IRO Journal on Sustainable Wireless Systems (ISSN: 2582-3167)
www.irojournals.com/irosws/

Prediction and Prevention of Theft in Jewellery Shop

S.P. Revathy[1], N. MadhiVathani[2], NaafiahFathima[3], A. MohammedIlyas[4]

[1]Assistant Professor, Information Technology, Velammal Engineering College, TamilNadu, India

[2,3,4]Student, Information Technology, Velammal Engineering College, TamilNadu, India

E-mail: [1]revathy.sp@velammal.edu.in, [2]madhivathani1123@gmail.com, [3]naafiahfathima1962@gmail.com, [4]ilyasrockey@gmail.com

Abstract

The internet of Things (IoT)-based total security is the most broadly used protection framework introduced by the technological developments. Sensors and cameras play a vital role in detecting movement and alerting the humans in lots of security applications. As these security gadgets are always accompanied with alarm systems, it is more popularly used for preventing the theft in public places like shopping malls and shops. In such areas, conventional CCTV cameras are usually used as it helps in non-stop human tracking, and detections of crimes. The proposed system is also on such intelligent security system capable of identifying mis-happenings in the public places. With real-time image feedback, the proposed device provides the owner with assurance even when they are not around. These studies examine the possibility of implementing automation technologies in the near future to provide complete protective control. The research suggests a fully automated security system that uses alarm messages and the internet of things (IoT) to predict and prevent unwanted activities in the jewellery shop.

Keywords: ESP32 Microcontroller, PIR sensor, Solenoid Valve, Exhaust Fan, Camera, Buzzer

1. Introduction

In the most recent modern era, safety and surveillance have become critical challenges because of theft and terrorism. The need for powerful video surveillance systems which can right now notify homeowners and other contributors of a household of ongoing thefts has been emphasised by using those incidents. Even though different precautious measures like CCTV

DOI: https://doi.org/10.36548/jsws.2023.3.002
Received: 13.06.2023, received in revised form: 15.07.2023, accepted: 02.08.2023, published: 10.08.2023

and advanced video recorders are at present available, identifying the burglars in disguise are still difficult . As a result, the crime rates keep on increasing day by day. When intruders cover their faces with materials like plastic, leather, or fabric, it becomes tough to recognize them with the use of face detection methodologies available. Traditional security systems do not provide real-time burglary notifications, and they do not allow homeowners to identify faces that may be hidden. In a similar way, legacy systems find it difficult to identify attackers in low-light conditions when using CCTV cameras without night vision capabilities.

This association requires either time-consuming and laborious manual video surveillance or the presence of a member or homeowner 24 hours a day. Furthermore, it may be challenging to search through recorded videos to find prospective intruders if the storage facility server has a lot of irrelevant photographs. To conquer those impediments, this research proposes a framework that sends trapped images of potential intruders to the police and authorized persons and moreover makes use of burglar alarms and harmless gases to hold thieves from getting away. This device presents an extra efficient method for detecting and preventing crimes and addresses the shortcomings of existing methods.

2. Related Work

The integration of human decision-making and control with automated systems will increase in the future of human-in-the-loop cyber-physical systems, allowing for increased efficiency, safety, and performance in manufacturing, transportation, and healthcare. This integration will have significant effects on the workforce and society as a whole and necessitate novel approaches to training, trust-building, and human-machine interaction[1]. A shortcoming and interruption open minded record framework is intended to keep up with the trust worthiness also, accessibility of information within the sight of equipment disappointments and pernicious attacks [2]. The development of strategies and mechanisms to guarantee the security and resilience of cyber-physical systems in the face of both intentional and unintentional attacks is referred to as "Towards cyber physical intrusion tolerance." [3]. Cyber-Physical-Human Systems, or CPHS, are systems that combine humans, physical systems, and computer networks to make them smarter and more effective[4]. The Byzantine Commanders Issue is an exemplary software engineering issue that models the test of accomplishing agreement in a circulated framework with worn out parts, where a few parts might act perniciously and attempt to disturb the agreement. Numerous solutions and variants have been proposed to address the issue, which is crucial to the creation of fault-tolerant distributed systems[5]. Down to earth

Byzantine adaptation to non-critical failure and proactive recuperation alludes to the advancement of strong agreement calculations that can endure noxious or defective parts in disseminated frameworks and recuperate from defects proactively.[6]. By dynamically adjusting the size of the request batches in response to changes in network conditions and load, adaptive request batching for Byzantine replication can boost the performance and scalability of Byzantine fault-tolerant systems. [7]. Inspired by the human autonomic nervous system, the article proposes the idea of autonomic computing, in which systems manage and adjust to changing conditions without human intervention. It talks about the advantages and drawbacks of using autonomic computing in a variety of applications [8]. The paper presents a self-designing disappointment location framework that adjusts to the quality of service (QoS) prerequisites of dispersed frameworks. A case study is used to discuss the proposed system's implementation and evaluation.[9] The paper proposes a self-manageable behavior strategy to improve group communication in distributed systems. It provides a comprehensive description and assessment of the proposed strategy, demonstrating its efficacy in enhancing group communication performance [10].

