BREAK-IN SURVEILLANCE USING LASER DETECTION

A PROJECT REPORT

Submitted by

DERVYN M. O. HICKMAN   -   210820106011

JOSHUA SELWYN S   -   210820106027

LUKE JONATHAN C   -   210820106035

In partial fulfillment for the award of the degree of

BACHELOR OF ENGINEERING

IN

ELECTRONICS AND COMMUNICATIONENGINEERING

KINGS ENGINEERINGCOLLEGE, CHENNAI

ANNA UNIVERSITY: CHENNAI 600025

MAY 2024

DECLARATION

We hereby declare that the project report entitled **"BREAK-IN SURVEILLANCE USING LASER DETECTION"** is submitted to the Department of Electronics and Communication Engineering in Kings Engineering College, Chennai.

Place: CHENNAI

Date:

SIGNATURE OF STUDENTS

DERVYN M. O. HICKMAN

(210820106011)

JOSHUA SELWYN S

(210820106027)

LUKE JONATHAN C

(210820106035)

ANNA UNIVERSITY : CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report **"BREAK-IN SURVEILLANCE USING LASER DETECTION"** is the Bonafide work of **DERVYN M. O. HICKMAN (210820106011), JOSHUA SELWYN S (210820106027), LUKE JONATHAN C (210820106035)** who carried out the project work under my supervision.

SIGNATURE

Dr.V.RAVICHANDRAN, M.E Ph.D

HEAD OF THE DEPARTMENT

Department Electronics and Communication

Engineering

Kings Engineering College

Irungattukottai, Sriperumbudur

SIGNATURE

Dr. S. LEKASHRI, M.E Ph.D

SUPERVISOR

Department of Electronics and

Communication Engineering

Kings Engineering College

Irungattukottai, Sriperumbudur

ACKNOWLEDGEMENT

ABSTRACT

In our technologically advanced society, **CCTV surveillance** remains the preferred choice for monitoring systems. However, inherent limitations persist, particularly in the alerting sector. These limitations inadvertently provide opportunities for burglars to carry out their nefarious intentions, even under the watchful gaze of cameras. The consequences can be dire—both for individuals directly affected and for society at large.

To address these challenges, we propose an **innovative triggering system** that discreetly notifies concerned parties when an intruder is detected, all without triggering audible alarms that might tip off the perpetrators. Our system not only alerts but also captures crucial evidence—the burglars' activities—ensuring a comprehensive security solution.

Our Break-In Surveillance model relies on a laser as the trigger switch. When motion is sensed, the laser either activates or deactivates the cameras. Unlike continuous recording, this targeted approach optimizes storage and power usage. By utilizing a laser tripwire, we ensure that the cameras engage only when necessary, thus preserving resources while maintaining vigilance.

Upon detecting an intruder, our system discreetly sends an alert message via SMS to the concerned person's smartphone. Additionally, a video alert captures the intruder's actions, providing immediate awareness. To enhance situational awareness further, we include the geographical location of the incident as a Google Map link. This empowers the concerned person to take swift action.

Our system not only benefits individuals but also supports law enforcement. By providing real-time alerts and precise location data, it streamlines police response. Imagine officers arriving at the crime scene before the intruders can escape—a game-changer in crime prevention.

Unlike 24/7 video recording, our targeted approach minimizes power consumption and storage requirements. This cost-effective model finds applications in various settings, including residences, schools, colleges, and government sectors.

In summary, our innovative triggering system bridges the gap between surveillance and action. By discreetly alerting concerned parties and capturing critical evidence, we enhance security while optimizing resources. Let us embrace technology to safeguard lives and property effectively.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1   GENERAL

In today's rapidly evolving society, where technological advancements have become synonymous with progress, the need for robust security measures has never been more paramount. While Closed-Circuit Television (CCTV) surveillance systems have become a ubiquitous presence in our daily lives, their effectiveness in thwarting criminal activities is often hampered by outdated alerting mechanisms. This critical deficiency in traditional surveillance infrastructure underscores the pressing need for innovation—a need that the Break-In Detection System seeks to address.

The Break-In Detection System represents a paradigm shift in the realm of security monitoring. By harnessing laser technology as a trigger switch, this cutting-edge system discreetly activates cameras only when motion is detected, minimizing false alarms and maximizing efficiency. Moreover, its advanced alerting features, including real-time video alerts and geospatial data sharing, empower users to respond swiftly and decisively to unauthorized intrusions. In an era defined by heightened security concerns, the Break-In Detection System emerges as a beacon of innovation, offering unparalleled protection for homes, businesses, and public spaces alike. Alarm systems, also known as burglar alarm systems, security protection systems, or intrusion detection systems, work based on similar technical principles. They utilize various sensors to detect break-ins into buildings or security areas. Additionally, methods and systems for break-in detection involve calibrating sensors, detecting external forcing applied to barriers, and setting energy threshold

values to identify abnormal behavior. Brake failure detection systems, which use sensors and monitoring software, are designed to identify problems with braking systems and alert drivers or operators to prevent accidents. Overall, innovative approaches like the Break-In Detection System play a crucial role in enhancing security and safeguarding our communities.

1.2   OBJECTIVE

The primary goal of this project is to design and implement an exceptionally efficient surveillance system. Leveraging a sophisticated LASER-LDR (Light Dependent Resistor) setup as a trigger mechanism, our system ensures that cameras activate only when motion is detected within the monitored area. Unlike conventional surveillance systems, notorious for their false alarms and inefficient alerting mechanisms, our approach prioritizes discretion and effectiveness. By minimizing the risk of intruders becoming aware of their detection, we enhance overall security.

In addition to motion-triggered camera activation, we envision incorporating an (SMS) alert feature. This real-time notification system will promptly inform designated individuals via their smartphones in the event of unauthorized intrusions. Our commitment to innovation extends beyond mere functionality; we aim to optimize resource allocation and reduce energy consumption. Through advanced technology and thoughtful design, our project seeks to redefine surveillance standards, providing comprehensive protection for residential, commercial, and institutional environments.

1.3 METHODOLOGY

System Design and Development: The initial phase of our project centers around meticulous system design and development. Our team collaborates to create a robust Break-In Surveillance System. This entails designing the hardware components, including the laser-based trigger switch and motion sensors. Simultaneously, we develop sophisticated software algorithms for precise motion detection, camera activation, and efficient alerting mechanisms.

Hardware Implementation: Once the system design is meticulously finalized, we proceed to the hardware implementation stage. Here, we assemble critical components—sensors, cameras, and communication modules—integrating them seamlessly with the laser trigger switch. Rigorous calibration and exhaustive testing ensure the accuracy and reliability of these hardware elements.

Software Development: In parallel, our software engineers engage in crafting the heart of our system—the software. We meticulously program the motion detection algorithms, camera control logic, and real-time alerting features. Additionally, geospatial data sharing functionality is embedded. Our focus lies on optimizing software efficiency and responsiveness to meet the highest standards.

Integration and Testing: The synergy between hardware and software components is paramount. Integration testing ensures seamless interaction among subsystems. Rigorous scenarios simulate varying light conditions, motion patterns, and environmental factors. Our goal is to validate the system's performance comprehensively, minimizing false positives and maximizing accuracy.

User Interface Design: A user-friendly interface is pivotal for effective system interaction. Our design team crafts an intuitive smart phone application. Users receive real-time alert messages, access live video footage, and explore geospatial data effortlessly. Usability testing refines the interface, ensuring a seamless experience for end-users.

Deployment and Evaluation: With a fully developed and rigorously tested system, we deploy it in diverse real-world environments—residential homes, educational institutions, and government facilities. User feedback and performance metrics guide our evaluation process. Iterative improvements based on these insights enhance overall functionality, ensuring user satisfaction and robust security.

This comprehensive approach ensures that our Break-In Surveillance System not only meets but exceeds expectations, safeguarding our communities effectively.

