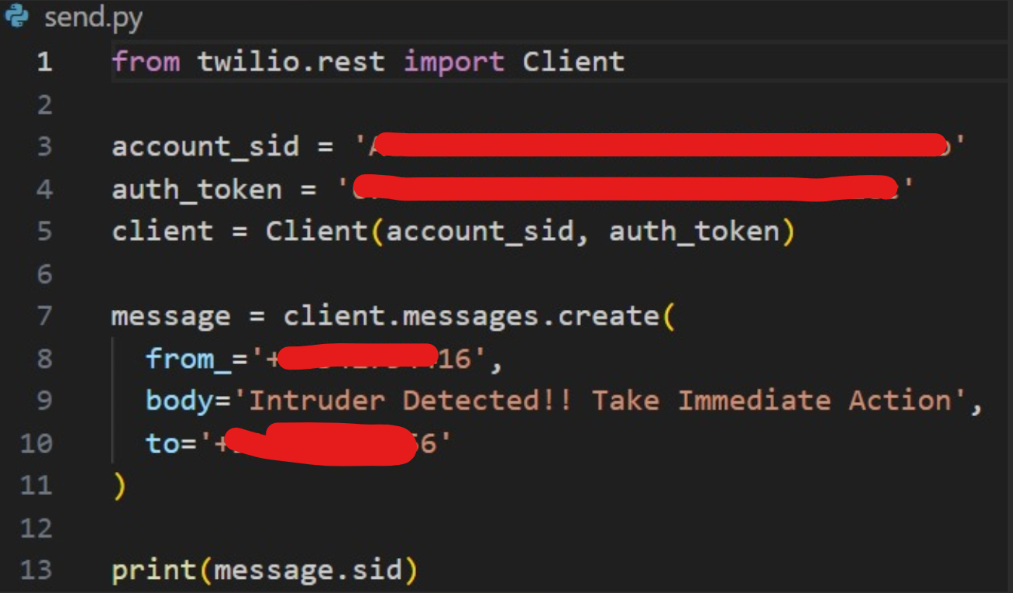
2. Database call

3. ML Model Called (Face Detection Library)

4. Exhaust all Database Entries

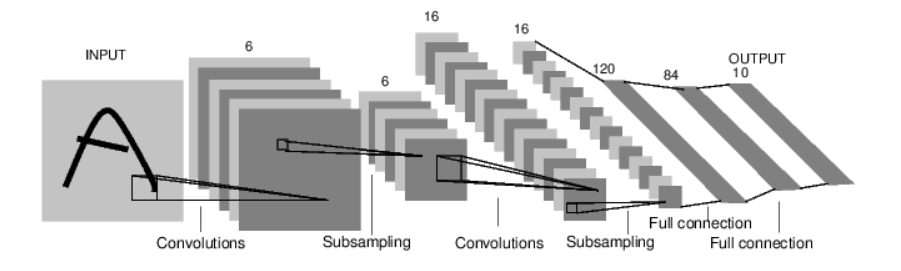
5. Output as Predicted Result (SMS Alert Generation)

For image classification and face recognition models from DLib namely, HOG Face Recognition has been used, which has been trained on extensive image data achieving an efficiency of above 90 on the test data. [6]



**Figure 3.2.2** Code for API call following Intruder Detection leading giving immediate alert

**3.3 Face Recognition Model Architecture**

****

**Figure 3.3.1** DLib Face Recognition Model Architecture [7]

Popular open-source library Dlib offers capabilities for computer vision, facial recognition, and machine learning. Dlib uses a potent face recognition model based on deep learning techniques in the context of face identification. Convolutional Neural Networks (CNNs) and Residual Networks (ResNets) are combined to train the face recognition model using a sizable dataset of annotated facial photos.

The primary phases in Dlib's face recognition procedure start with employing an object detector based on the Histogram of Oriented Gradients (HOG) feature to identify faces in an input image. After faces are identified, a shape predictor model is used to locate the facial landmarks, such as the mouth, nose, and eyes. These landmarks are essential for aligning faces so that features may be extracted consistently.

Next, Dlib uses a deep neural network to extract a descriptor—a numerical representation of facial features—from the aligned faces. The descriptor is resilient to changes in lighting, posture, and facial emotions while capturing crucial information about the distinctive qualities of the face.

Dlib compares the input face's descriptors with those in a known face database during the recognition stage. To determine which descriptor is most likely to match, the library uses metric learning algorithms to measure the similarity of descriptors. Since Dlib's facial recognition technology has proven successful in practical settings, it is a well-liked option for applications like biometrics, security systems, and human-computer interaction.

**Chapter 4**

**Result and Discussion**

By following the described methodology, a fully functional Intrusion Detection System for Internet of Things(IoT) enabled camera feed was deployed, capable of detecting intruding faces in a live stream and using Twilio API delivering a fast and secure message to the respondent via SMS.



**Figure 4.1** SMS sent by Twilio API on intrusion detection

As we can see, the project is able to send text messages to the mobile of the respondent and also stores the photograph of the intruder creating a secure environment which can be used from houses to businesses alike for maximizing security through installation of smart cameras.

**Chapter 5**

**Conclusion and Future Work**

Through this project, I have developed a system that can process and identify if a person visiting a camera is a intruder or a known person and give alert to the user immediately. It also stores a database with the names of all the known persons which can also be added to later on. For better portability we have used SQLite which is not a standalone application and comes embedded with the latest version of Python ensuring the code runs on IoT platforms like smart camera.

Although this model was fairly accurate on test data, and performs very well in such scenarios it is still not a hundred percent fool proof and is prone to error. A human along with such a detection system could greatly aid the human as well as the overall accuracy and crime detection on crime scene.

There are numerous directions to take in order to improve the intrusion detection system in the future. Enhancing the system's resilience in difficult situations, such dim lighting or obscured vistas, might be a top concern. Furthermore, adding machine learning models for behavior analysis and anomaly detection could improve the system's capacity to discern between legitimate activity and possible dangers.

Additionally, investigating the integration of edge computing technologies to locally analyze data on smart cameras can help lower latency and improve responsiveness of the system. Working along with other cutting-edge technologies, such as cloud-based services and the Internet of Things (IoT), may create new opportunities for scalability and remote monitoring.

**References**

[1]Sandeep Pirbhulal, et al. "Scalable machine learning-based intrusion detection system for IoT-enabled smart cities." 2019 13th International Conference on Sensing Technology (ICST).

[2]Mohd Husanain, et al. "Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System." Journal of Security and Privacy of Sensor and Actuator Network.

[3] Rajasekhar Chaganti, et al. "Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks." Journal of Enhanced Cyber-Physical Security in IoT, 2022.

[4] Project Jupyter.” https://www.jupyter.org (accessed December. 23, 2023).

[5]OpenCV: Open computer vision library — https://opencv.org/ (accessed December. 29, 2023).

[6]face\_recognition (github): https://github.com/ageitgey/face\_recognition (accessed November. 18, 2023).

[7] DLib C++ Library : source : http://dlib.net/ (accessed November. 20, 2023).