3. Proposed Work

3.1 Overview

In order to catch thieves and prevent theft, the proposed security system makes use of a combination of surveillance cameras, PIR sensors, microprocessors, and Internet of Things technology. The cameras operate typically for surveillance functions throughout business hours. Anyways, while the store or bank is shut, the accepted person can enact the safety gadget via a web page. Any human presence is detected by the PIR sensor, and if one is found, the camera takes a photograph, sends it to the authorized person and the police through email/SMS . The microcontroller confines the burglar with the aid of emitting a noise and releasing non-poisonous gas, deterring their break out. The authorized individual can transfer off the security gadget when the police shows up, and the gas remover removes the fuel from the place. Even though this system seems to be properly-geared up with a selection of security features to discourage robbery and trap thieves, right implementation is important to keep away from fake alarms and make sure that the released gas is innocent. Furthermore, adhering to lawful conventions is crucial while managing the robbery incidents to avoid any serious complexities.

3.2 Methodology

For the duration of everyday commercial enterprise hours, cameras are used inside the proposed machine to screen a financial institution or shop. A webpage may be utilized by an authorized person to activate the security mechanism after the shop or bank has been closed. A PIR sensor could be activated through the microcontroller whilst the security mechanism is turned on to detect any human presence within the place. The digi cam will take an image of the person if it detects their presence and send it to the authorized person through email. The microprocessor will produce a loud sound and an harmless save to prevent the burglars from fleeing. The authorized person can turn off the security machine while the police arrives, and the gasoline remover can get rid of the gasoline from the area, permitting the police to capture the thief. Detecting and stopping theft is made possible by this strategy.