1.4   ORGANIZATION OF REPORT

The comprehensive report is meticulously organized into six CHAPTERs, each serving a distinct purpose:

Introduction and Objectives (CHAPTER 1): In this foundational CHAPTER, we delve into the project's context and set clear objectives. We outline the rationale behind our endeavor and provide insights into the methodologies chosen for implementation.

Literature Review (CHAPTER 2): Our exploration extends to existing patient monitoring techniques documented in the literature. Through an exhaustive survey, we scrutinize conventional systems, conducting a detailed analysis. This

critical review informs our approach and highlights gaps that our project aims to bridge.

Wi-Fi-Based System Development (CHAPTER 3): Existing hospital patient monitoring systems often rely on a blend of wired and wireless technologies. Wired systems, with their physical connections, transmit data reliably. However, our focus lies on the Wi-Fi-based system—a paradigm that offers greater mobility and flexibility. Despite its advantages, we address challenges such as signal interference and bandwidth limitations.

Proposed System Implementation (CHAPTER 4): Here, we delve into the heart of our project—the proposed system. We elucidate the intricate process of implementation, from hardware components to software modules. The working principles of these components are explored, emphasizing seamless integration and robust functionality.

Results and Performance Evaluation (CHAPTER 5): Rigorous testing scenarios form the backdrop for evaluating our developed system. By subjecting it to diverse inputs, we measure accuracy and gauge performance. This CHAPTER provides empirical evidence of our system's efficacy, ensuring alignment with our objectives.

Conclusion and Future Scope (CHAPTER 6): As we draw the curtain on this study, we summarize our findings and outcomes. Future research avenues related to our work are thoughtfully discussed, paving the way for continued innovation in patient monitoring systems.

CHAPTER 02

LITERATURE REVIEW

2.1 GENERAL

To address this issue, researchers and developers have explored various methodologies and technologies that leverage speech signals to simplify and enhance the lives of common people. This literature survey aims to provide an overview of the existing work in this domain, some project papers survey are listed below:

Luiz Paulo Oliveira Paula, Nuruzzaman Faruqui, Imran Mahmud MD. Whaiduzzaman, Eric Charles Hawkinson, Sandeep Trivedi, 2023, "A Novel Front Door Security (FDS) Algorithm Using Google Net-BiLSTM Hybridization" discussed about the security concerns drive innovation in surveillance. Traditional front-door security systems, while prevalent, face limitations in threat detection. Recent advancements introduce the Front Door Security (FDS) algorithm, leveraging Human Activity Recognition (HAR) to classify threats with 73.18% accuracy. FDS employs Google Net- BiLSTM architecture to identify actions like kicking, punching, hitting, and gun violence, enhancing real-time threat detection and alert capabilities. This survey underscores the significance of HAR in strengthening security surveillance, advocating for continuous innovation to address evolving security challenges effectively.

Rasadurai Kumaravel, 2023, "AI Based Smart Surveillance System" shows us the burgeoning demand for safety and security has propelled the development of AI-based smart surveillance systems. These systems autonomously analyze various surveillance data types, including video, image, and audio, without human intervention. Recent advancements in computer vision, sensor technology, and

AutoML have significantly contributed to the evolution of intelligent surveillance solutions. Despite numerous surveillance systems available, the absence of live decision-making and predictive analysis capabilities remains a notable gap. This survey highlights the increasing relevance of AI-based surveillance systems and emphasizes the need for real-time decision-making capabilities to enhance security measures effectively.

Avanti Pawar,Ajay Lahane, 2020, "Design and Implementation of IoT based Smart Surveillance" is discussed about the Internet of Things (IoT) offers transformative potential in home automation. This project proposes an IoT implementation for monitoring and controlling home appliances via the cloud, leveraging Wi-Fi connectivity and Raspberry Pi as the server system. The survey highlights the benefits of IoT, including enhanced convenience, security, and energy efficiency. By enabling remote management of environmental parameters and appliances, this system promises to streamline daily routines and improve quality of life. With the proliferation of IoT technologies, there is a growing demand for innovative solutions that offer seamless connectivity and user-friendly interfaces for smart home automation.

Sonali P. Gulve, Suchitra A. Khoje, Prajakta Pardeshi, 2017, Implementation of IoT-Based Smart Video Surveillance System is about Smart video surveillance, an IoT-enabled solution, revolutionizes security measures by leveraging internet connectivity. This system detects and records human presence, enhancing safety and providing real-time alerts via SMS and email. Implemented using Raspberry Pi, Arduino, OpenCV, and GSM modules, it ensures comprehensive monitoring and notification capabilities. Beyond security, the system optimizes power consumption by controlling electronic appliances, showcasing its intelligence and practicality.

With increasing concerns for safety and efficiency, such IoT-based solutions are becoming essential for modern-day surveillance and home automation needs.

Michael Bramberger, Roman P. Pflugfelder, Arnold Maier, Bernhard Rinner, Bernhard Strobl, Helmut Schwabach, 2014, "A Smart Camera for Traffic Surveillance" discussed about the convergence of CMOS image sensors and powerful processors in embedded systems has spurred the development of smart cameras, revolutionizing surveillance and traffic management. These devices integrate video sensing, processing, and communication, offering versatile solutions for various applications. This survey explores the implementation of smart cameras for traffic surveillance, showcasing their ability to capture video streams, analyze traffic data, and transmit information to network nodes. Experimental results demonstrate the feasibility and effectiveness of these systems, indicating their potential to enhance traffic monitoring and management capabilities in urban environments.

R.A. Persad, C. Armenakis, G. Sohn, 2010, Calibration of a PTZ Surveillance Camera using 3D Indoor Model shows us how indoor video surveillance systems have traditionally relied on 2D image analysis for security monitoring and event detection. Integrating these systems with 3D geospatial data enhances scene interpretation but poses challenges. This survey highlights the importance of integrating visual surveillance with 3D models to improve understanding of scene dynamics. It discusses methods for calibrating single-view video cameras to 3D wireframe models, focusing on tracking people in 3D space. The survey emphasizes the significance of incorporating motion considerations, such as Pan-Tilt-Zoom (PTZ) camera movements, and discusses promising approaches for estimating camera parameters in both simulated and real-world environments.

Satadal Saha,Subhadip Basu,Mita Nasipuri,Dipak Kr. Basu, 2010, Localization of License Plates from Surveillance Camera Images: A Color Feature Based ANN Approach is discussed about how traffic monitoring systems play a vital role in modern societies, detecting violations and managing traffic flow. Key modules, like license plate localization, are critical for system efficacy. This survey assesses methods for license plate localization, focusing on techniques utilizing color information and artificial neural networks. Evaluating real-world implementations in diverse environments, particularly in Indian cities, provides valuable insights. The survey highlights the importance of accurate localization for effective traffic management and underscores the potential of advanced technologies to enhance surveillance systems.

Wook-Sun Shin,Chang-Hun Lee,Doo Heon Song,2006, Vehicle Classification by Road Lane Detection and Model Fitting Using a Surveillance Camera is one of the important functions of an Intelligent Transportation System (ITS) is to classify vehicle types using a vision system. We propose a method using machine-learning algorithms for this classification problem with 3-D object model fitting. It is also necessary to detect road lanes from a fixed traffic surveillance camera in preparation for model fitting. We apply a background mask and line analysis algorithm based on statistical measures to Hough Transform (HT) in order to remove noise and false positive road lanes. The results show that this method is quite efficient in terms of quality.

