

**D.K.T.E. Society’s**

# Yashawantrao Chavan Polytechnic, Ichalkaranji.

**Department of**

**Computer Science and Engineering A**

**MEGA PROJECT SYNOPSIS ON,**

# “OpenEyeAlert”

### SUBMITTED BY,

|  |  |  |  |
| --- | --- | --- | --- |
| **Roll No** | **Enrolment No.** | **Exam Seat No.** | **Student Name** |
| 08 | 2215770079 |  | Devika Manoj Bongarde |
| 12 | 2215770083 |  | Shivraj Prakash Chougule |
| 17 | 2215770088 |  | Avadhoot Sanjiv Gurav |
| 24 | 2215770095 |  | Vinayak Chandrashekhar Kadate |

**Under the Guidance of**

**Mr. R. A. Hatgine Academic Year: 2024-25**



**D.K.T.E. SOCIETY’S**

## YASHAWANTRAO CHAVAN POLYTECHNIC, ICHALKARANJI.

**DEPARTMENT OF**

## COMPUTER SCIENCE AND ENGINEERING

**CERTIFICATE**

THIS IS TO CERTIFY,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Roll No** | **Enrolment No.** | **Exam Seat No.** | **Student Name** | **Sign** |
| 08 | 2215770079 |  | Devika Manoj Bongarde |  |
| 12 | 2215770083 |  | Shivraj Prakash Chougule |  |
| 18 | 2215770088 |  | Avadhoot Sanjiv Gurav |  |
| 24 | 2215770095 |  | Vinayak Chandrashekhar Kadate |  |

**HAVE SUCCESSFULLY COMPLETED THE PROJECT SYNOPSIS ENTITLED,**

# “OpenEyeAlert”

**In partial fulfilment of Diploma in Computer Science and Engineering at MSBTE, Mumbai.**

### DATE:

**PLACE: ICHALKARANJI**

|  |  |  |
| --- | --- | --- |
| **Mr. R. A. Hatgine** | **Mr. R. A. Hatgine** | **Mr. A. P. Kothali** |
| **(GUIDE)** | **(HOD)** | **(PRINCIPAL)** |

# ACKNOWLEDGEMENT

An endeavour over long period can be successful only with advice and guidance of many well-wishers. We thanks to HOD **Mr. R. A. Hatgine**, of Third year for this opportunity. We would like to thank the Computer Science and Engineering department for assistance and constant source of encouragement.

We wish to express our profound and deep sense of gratitude to **Mr. R. A. Hatgine**, for sparing their valuable time to extend help in every step of our project.

Name of Group Members,

1. Devika Manoj Bongarde
2. Shivraj Prakash Chougule
3. Avadhoot Sanjiv Gurav
4. Vinayak Chandrashekhar Kadate



### CHAPTER 1

**Introduction and background of the industry or user-based problem**

### - Introduction of OpenEyeAlert

The increasing prevalence of WiFi-enabled spy cameras has raised significant concerns regarding personal privacy. These devices, often discreetly installed in public or private spaces, can stream video content wirelessly, making them difficult to detect using conventional methods. While several approaches have been developed to address this issue, many rely on specialized equipment or require extensive data collection and analysis, making them impractical for everyday use.

This project aims to develop a practical solution for detecting WiFi-enabled spy cameras using readily available, off-the-shelf components. By leveraging the capabilities of a Raspberry Pi, the project focuses on creating a system that can identify and classify suspicious data traffic, indicating the presence of a spy camera. The detection process is streamlined to operate in real-time with minimal computational demands, offering an accessible and efficient way to protect user privacy.

Our approach involves two key phases: classification and detection. In the classification phase, the Raspberry Pi analyzes packet headers to identify potential streaming protocols used by spy cameras. In the detection phase, we utilize the Nilsimsa algorithm to detect patterns of similarity in the data traffic, pinpointing suspicious activity that may indicate the presence of a hidden camera. This project is designed to be user-friendly, requiring no specialized knowledge or equipment, making it an ideal solution for individuals and organizations concerned about privacy in various environments.