3.2.1. Block Diagram

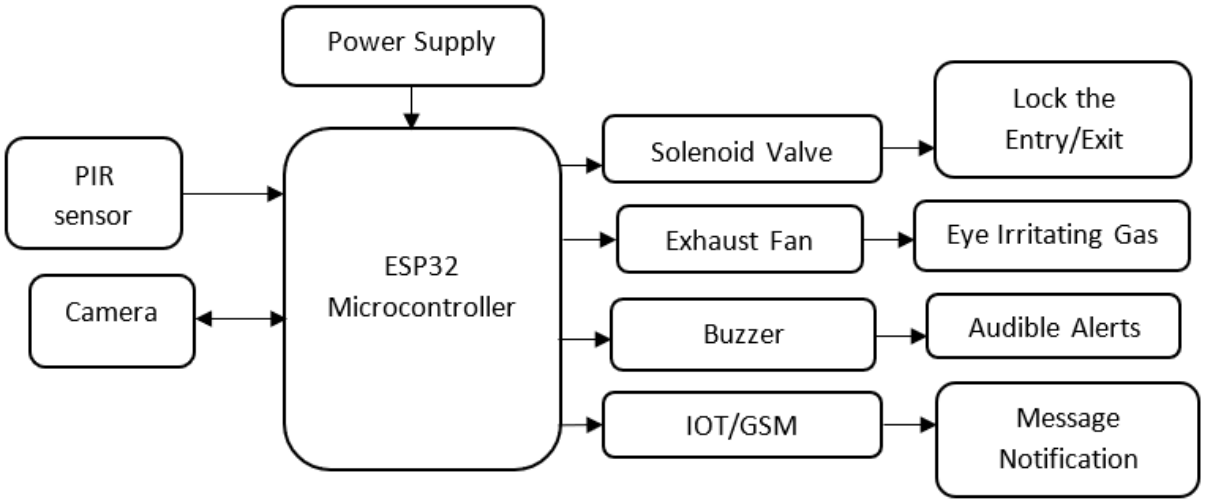

Figure 1. Proposed Block Diagram

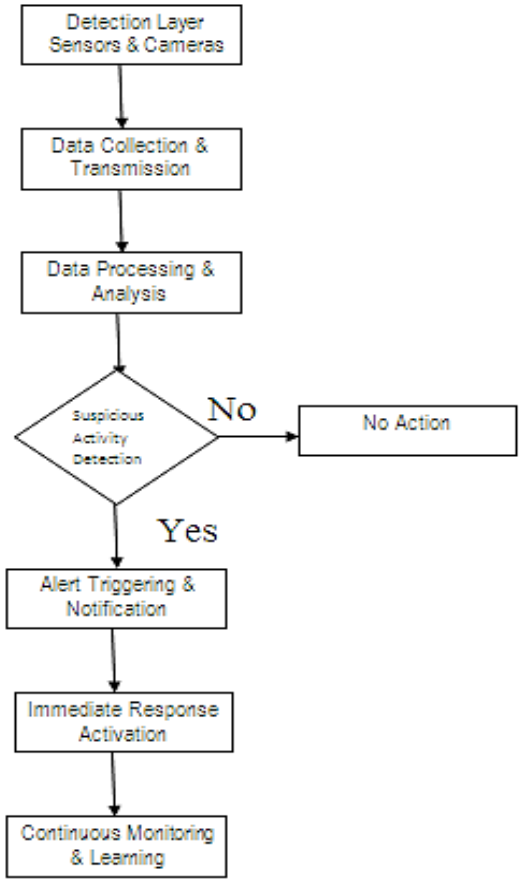

Figure 2. Proposed Flow Process

Sensors and Cameras Layer: The sensors and cameras layer is responsible for detecting any suspicious activities within the jewelry shop. These sensors and cameras would be strategically placed in different locations around the shop to cover all areas, including display cases, entrances, and exits. They would be designed to detect motion, sound, temperature changes, and other factors that could indicate a potential theft.

Data Acquisition Layer: The data acquisition layer is responsible for acquiring and transmitting the data collected by the sensors and cameras to the data processing layer. This layer could include hardware such as gateways, routers, and switches, which would be used to transfer the data from the sensors and cameras to the data processing layer.

Data Processing Layer: The data processing layer is responsible for processing the data received from the sensors and cameras and applying machine learning algorithms and predictive analytics to detect any suspicious activities. This layer could include cloud-based servers, edge computing devices, and data processing software.

Alerting Layer: The alerting layer is responsible for triggering an alert to the shop owner or security personnel when the system detects any suspicious activities. The alerting layer could include email, SMS, or push notifications sent to mobile devices.

Response Mechanism: The alert would prompt the shop owner or security personnel to take immediate action to prevent the theft. Depending on the situation, the response mechanism could include calling the police, sounding an alarm, or confronting the potential thief. The response would be based on the severity of the situation and the available resources.

Continuous Monitoring and Improvement: The system would continuously monitor the shop for any suspicious activities and adjust its algorithms and parameters as needed to improve its accuracy and reduce false alarms. The software would use feedback from the shop owner and security personnel to improve its performance and ensure that it is detecting and alerting only on genuine theft attempts.

In widespread, the gadget is meant to prevent the escape of the burglar at the same time concurrently alerts the authorities about the unauthorized human entry while the shop is closed. However, as a way to keep away from false alarms and make certain safety, it's far vital to ensure that the machine is efficiently designed, applied, and maintained.

3.3 Differentiating Between Burglars and Normal Persons

The key to differentiating between burglars and normal persons lies in the feature extraction and analysis step. The system is trained using a dataset that contains various examples of normal activities inside the jewelry shop, as well as instances of known burglary attempts or suspicious behavior. This training helps the system learn to recognize the differences between normal customers, staff, or visitors and potential threats.

The system can be designed to look for specific patterns that indicate burglary attempts, such as masked faces, crowbar-like objects, unusual movements during non-business hours, or attempts to tamper with jewelry displays. By comparing the real-time extracted features with learned patterns, the system can make informed decisions about potential theft and trigger the alarm when necessary.

This procedure is enacted during the jewelry store's closure, thereby significantly reducing the likelihood of regular customers accessing the shop. In the event that the shop

owner or other security personnel arrives, they will already be acquainted with this security protocol.

3.4. Alogithm

```
Begin.
Input capturedvideo.
FUNCTION theftDetection():
   WHILE true:  // Continuous monitoring
      frames = captureVideoFrames()  // Capture video frames from security cameras
      features = extractFeatures(frames)  // Extract features from the frames
          if isSuspiciousActivity(features):  // Check for suspicious activity
        triggerAlarm()  // Activate the alarm system
        notifySecurityPersonnel()  // Notify security personnel or shop owner
FUNCTION captureVideoFrames():
                def captureVideoFrames(camera_index=0):
   capture = cv2.VideoCapture(camera_index)
   if not capture.isOpened():
      print("Error: Unable to access the camera.")
      return
   while True:
      ret, frame = capture.read()
End while.
End if.
```

```
    FUNCTION extractFeatures(frames):
        ret, frame = cap.read()
    return features
FUNCTION isSuspiciousActivity(features):
    compare(stored_features & current_features)
    if is_suspicious(previous_features, current_features):
        return "Suspicious activity detected!"
End if.
FUNCTION triggerAlarm():
    if theft_detection_trigger():
        activate_alarm()
End if.
    FUNCTION notifySecurityPersonnel():
    def send_notification(subject, body):
     sender_email = "sen_email@gmail.com"
    sender_password = "send_password"
    receiver_email = "receiver_email@gmail.com"
            send_notification("Theft Detected", "A theft has been detected in your shop.")
```