CHAPTER 3

EXISTING SYSTEM

3.1 GENERAL

Closed-Circuit Television (CCTV), also known as video surveillance, involves the use of video cameras to transmit signals to specific locations, typically displayed on a limited set of monitors. Unlike broadcast television, where signals are openly transmitted, CCTV operates within a closed loop, ensuring that everything captured remains in-house and is not broadcasted over public airwaves. The history of CCTV dates back to the early 20th century. In June 1927, Russian physicist Léon Theremin developed an early mechanical CCTV system, which consisted of a manually-operated scanning-transmitting camera and wireless shortwave transmitter and receiver. This system, with a resolution of a hundred lines, was commandeered by Kliment Voroshilov and installed in the courtyard of the Moscow Kremlin to monitor approaching visitors. Another notable early CCTV system was installed by Siemens AG in Nazi Germany in 1942 at Test Stand VII in Peenemünde. It was used to observe the launch of V-2 rockets.

Over time, CCTV technology has evolved significantly. Analog cameras were initially used, but today's systems employ digital surveillance cameras with advanced features such as video analytics capabilities. These systems find applications in various contexts, including security, industrial plants, and public spaces. In areas requiring additional security or ongoing monitoring, video surveillance using CCTV cameras is common. Whether it's monitoring dangerous environments or preventing crime, CCTV plays a crucial role in maintaining safety and security worldwide.

Remember that while CCTV enhances security, it also sparks debates about privacy rights, especially when used for public surveillance. Balancing security needs with

individual privacy remains a critical consideration in the deployment of this technology. So, whether you're in a bustling city or a quiet neighborhood, chances are that you're being watched by a network of surveillance cameras, silently safeguarding our surroundings

3.2   DRAWBACKS

CCTV systems, prevalent in both commercial and public domains, offer the assurance of 24/7 surveillance but carry with them often-overlooked downsides, including privacy issues and ethical dilemmas1. Here are some key concerns:

Invasion of Privacy

Privacy concerns arise when security cameras are placed in areas where individuals expect privacy. For instance, placing CCTV in spaces like changing rooms or restrooms is widely considered an infringement upon personal space. The American Civil Liberties Union (ACLU) highlights the intrusive nature of public video surveillance, emphasizing its potential to capture individuals in private moments without their consent.

Abuse of Surveillance Footage

Surveillance footage may be misused by those with access to it. Episodes of unauthorized sharing or using footage for purposes other than security have been reported. For example, personnel might use video from CCTV inappropriately, leading to blackmail or public shaming. This misuse underlines a significant ethical dilemma of CCTV, where the boundary between security and privacy blurs.

Impact on Civil Liberties

CCTV deployment can lead to a greater sense of safety, yet it may also impinge on civil liberties. There's a concern that constant surveillance in public places could

stifle free speech and the right to protest. The tension between security and individual rights remains a critical issue1.

Effectiveness Against Crime

Despite their widespread use, CCTV systems do not always deter criminals effectively. Some studies suggest that criminals adapt by wearing disguises or avoiding areas with visible cameras. Moreover, the mere presence of cameras does not guarantee timely intervention or prevention of crimes.

False Sense of Security

People often assume that the presence of cameras ensures safety. However, relying solely on CCTV can create a false sense of security. Cameras cannot prevent all incidents, and their effectiveness depends on factors like camera placement, lighting conditions, and operator vigilance.

High Costs of Implementation and Maintenance

The initial installation cost is just the tip of the iceberg. Ongoing maintenance, repairs, and upgrades contribute significantly to the overall expense. Businesses and organizations must allocate resources for regular inspections, camera adjustments, and system updates.

Storage and Management Issues

Storing and managing vast amounts of video data pose challenges. CCTV systems generate terabytes of footage daily, requiring efficient storage solutions. Retrieving specific footage for investigations can be time-consuming.

Limitations in Surveillance Coverage

Cameras have fixed fields of view. Blind spots can occur, especially in large areas or complex environments. Pan-tilt-zoom (PTZ) cameras partially address this issue but come with their own limitations.

Technical Failures and Reliability

Cameras can malfunction due to weather, power outages, or equipment failures. Regular maintenance and redundancy measures are necessary to ensure reliability.

CHAPTER 4

PROPOSED SYSTEM

4.1 GENERAL

In the ever-evolving landscape of security technology, the Break-In Surveillance system stands as a beacon of innovation. Its ingenious use of a LASER trigger for motion sensing heralds a paradigm shift, redefining how we safeguard our homes. Let us delve into its multifaceted features:

Traditional surveillance systems often rely on continuous video recording, consuming power and storage resources indiscriminately. The Break-In Surveillance system takes a different approach. It lies dormant until motion is detected, conserving energy and minimizing unnecessary footage clutter. This efficiency not only optimizes performance but also ensures that relevant events—those moments of intrusion—are captured with precision and clarity.

The true strength of this system lies in its immediacy. When motion triggers its sensors, it springs into action. Cameras activate, capturing footage of the intruding activity. But what sets it apart is its ability to send real-time alerts directly to the user's smartphone via SMS and video notifications. Whether you're at home or away, this instant communication empowers you to respond promptly to potential threats.

Context matters. Alongside the alert, the system includes the geographical location of the incident—a Google Map link. Imagine receiving an alert and instantly knowing where the breach occurred. This layer of insight enables precise action. Law enforcement, armed with valuable information, can arrive promptly, potentially reducing response time and enhancing overall security.

The Break-In Surveillance system transcends home use. Its cost-effective design and minimal equipment requirements make it an attractive solution for diverse

environments. In educational settings, administrators can monitor campus security, ensuring the safety of students and staff. Government sectors benefit too—securing critical infrastructure and public spaces becomes more efficient.

No system is flawless. As an IoT-enabled device, the Break-In Surveillance system faces cybersecurity risks. Vigilant security measures and regular updates are imperative to thwart potential breaches and protect user privacy. Additionally, its reliance on motion detection may lead to false alarms triggered by benign movements or environmental factors. Fine-tuning sensitivity and algorithms strikes the delicate balance between accuracy and minimizing false positives.
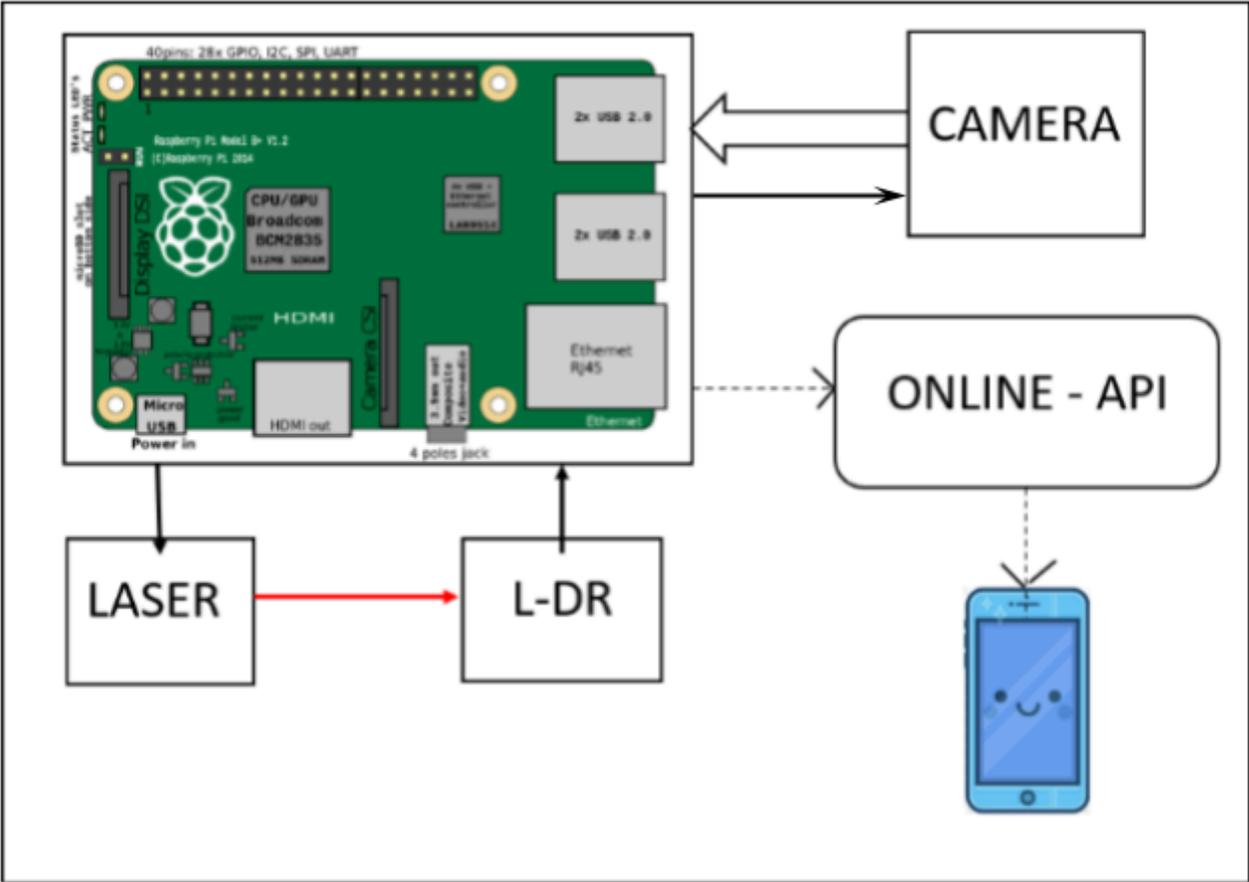
4.2 BLOCK DIAGRAM