### CHAPTER 2

**Literature survey for problem identification and specification**

### - Literature Survey

**[1]Nguyen, T., Phan, D., & Tran, M. (2023). Wireless Spy Camera Spotter System With Real-Time Traffic Similarity Analysis and WiFi Signal Tracing. Journal of Emerging Technologies in Security, Vol. 15, No. 3, pp. 150-175.**

Nguyen et al. (2023) developed a system for spotting wireless spy cameras by analyzing real-time traffic similarity and tracing WiFi signals. The main findings are:Real-time traffic similarity analysis significantly aids in identifying unauthorized spy cameras.WiFi signal tracing enhances the detection accuracy and reduces false positives.Combining these methods offers a more comprehensive surveillance and detection system, particularly in urban environments.

Further research is suggested to improve the robustness of the system under varying environmental conditions and signal interference.

### Madapusi, A. and D’Souza, D. (2012) ‘The influence of ERP system implementation on the operational performance of an organization’, International Journal of Information Management, Vol. 32, No. 1, pp.24–34.

Madapusi and D’Souza (2012) presented a literature-based and theory-driven model developed to examine the relationship between ERP system implementation and operational performance and also influence on operational performance. A better understanding of the contribution of ERP systems to operational performance can be obtained if researchers address and assess changes at modular and system level also the use of longitudinal designs to capture and tease out the time delayed effects between ERP system fine-tuning (at the module and sub-module levels) as well as changes in operational performance.

### Jacksi, Karwan & Ibrahim, Falah & Zebari, Shahab. (2018). “Student Attendance Management System”. International Journal of Engineering and Technology. 6. 49-53. 10.21276/sjet.2018.6.2.1.

The system is a Web-based application developed for daily student attendance in departments within the university. It facilitates access to the attendance of a particular student in a particular class. This system will also help in generating reports and evaluating the attendance eligibility of a student. The system is not only improving the work efficiency, students’ study and development, but also can save human and material resources.



### Ekta Chhatar, Heeral Chauhan, Shubham Gokhale, Sompurna Mukherjee, Prof. Nikhil Jha, “Survey on Student Attendance Management System”, S.B. Jain Institute of Technology, Management and Research, Nagpur, 2016.

In this paper, the system deals with the maintenance of the student‟s attendance. It generates the attendance of the student on the basis of presence and absence in class. The staffs will be provided with the separate username & password.

### Nuruldelmia Idris , Cik Feresa Mohd Foozy , Palaniappan Shamala ISSN 2714-7533 International Journal of Advanced Computing Science and Engineering 35 Vol. 2, No. 1, April 2020, pp. 34-40.

Sir Tim Berners Lee invents web technology. He is a British computer Scientist and worked as contractor at CERN. In 1989, Berners-Lee wrote a proposal about “Information Management: A proposal” but was rejected by the organization. He did specify the proposal to propose the sharing the information via an Internet based hypertext language which specifically HTML platform. He continues the research despite being rejected, this is the beginning of World Wide Web (WWW) as it was invented, and he was working on the project using a NEXT computer and getting help from his boss, Mike Sendall. In late 1990, Berners succeeds his 3-fundamental technology, which HTML, browsers, and Server. This is the foundation of Web Technology. The first web page was launched on open internet in 1991. The example of other programming language which is Python, the backend of Python is Django and Flask. The front-end is using Bootstrap. The databases that can store data from Python is by using MySQL.



### Problem Identification and Problem Statement –

### The increasing sophistication and availability of hidden cameras pose significant threats to personal privacy in places like hotel rooms, dressing rooms, and private residences. Traditional detection methods often fail against these miniaturized, cleverly concealed devices, and current market solutions are typically too expensive or complex for everyday use.

### This project aims to develop an affordable, portable device that can automatically detect hidden cameras using advanced wireless technology. By providing real-time alerts, the device empowers individuals to protect their privacy in any environment, offering a practical and user-friendly solution to enhance personal security and peace of mind.