Figure 4.2
(Block diagram of break in surveillance using laser detection)

Our robust break-in surveillance model relies on the formidable Raspberry Pi 3B+ as its central processing unit. In the detailed block diagram, you can discern the intricate connections between the Raspberry Pi, a laser module, and an LDR (light-dependent resistor) sensor. The laser, meticulously powered by the Raspberry Pi, emits a focused beam directed toward the LDR. Together, they form an efficient laser tripwire system. When an intruder disrupts the laser beam, the LDR's resistance promptly increases, signaling to the Raspberry Pi that an unauthorized entry may have occurred.

The second pivotal component in our setup is the legacy camera. This camera seamlessly interfaces with the Raspberry Pi via a dedicated bus cable. Through this connection, the legacy camera receives power, and data from the camera is transferred to the Raspberry Pi. When the laser tripwire registers an intrusion, the camera springs into action, capturing high-resolution images or recording video footage of the trespasser.

Beyond the hardware, our model incorporates essential software components. Notably, the Raspberry Pi collaborates with an online API—an interface that facilitates communication between computers over the internet. In our implementation, we harness the Twilio API. This powerful tool enables seamless communication between the Raspberry Pi and any designated smartphone.

Here's how our system responds during an intrusion event: when the laser tripwire detects disturbance, the Raspberry Pi activates the camera, securely storing video footage within its internal memory. Simultaneously, it communicates with the online API to dispatch an intrusion alert, complete with precise location details, to the pre-programmed smartphone.

In summary, our comprehensive solution ensures swift detection, documentation,

and notification in the face of unauthorized access. By combining hardware and software seamlessly, we create a robust defense against intruders. Our commitment to security extends beyond mere technology—it safeguards peace of mind for homeowners and businesses alike.

4.3 HARDWARE COMPONENTS

4.3.1 Raspberry Pi 3B+

Figure 4.3.1
(Raspberry Pi 3B+)

In the ever-expanding landscape of single-board computers, the **Raspberry Pi 3B+** stands as a testament to innovation. Its compact form factor belies its capabilities, making it a favorite among hobbyists, educators, and embedded system enthusiasts. At its heart lies the **Broadcom BCM2837B0 System-on-Chip (SoC)**—a 64-bit quad-core ARM Cortex-A53 processor humming along at 1.4 GHz. Whether you're crunching data, running simulations, or tinkering with code, the Pi's responsiveness is palpable. But it's not just about processing power; it's about wireless connectivity too. Dual-band Wi-Fi (802.11ac) ensures seamless communication, while Bluetooth 4.2 opens doors to IoT possibilities. Ports galore—USB, HDMI, audio—invite peripherals and multimedia experiences. And

that microSD card slot? It's where your projects reside, where you swap OSes, where creativity thrives. Affordability and educational impact converge—the Pi isn't just a tool; it's an educational revolution. Beyond the basics, AI, robotics, and neural networks beckon. The Pi dreams of autonomous drones, smart home hubs, and weather-predicting algorithms. It's a canvas for imagination—a playground where ideas take flight. In summary, the **Raspberry Pi 3B+** bridges curiosity and creativity, empowering a global community to explore, invent, and redefine what's possible—one GPIO pin at a time.
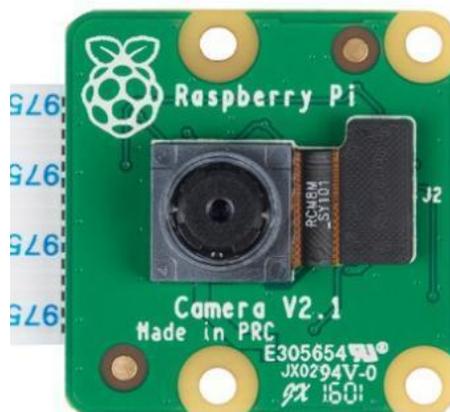
4.3.2 Raspberry Pi Legacy Camera Module-2

Figure 4.3.2
(Raspberry Pi Legacy Camera Module-2)

The Raspberry Pi Camera Module 2, a remarkable addition to the Raspberry Pi ecosystem, epitomizes versatility and performance. Its compact form houses an impressive 8-megapixel Sony IMX219 image sensor, complemented by a fixed-focus lens. This dynamic duo delivers stunning static images at 3280×2464 pixels and supports video recording at 1080p30, 720p60, and 640×480p90. The Camera Module 2 seamlessly integrates with all Raspberry Pi models, bridging the gap between computational power and visual creativity. Whether you're constructing surveillance systems, capturing moments in DIY photography, or

exploring computer vision applications, this module stands as a testament to engineering excellence. Its plug-and-play compatibility ensures a hassle-free experience, while its infrared (NoIR) variant opens doors to low-light imaging. As the lens peers into the world, it captures not just pixels but possibilities—each frame a canvas for innovation. The Raspberry Pi Camera Module 2 isn't merely an accessory; it's a catalyst for exploration, empowering makers, educators, and visionaries alike.
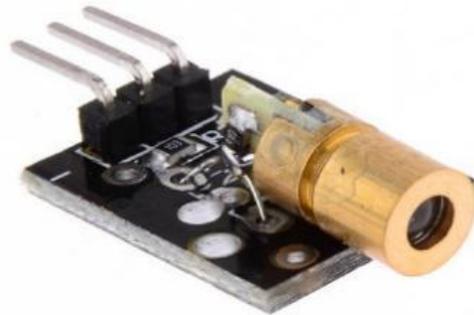
4.3.3 LASER Diode Module

Figure 4.3.3
(LASER Diode Module)

A LASER (Light Amplification by Stimulated Emission of Radiation) Diode Module represents a compact and sophisticated device that harnesses the principles of stimulated emission to emit a highly concentrated beam of light. At its core lies a semiconductor diode—an electronic component that efficiently converts electrical energy into coherent light. This coherence ensures that the emitted waves maintain a consistent phase relationship, traveling in a single, precisely defined direction. The applications of LASER diode modules span diverse fields, from telecommunications and bar code scanning to laser printing, medical instrumentation, and optical

sensors. Their reliability, compact form factor, and ability to deliver focused light beams make them indispensable tools for precision tasks.

4.3.4 Light-Dependent Resistor

Figure 4.3.4
(Light-Dependent Resistor)

A Light-Dependent Resistor (LDR), also known as a photo resistor, is a passive electronic component that exhibits a change in resistance based on the intensity of incident light. As ambient light levels vary, the LDR's resistance dynamically decreases with increasing light intensity and vice versa. These LDRs consist of semiconductor materials whose conductivity is intricately tied to the amount of light they receive. Widely employed in light-sensitive circuits, LDRs play pivotal roles in automatic streetlights, camera exposure controls, and solar panels. Their simplicity, cost-effectiveness, and responsiveness make them indispensable for detecting and adapting to changes in light conditions across various electronic applications.

4.3.5 Monitor

Figure 4.3.5
(Monitor)

A monitor, also referred to as a display screen or Visual Display Unit (VDU), serves as an essential electronic device for presenting visual information generated by computers and other electronic systems. These displays vary in size and resolution, spanning from compact screens for personal computers to expansive panels tailored for professional use. Monitors seamlessly connect to computers via interfaces such as VGA, HDMI, or Display Port, enabling users to interact with digital content and view application output. Whether analyzing complex data, editing multimedia, or immersing in creative endeavors, monitors remain indispensable tools in modern computing environments.

4.3.6 Keyboard

Figure 4.3.6
(Keyboard)

A keyboard, a fundamental peripheral input device, serves as the conduit for inputting text, characters, and commands into computers and electronic devices. Its design encompasses a meticulously arranged set of keys, spanning alphanumeric characters, function keys, and specialized controls like Enter, Shift, and Control. Keyboards come in both wired and wireless variants, each tailored to specific needs. From standard layouts to ergonomic designs and compact forms, keyboards facilitate essential tasks—typing documents, composing emails, navigating software interfaces, and executing multifarious functions. Customizable keycap designs, switch types, and backlighting options cater to individual preferences, ensuring a seamless and personalized user experience.

4.3.7 Mouse

Figure 4.3.7
(Mouse)

A mouse serves as a handheld pointing device, intricately designed to control the cursor and facilitate interactions within Graphical User Interfaces (GUIs) on computers and electronic devices. Its compact form factor accommodates one or more buttons and a scrolling wheel, ensuring seamless navigation. By tracking movement across flat surfaces—often through optical or laser sensors—the mouse empowers users to execute a myriad of tasks. From selecting items and dragging files to precise menu navigation, this unassuming peripheral plays a pivotal role in modern computing. Whether wired or wireless, ergonomic considerations prioritize user comfort during extended usage.

4.3.8 microSD

Figure 4.3.8
(microSD)

MicroSD cards are incredibly cost-effective. High-performance 32GB microSD cards can be obtained for as little as $10. Considering the affordability and ample storage capacity, they are an ideal choice for Raspberry Pi users. While Raspberry Pi OS can run on an 8GB card (especially with the Lite version), a 32GB card strikes a balance between space and cost. It provides enough room for most use cases without being significantly more expensive than smaller cards. If you're interested in running emulators or storing multimedia files, a 32GB card is the minimum. Emulated games, especially PlayStation 1 CD-ROM images, can quickly consume storage space. With regular updates and growing storage requirements, an 8GB card may soon become insufficient. To determine the best microSD card for your Raspberry Pi, performance testing is essential. Factors like read/write speeds, reliability, and compatibility matter.

4.4   SOFTWARE COMPONENTS
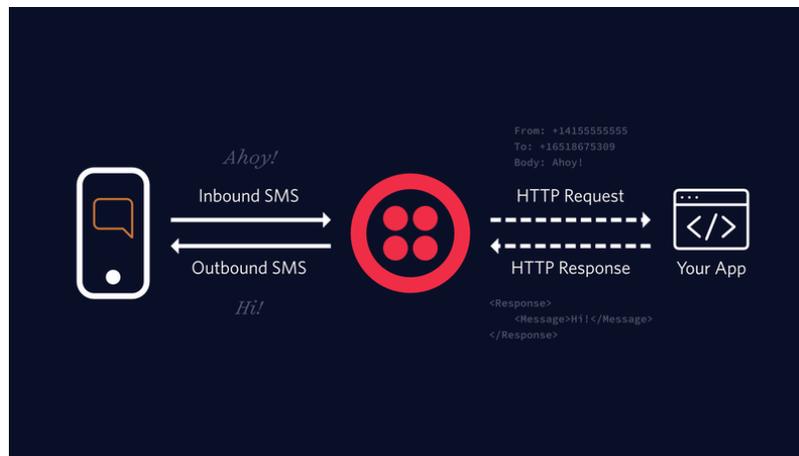
4.4.1   Online API (Twilio)

Figure 4.4.1
(Twilio – online API)

Twilio, a prominent player in the realm of cloud communications, offers a robust suite of APIs (Application Programming Interfaces) that empower developers to weave communication capabilities into their applications. Twilio's APIs serve as the connective tissue, bridging the gap between software applications and the real world. These APIs enable seamless communication across diverse channels—SMS, voice calls, video, and more. Whether you're building a customer support chatbot, verifying user phone numbers, or orchestrating conference calls, Twilio's APIs provide the building blocks. Twilio adheres to the REST (Representational State Transfer) architectural pattern. When we mention a "REST API," we're referring to an API accessible via HTTP at predefined URLs. These URLs represent resources—information or content accessible at specific locations. Twilio's ecosystem boasts separate REST APIs for various functionalities, each with its own set of endpoints. To interact with Twilio's APIs, you authenticate using HTTP Basic authentication. Your Twilio account SID serves as the username, and your auth

token acts as the password. These credentials ensure secure communication between your application and Twilio's servers. Alternatively, API keys provide an alternative authentication method. Twilio leverages webhooks—an essential part of event-driven architecture. When specific events occur (e.g., an incoming SMS), Twilio sends an HTTP request to a URL you specify. This callback mechanism allows your application to react dynamically to external events. While direct HTTP requests work, Twilio offers SDKs (Software Development Kits) for various programming languages. These libraries abstract away low-level details, simplifying API interactions. Whether you're coding in Python, JavaScript, Java, or Ruby, Twilio's SDKs streamline development. Twilio's APIs find applications across industries. Imagine integrating SMS notifications into your e-commerce platform, enabling customers to track orders. Beyond SMS and voice, Twilio's portfolio extends to video, chat, fax, and even IoT (Internet of Things). Whether you're building telehealth solutions, virtual events, or smart home applications, Twilio's APIs adapt to your needs. Twilio's infrastructure spans the globe, optimizing communication networks.

4.4.2 Python

Figure 4.4.2
(Python)

Python, a high-level, interpreted programming language, stands as a beacon of simplicity, readability, and versatility. Conceived by Guido van Rossum in the late