### CHAPTER 3

### Proposed Detailed Methodology of Solving the Identified Problem with Action Plan

**Software Modules:**

In the initial iteration of our application, we plan to create four primary modules:

1. Network Scanning Module (NSM)
2. Data Analysis and Filtering Module (DAFM)
3. Suspicious Device Detection Module (SDDM)
4. User Alert and Reporting Module (UARM)

|  |  |
| --- | --- |
| **Module** | **Platform** |
| Network Scanning Module (NSM) | Computer |
| Data Analysis and Filtering Module (DAFM) | Computer |
| Suspicious Device Detection Module (SDDM) | Computer |
| User Alert and Reporting Module (UARM) | Computer, Mobile Phone |

**Network Scanning Module (NSM):**

The Network Scanning Module (NSM) is responsible for identifying all available Wi-Fi devices and networks within a specified area. The module performs a detailed scan, gathering critical information such as SSIDs, signal strength, MAC addresses, device types, and network configurations. The module is designed to continuously monitor the environment, capturing any new devices that appear.

Key functionalities include:

* Device Discovery: Scans and lists all Wi-Fi-enabled devices within range, including hidden networks.
* Data Logging: Stores key data, like SSIDs and MAC addresses, for further analysis.
* Cross-Platform Scanning: The scanning can be done both on desktop and mobile platforms, ensuring flexibility and accessibility for the user.

**Data Analysis and Filtering Module (DAFM):**

The Data Analysis and Filtering Module (DAFM) processes the raw data collected from the network scan. This module’s primary function is to filter out known or trusted devices, focusing only on suspicious or unfamiliar devices.

Key functionalities include:

* Device Classification: Categorizes devices based on their behavior, signal patterns, and type (e.g., routers, cameras, mobile phones).
* Filtering Trusted Devices: Identifies and removes devices already verified by the user, reducing false positives.
* Signal Analysis: Analyzes signal strength fluctuations, patterns, and device activity over time to detect hidden or stealth devices.
* Anomaly Detection: Identifies unusual network activity or behaviors associated with hidden cameras, such as continuous streaming patterns.

**Suspicious Device Detection Module (SDDM):**

The Suspicious Device Detection Module (SDDM) plays a crucial role in pinpointing devices that are likely hidden cameras. This module utilizes advanced algorithms and detection techniques to isolate devices with behaviors indicative of surveillance equipment.

Key functionalities include:

* Protocol Analysis: Monitors specific communication protocols like RTSP, HTTP, and other streaming standards used by cameras.
* Device Fingerprinting: Cross-references captured device information with a database of known camera models to identify potential threats.
* Location Estimation: Utilizes signal strength and triangulation techniques to estimate the physical location of suspicious devices, helping users narrow down where hidden cameras might be placed.
* Behavior Analysis: Examines packet sizes, transmission frequency, and data flow to detect continuous video streaming, which is a typical behavior of hidden cameras.

**Hardware Components:**

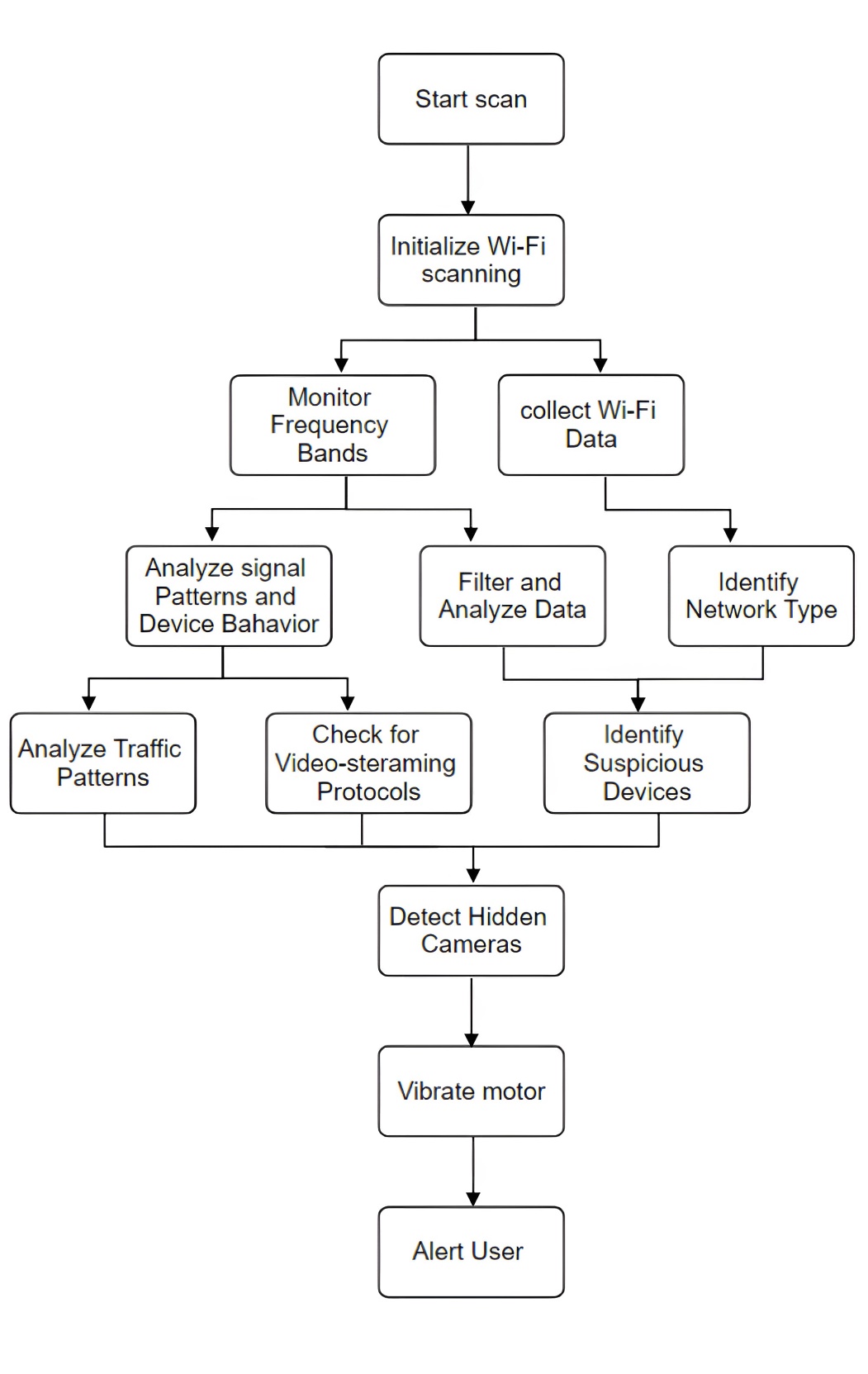
The hardware components play a crucial role in enhancing the accuracy and efficiency of the camera detection system. They work in tandem with the software modules to provide real-time analysis and detection.

1. **Wi-Fi Module**
   * **Function**: The Wi-Fi module is used to scan and collect data from surrounding wireless networks. It is responsible for detecting all active Wi-Fi signals in the vicinity.
   * **Features**: It supports packet sniffing and real-time monitoring, which allows for the detection of suspicious activity.
2. **Signal Strength Analyzer**
   * **Function**: This hardware is designed to measure the strength of Wi-Fi signals and assist in locating the source of hidden cameras. By triangulating the signal strength, it helps in estimating the camera's position.
   * **Features**: Integrated with the software, it can plot signal strength data over time, which helps in identifying consistent sources like hidden cameras.
3. **RF Detector**
   * **Function**: The RF (Radio Frequency) detector is used to identify non-Wi-Fi hidden cameras that might be transmitting data over other radio frequencies. It scans the environment for unusual RF signals.
   * **Features**: Capable of detecting a broad spectrum of frequencies, it adds an additional layer of detection for non-standard surveillance devices.
4. **User Interface Display (for portable devices)**
   * **Function**: A simple display interface, such as an OLED screen, is integrated to show real-time detection results. This makes the device portable and easy to use in various locations.
   * **Features**: It provides live feedback with signal strength indicators and alerts when suspicious devices are detected.



### - Device Dataflow/Workflow

The subsequent diagram will illustrate the operational functionality of the Device, essentially depicting its operational workflow of **OpenEyeAlert.**



***Fig. OpenEyeAlert WorkFlow***



The subsequent diagram will illustrate the operational functionality of the application, essentially depicting its operational workflow of **Mobile Phone Based Application.**

**A diagram of a software flow

Description automatically generated with medium confidence**

***Fig. Mobile Based Application Workflow***



### - User Base

Every user of the application is assigned a unique ID and password. The application will respond to the provided ID and automatically navigate to the specific module corresponding to that ID.