1980s, Python has transcended borders to become one of the most widely adopted languages globally. Its syntax, deliberately designed for human comprehension, fosters clarity—an asset for both novices and seasoned developers. Python gracefully accommodates multiple programming paradigms—procedural, object-oriented, and functional—granting practitioners the freedom to mold their coding styles. But Python's allure extends beyond elegance; it boasts an expansive standard library. Here, modules and functions await, addressing diverse needs—from file I/O and networking to web development and data analysis. Consider Python the Swiss Army knife of programming languages, adept at myriad tasks. Web developers wield frameworks like Django and Flask, sculpting responsive sites. Data analysts wield Pandas and Matplotlib, crafting visual narratives from raw data. Machine learning practitioners harness TensorFlow and PyTorch, birthing intelligent algorithms. Even mundane chores—automating repetitive tasks—find solace in Python's embrace. Yet, Python's true magic lies in its community—a bustling ecosystem of enthusiasts, educators, and contributors. Their collective wisdom, documented in tutorials and libraries, fuels Python's ascent.
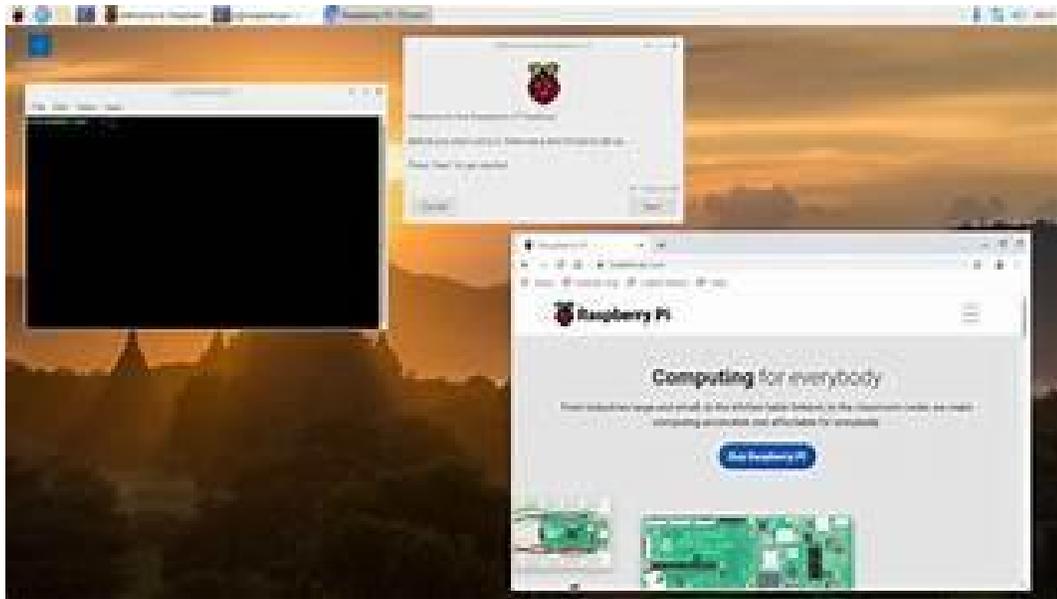
4.4.3   Raspberry Pi OS (Legacy)

Figure 4.4.3
(Raspberry Pi Legacy OS)

Raspberry Pi OS (formerly known as Raspbian) serves as the official operating system meticulously crafted for Raspberry Pi single-board computers. Rooted in the venerable Debian Linux distribution, it stands optimized for the ARM architecture that underpins Raspberry Pi devices. This tailored OS offers a welcoming desktop environment adorned with pre-installed applications, rendering it an ideal platform for a diverse array of projects and tasks. However. These older releases, while no longer actively maintained or updated by the Raspberry Pi Foundation, retain their functional essence. Their legacy status doesn't imply stagnation; rather, it signifies continuity. These versions, although lacking the cutting-edge features of their successors, find purpose in specific contexts. Why choose Raspberry Pi OS (Legacy)? The answer lies in its compatibility with older hardware and specialized software configurations. For projects where stability and familiarity outweigh the allure of novelty, the Legacy variant remains a steadfast choice. Under the hood, Raspberry Pi OS (Legacy) wields the apt package management system—a conductor orchestrating symphonies of installations, updates, and dependencies. The terminal, that timeless companion, awaits commands like an old friend. sudo apt-get update echoes through the corridors of time, fetching repositories. And raspi-config

unfurls a menu of possibilities: overclocking, localization, and more. Even the venerable sudo shutdown -h now retains its solemnity, bidding the system adieu. Legacy apps and libraries persist, etching their presence into the digital fabric. Python scripts, crafted in simpler epochs, hum with purpose. raspistill captures snapshots, while raspivid records videos—tools that have witnessed countless time-lapse photography sessions, surveillance endeavors, and art installations. And then there's GPIO—the bridge between hardware and software, where pins pulse with legacy code. The desktop ensemble beckons: LibreOffice Writer, Calc, and Impress stand ready for productivity. Chromium, the browser, navigates the web, while Thonny—the Python IDE—invites code creation. Raspberry Pi OS (Legacy) transcends mere functionality. As Bullseye (Debian 11) beckons, Raspberry Pi OS (Legacy) nods in acknowledgment. The torch passes, but the flame endures. Bullseye introduces modernity—64-bit architecture, fresh packages, and security enhancements—yet pays homage to its predecessor.

CHAPTER 05

RESULTS & DISCUSSION

5.1   WORKING STEPS

Over all set up of the break-in surveillance system

In this meticulously designed and technologically sophisticated security configuration, a precisely aligned laser and a light-dependent resistor (LDR)

collaborate to create a discreet yet highly effective tripwire mechanism. Typically positioned at entry points or near windows, this tripwire setup operates silently, like an invisible thread stretched across the threshold. When an intruder unwittingly crosses this laser beam, the LDR detects the interruption and triggers an alert.

But that's just the beginning. The true ingenuity lies in the concealed surveillance network. Strategically placed cameras, carefully hidden within walls, ceilings, or other inconspicuous locations, capture high-resolution footage without compromising their covert positioning. These unobtrusive sentinels observe every movement, recording the intruder's actions with precision. The video feed provides a visual narrative—a silent witness to any unauthorized entry.

Why is this video recording so crucial? Because it reveals intent. Was the intruder merely lost or curious, or did they have more sinister motives? The footage becomes a digital detective, piecing together the puzzle of the intruder's behavior. Perhaps they hesitated, glancing around nervously, or moved with purposeful determination. Every detail matters.

And then there's the Raspberry Pi—the silent orchestrator behind the scenes. Seamlessly integrated into the system, the Raspberry Pi processes data, analyzes patterns, and ensures seamless communication. It remains discreetly off-site, away from prying eyes. Its role extends beyond surveillance; it's the brain that interprets the data, triggers alarms, and communicates with the central monitoring station.

Imagine the laser beam crisscrossing the room, invisible to the naked eye, while the cameras silently document the intruder's every step. The security system operates like a symphony, each component playing its part flawlessly. The laser, the LDR, the hidden cameras, and the Raspberry Pi—all working together to safeguard the premises.

In this digital dance of security, the intruder remains blissfully unaware. They see nothing amiss, no blinking lights or obvious sensors. But behind the scenes, technology weaves its protective web. The owner and security guard rest assured, knowing that their fortress is fortified by innovation

Before the intrusion

(intruder is yet to enter the building)

In this meticulously designed security configuration, the laser trigger is deliberately kept in a perpetually 'ON' state, ensuring continuous activation of the tripwire mechanism. Simultaneously, the Raspberry Pi executes its background program seamlessly, remaining inconspicuous and off-site while monitoring the

system's integrity. The camera, cleverly concealed within the wall, captures any unauthorized entry without alerting the intruder. As shown in the figure, we can observe that the laser remains in the 'ON' state, and the intruder has yet to enter the building, completely unaware of the surveillance system. The owner and security guard rely on this covert setup to safeguard the premises against potential threats. The laser beam, invisible to the naked eye, crisscrosses the room, creating an intricate web of protection. Meanwhile, the Raspberry Pi processes data, analyzing patterns and anomalies, ready to trigger an alarm if necessary. The hidden camera, with its wide-angle lens, records every movement, ensuring that no corner goes unmonitored. The security system operates silently, like a vigilant sentinel, ensuring peace of mind for those within its protective embrace.

After the intrusion
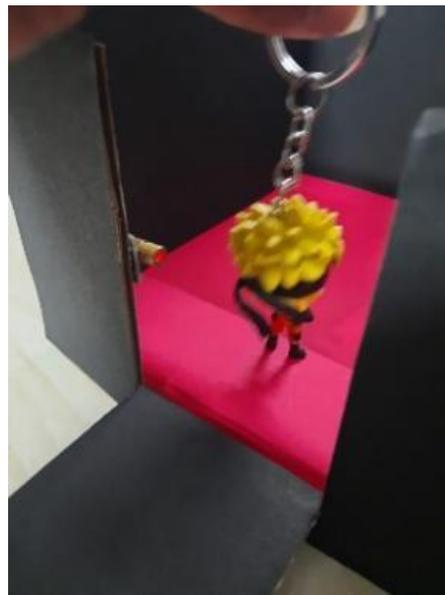
**(The intruder is entering the building)**

In this carefully orchestrated security setup, the intruder moves stealthily into the building, their actions unwittingly triggering a sequence of events. The laser beam, imperceptible to the naked eye, slices through the air, intersecting with the Light Dependent Resistor (LDR). Like a digital sentinel, the LDR senses the interruption, setting off a chain reaction.

First, the laser trigger—a perpetually 'ON' guardian—registers the intruder's passage. It's a silent acknowledgment, a nod from the system. Meanwhile, concealed cameras—strategically positioned within walls and corners—spring to life. Their lenses capture every detail—the hesitant step, the furtive glance—as the intruder navigates the space.

The Raspberry Pi, tucked away in its digital sanctuary, processes data seamlessly. Its background program hums with purpose, ensuring the system's integrity. And there, within the compact confines of the Raspberry Pi module, lies the microSD card—a repository of truth. It silently records the intrusion, preserving moments that will remain hidden until revealed.

The video is saved on desktop
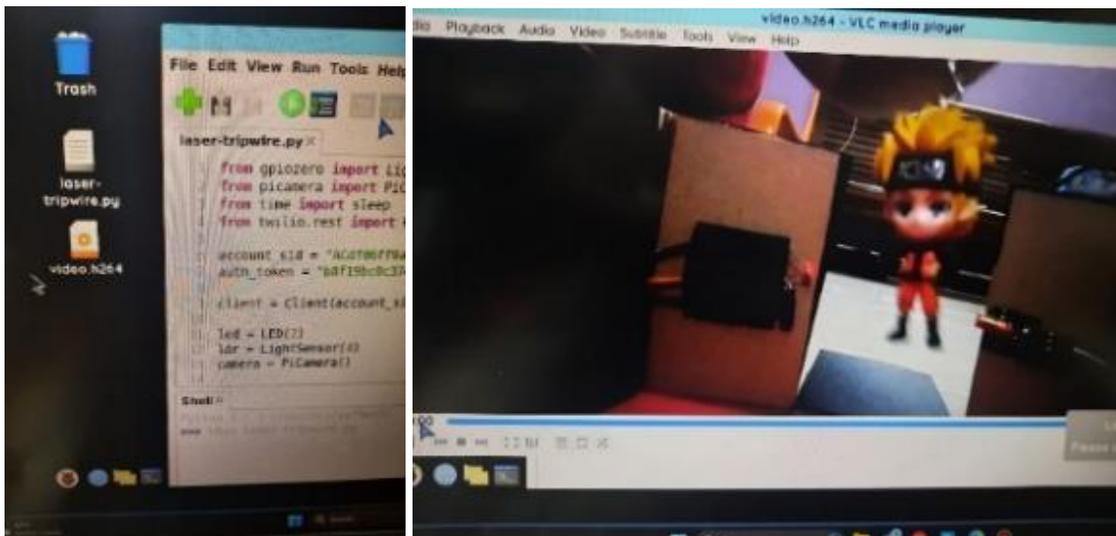
(Saved video will be available on the desktop to view when ever need)

The meticulously recorded video of the intrusion now resides securely on our desktop, as indicated by the image displayed on the right side. This prudent measure ensures that the captured footage can be meticulously reviewed later, serving as a vital asset during the investigative process. Each frame holds a story, the intruder's movements, their intentions, and perhaps even a glimpse of their face. These meticulously recorded details hold immense significance, especially

in situations where law enforcement may not arrive at the intrusion scene promptly. The captured video footage, securely stored on our desktop, becomes a vital asset—a digital breadcrumb trail leading to the intruder. As the security guard reviews each frame, they step into the shoes of a digital detective. Who was this intruder? What drove them here? The answers lie within these silent pixels, waiting to assist the police department in their pursuit

Short Messaging Service (SMS) alert
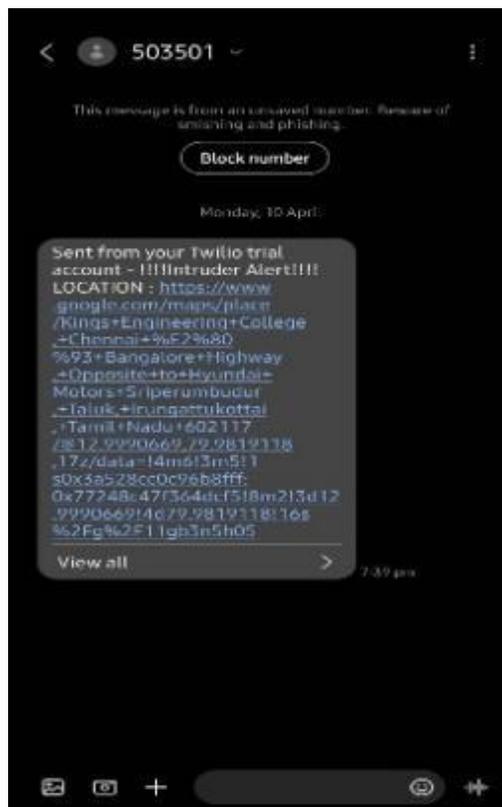
(SMS sent to the user along with the geo-location)

When the laser trigger activates and the concealed cameras silently record the

intrusion, the vigilant Raspberry Pi springs into action. Its seamless communication protocol, powered by the Twilio API, dispatches an SMS alert directly to the owner's phone. This timely notification includes not only the fact of the intrusion but also the precise geo-location—a digital breadcrumb that guides security personnel. Imagine the owner, alerted in real time, assessing the situation from afar. Simultaneously, the system alerts law enforcement, ensuring they arrive swiftly, like digital first responders. The intruder, unaware of this orchestrated response, faces a net closing in—a testament to the power of technology in safeguarding our spaces.

5.2   Performance Evaluation

The Break-In Surveillance system represents a significant leap forward in security technology. Its innovative use of a laser trigger for motion sensing redefines how we protect our homes. Let's explore its key features:

Energy Efficiency and Precision:
Unlike traditional surveillance systems that continuously record, the Break-In Surveillance system remains dormant until motion is detected. This approach conserves energy and minimizes unnecessary footage clutter. By activating only during relevant events (intrusions), the system ensures precise and clear capture of critical moments.

Immediacy and Real-Time Alerts:
When motion triggers its sensors, the system springs into action. Cameras activate, recording footage of the intruder. What truly sets it apart is its ability to send real-time alerts directly to the user's smartphone via SMS and video notifications.

Whether you're at home or away, this instant communication empowers swift responses to potential threats.

Contextual Insight:

Alongside the alert, the system provides the geographical location of the incident through a Google Map link. Imagine receiving an alert and instantly knowing where the breach occurred. This layer of insight enables precise action. Law enforcement armed with this valuable information can arrive promptly, potentially reducing response time and enhancing overall security.

Versatility Beyond Homes:

The Break-In Surveillance system isn't limited to home use. Its cost-effective design and minimal equipment requirements make it suitable for diverse environments. In educational settings, administrators can monitor campus security, ensuring the safety of students and staff. Government sectors benefit as well, using it to secure critical infrastructure and public spaces more efficiently.

Challenges and Mitigations:

No system is flawless. As an IoT-enabled device, the Break-In Surveillance system faces cybersecurity risks. Vigilant security measures and regular updates are crucial to thwart potential breaches and protect user privacy. Additionally, its reliance on motion detection may lead to false alarms triggered by benign movements or environmental factors. Fine-tuning sensitivity and algorithms strikes the delicate balance between accuracy and minimizing false positives.

In summary, the Break-In Surveillance system's energy efficiency, immediacy, contextual insight, and versatility position it as a powerful security solution. However, ongoing vigilance and fine-tuning are essential to address its limitations

and ensure optimal performance.