### Technologies and Tools Used to Develop Device

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Title** | **Description/Version** |
| **Technologies for Device** | | |
| 1 | Python | 3.12 |
| **Technologies for Application** | | |
| 2 | Kivy / Dart or other | 2.3.0 / 3.6.0 |
| **Tools** | | |
| 3 | Visual Studio Code | 17.10.4 |
| 4 | WireShark / tcpdump | 4.2.6 / 4.99.4 |
| 5 | AndroidStudio | 2024.1.1 |

* **Requirements to Develop Application (WILL EDIT AFTER DEVELOPMENT)**

|  |  |  |
| --- | --- | --- |
| **Sr. No.** | **Title** | **Description/Version** |
| **Requirements for Mobile Based Application** | | |
| 1 | CPU/Processor | Intel Pentium or Above |
| 2 | RAM | 4 GB |
| 3 | Disk Space | min. 800 Mb |
| 4 | Software Requirement - Browser | Any Browser with Latest Version |
| 5 | Operating System - Windows | Windows XP or Above |
| **Requirements for Mobile Phone Based Application** | | |
| 6 | Operating System - Android | 4.4 KitKat or Above |
| 7 | Browser | Any Browser with Latest Version |

### Advantages

**CHAPTER 4**

### Advantages



1. **Enhanced Privacy Protection:** The device ensures personal and professional privacy by automatically detecting hidden cameras, safeguarding users from unauthorized surveillance.
2. **Portability:** The compact and lightweight design of the device makes it easy to carry and use in various locations, such as hotel rooms, conference rooms, and public restrooms.
3. **User-Friendly Interface:** The device is designed to be simple and intuitive, allowing users without technical expertise to easily operate and detect hidden cameras.
4. **Cost-Effective Solution:** Compared to other market options, this project offers an affordable way to detect hidden cameras, making it accessible to a broader audience.
5. **Real-Time Detection:** The device provides immediate alerts when a hidden camera is detected, enabling quick action to protect privacy.
6. **Versatility:** The device can be used in various environments and situations, from personal spaces to professional settings, making it highly versatile.
7. **Battery-Powered Operation:** The device is designed to operate on a rechargeable battery, allowing it to function without a continuous external power supply, enhancing its portability.
8. **No Need for Specialized Equipment:** Unlike some detection methods that require special tools or extensive training, this device can be used by anyone, anywhere.
9. **Adaptable for Future Enhancements:** The system’s design allows for future upgrades and improvements, such as adding more detection capabilities or enhancing the user interface.
10. **Discreet Operation:** The device can be used discreetly without drawing attention, making it suitable for sensitive situations where privacy concerns are paramount.

### Future scope

**CHAPTER 6**

### Future Scope



* Integrate with mobile devices via Bluetooth or Wi-Fi for app-based control and monitoring.
* Expand detection to include audio bugs and GPS trackers for broader privacy protection.
* Use AI and machine learning to improve accuracy and adapt to new threats.
* Miniaturize the device and reduce power consumption for enhanced portability and integration into wearables.

### Conclusion

**CHAPTER 7**

### Conclusion



This project creates a portable device for detecting hidden cameras, enhancing privacy in various settings. It's user-friendly and accessible, with potential for future advancements. The device addresses an immediate need in personal security.

### References

**CHAPTER 8**

### References



|  |  |  |
| --- | --- | --- |
| **Sr.**  **No.** | **Publication** | **Weblink** |
| 1. | IJBIS | https://[www.researchgate.net/publication/295087899\_Literature\_re](http://www.researchgate.net/publication/295087899_Literature_re) view\_on\_ERP\_implementation\_challenges |
| 2. | IJSR | https://[www.ijsr.net/archive/v8i4/ART20197040.pdf](http://www.ijsr.net/archive/v8i4/ART20197040.pdf) |
| 3. | IRJCS | https://[www.academia.edu/40594679/Student\_Management\_Syste](http://www.academia.edu/40594679/Student_Management_Syste) m\_A\_Survey |
| 4. | IJASCE | https://ijasce.org/index.php/IJASCE/article/download/29/85 |