CHAPTER 6

CONCLUSION

6.1   CONCLUSION

In the ever-evolving landscape of security technology, the seamless integration of LASER Detection Technology into break-in surveillance stands as a beacon of progress. This transformative leap enhances security measures across residential and commercial domains, fortifying our defenses against unauthorized access. The precision and sensitivity inherent in laser detection systems create a formidable shield, enabling swift and effective responses to potential breaches. As we delve deeper into the intricacies of LASER technology, we uncover its multifaceted impact on surveillance strategies.

At the heart of LASER detection lies its unparalleled accuracy. Unlike conventional methods, which may trigger false alarms, LASER systems discern intruders discreetly. Whether safeguarding a family home or a bustling business, this precision instills confidence.

Beyond the confines of traditional surveillance, LASER technology finds applications in diverse realms. Picture an industrial facility where critical assets demand protection. Here, LASER detection seamlessly integrates into perimeter security, creating an invisible net that alerts authorities to any breach. The adaptability of LASER systems extends further—think of automated warehouses, where motion detection ensures efficient inventory management. In this interconnected world, LASER's versatility shines.

As technology marches forward, so does our commitment to excellence. LASER Detection Technology epitomizes this dedication. It's not just about thwarting break-ins; it's about creating safer environments. Families sleep soundly, knowing their homes are fortified. Business owners focus on growth, assured that their assets remain secure. The ripple effect extends to society—a collective sense of safety that transcends walls and boundaries.

The journey doesn't end here. Researchers, engineers, and visionaries continue to refine LASER systems. Perhaps we'll witness breakthroughs—enhanced range, adaptive algorithms, or seamless integration with AI. The promise of a more secure future beckons. And as we harness the power of LASER technology, we weave a tapestry of protection—one that embraces individuals, families, and businesses alike.

In summary, LASER Detection Technology isn't just a leap; it's a quantum leap. It's the silent guardian, the watchful eye, and the beacon of progress. So let us embrace it, celebrate it, and weave it into the fabric of our security landscape. For in doing so, we pave the way for a world where safety knows no bounds.

6.2   FUTURE SCOPE

The future scope of this innovative Break-In Surveillance system utilizing LASER technology is both promising and vast. As technology continues its relentless march forward, several potential avenues emerge for further development and enhancement, ensuring that our security measures remain at the cutting edge.

Integration with Artificial Intelligence (AI):
Imagine a surveillance system that not only detects intruders but also understands their intent. By incorporating AI algorithms, we can elevate the system's capabilities. Machine learning models can learn from historical data, adapt to changing patterns, and differentiate between harmless movements (like a pet or a falling leaf) and genuine threats. False alarms become a thing of the past, and security personnel receive precise alerts, allowing them to respond swiftly and effectively.

Enhanced Connectivity:
The future lies in seamless connectivity. Picture a Break-In Surveillance system that communicates effortlessly across devices, networks, and platforms. Emerging

wireless communication protocols, such as 5G and IoT (Internet of Things), hold the key. Real-time data transmission ensures that security updates flow seamlessly, whether you're monitoring your home from the office or overseeing a sprawling commercial complex from a remote location.

Advanced Sensor Technologies:

Our quest for precision knows no bounds. Beyond visible light, consider integrating thermal imaging or depth-sensing capabilities. Thermal cameras can detect body heat, making intruders visible even in pitch darkness. Depth sensors provide three-dimensional information, allowing the system to distinguish between humans and inanimate objects. Rain, fog, or smoke—these sensors pierce through environmental challenges, ensuring reliable detection.

Cloud-Based Storage and Analysis:

The cloud revolutionizes data management. Imagine a centralized repository where all surveillance footage resides—a secure vault accessible from anywhere. Cloud-based storage eliminates the limitations of physical drives, ensuring scalability and redundancy. But it's not just about storage; it's about analysis. AI algorithms can sift through terabytes of data, identifying patterns, anomalies, and potential threats. Investigators can rewind time, reconstruct events, and extract valuable insights.

Smart Home Integration:

The future isn't just about security; it's about convenience. Imagine a seamless blend of security and home automation. Your Break-In Surveillance system communicates with your smart thermostat, lighting, and door locks. When you leave for work, it arms itself. If an intruder triggers an alert, it not only notifies you but also locks doors, dims lights, and activates sirens. Voice commands—your virtual butler—control it all. Security becomes an integral part of daily life.

Expansion to Various Sectors:

The Break-In Surveillance system transcends boundaries. While residential and commercial properties benefit, its impact extends further. Picture it safeguarding critical infrastructure—power plants, water treatment facilities, and transportation hubs. Government buildings, museums, and public spaces—the system adapts. Its watchful eye ensures safety during crowded events, deters vandalism, and prevents unauthorized access. The same technology that secures your home secures society.

In summary, the future of Break-In Surveillance is dynamic. It's not just about hardware; it's about intelligence, connectivity, and adaptability. As we embrace LASER technology, we weave a safety net—one that protects lives, assets, and peace of mind.

REFERENCES

[1] , 2017, "**Implementation of IoT-Based Smart Video Surveillance System"** Conference Paper in Advances in Intelligent Systems and Computing May 2017 DOI: 10.1007/978-981-10-3874-7_73

1) **, 2023, "A Novel Front Door Security (FDS) Algorithm Using Google Net-BiLSTM Hybridization", Journal Name,** 10.1109/ACCESS.2023.3248509

2) **Design and Implementation of IoT based Smart Surveillance**

ISSN: 2278-0181 Vol. 9 Issue 04, April-2020

3) **Calibration of a PTZ Surveillance Camera Using 3D Indoor Model Geomatics Engineering**,

GeoICT Lab Earth and Space Science and Engineering

York University 4700 Keele St., Toronto, Ontario,

M3J 1P3 Canada (ravi071, armenc, gsohn)@yorku.ca

4)   , 2010, **"Localization of License Plates from Surveillance Camera Images: A Color Feature Based ANN Approach"** International Journal of Computer Applications (0975 - 8887) \

Volume 1 – No. 23

5)   **A Smart Camera for Traffic Surveillance**

6)   **AI Based Smart Surveillance System**

Article in International Journal of Scientific Research in Science Engineering and Technology · January 2023

DOI: 10.32628/IJSRSET229672

7)   **Vehicle Classification by Road Lane Detection and Model Fitting Using a Surveillance Camera**

March 2006

Journal of Information Processing Systems 2(1):52-57

DOI:10.3745/JIPS.2006.2.1.052

APPENDIX – 1

CODING

```python
import RPi.GPIO as GPIO

import time

import os

from twilio.rest import Client

from gpiozero import LightSensor

from picamera import PiCamera

from time import sleep


ldr = LightSensor(4)

camera = PiCamera()
```

```python
channel = 4

GPIO.setmode(GPIO.BCM)

GPIO.setup(channel,GPIO.IN)

while True:

    sleep(0.1)

    if ldr.value < 0.5:

        camera.start_preview()

        camera.start_recording('/home/pi/Desktop/video.h264')

        sleep(5)

        camera.stop_recording()

        camera.stop_preview()

account_sid =  "enter your account SID here"

auth_token =   "enter your account AUTH TOKEN here"


client = Client(account_sid, auth_token)


# Note : Change xxxx with your phone number


message = client.messages.create(

                from_='whatsapp:+14155238886',

                body='INTRUDER ALERT ',

                to='whatsapp:+91xxxxxxxxxx'
```

```python
                )
def callback(channel):

    print("geo location")

    message = client.messages.create(

                from_='whatsapp:+14155238886',

                body='http://maps.google.com/maps?q=24.197611,120.780512',

                to='whatsapp:+91xxxxxxxxxx'

                )

    time.sleep(60)


GPIO.add_event_detect(channel,GPIO.BOTH, bouncetime=300)

GPIO.add_event_callback(channel, callback)
```

APPENDIX – 2