3.5 Requirements

3.5.1. Hardware Components

ESP32- Receives the signal form the PIR sensor and controls the exhaust fan, solenoid valve , camera and buzzer

Buzzer- It is controlled by the ESP32 to send audible alerts

PIR Sensor- Detects the movement of the unwanted entries and sends a motion detection signal to the ESP32

Exhaust Fan- Controlled by the processor to emit the harmless gas

Solenoid Valve- Controlled by the processor to lock the entry /exit

USB Camera – Controlled by the processor to capture the images /videos on trigger

3.5.2 Software Components

Arduino IDE – The working of the components was coded using the Arduino IDE

Python – Enables the proper processing of the data received

4. Results and Discussion

The safety system that has been proposed is a comprehensive solution that uses modern technology to seize thieves and prevent robbery. Its ability to become aware of human presence when the shop is closed, trap snap shots, and cause sound and gasoline discharge components make it a beneficial asset in expanding the security of stores and banks. The usage of observation cameras and PIR sensors can likewise deliver vast evidence to judicial tactics.

However, there are probable problems and constraints that have to be tended to. To avoid prison and safety issues, the use of gas and sound release mechanisms should be cautiously controlled. Moreover, fake alarms can occur, causing customers and personnel unnecessary pressure and inconvenience. As an end result, protection, false alarm prevention, and felony compliance all rely on effective layout, implementation, and upkeep.

The proposed protection framework can likely work on the security of shops and banks. It may effectively prevent theft, catch burglars, and give clients and employees peace of mind by addressing potential barriers and enforcing high security.

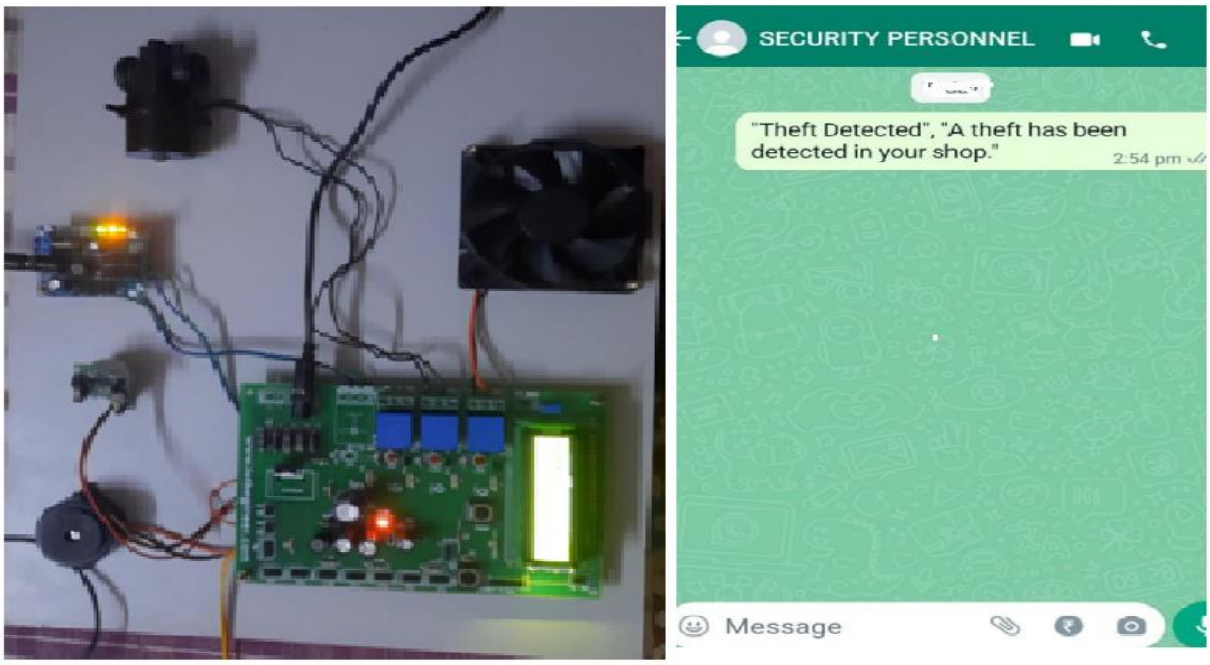

Figure 3. Implementation of Hardware

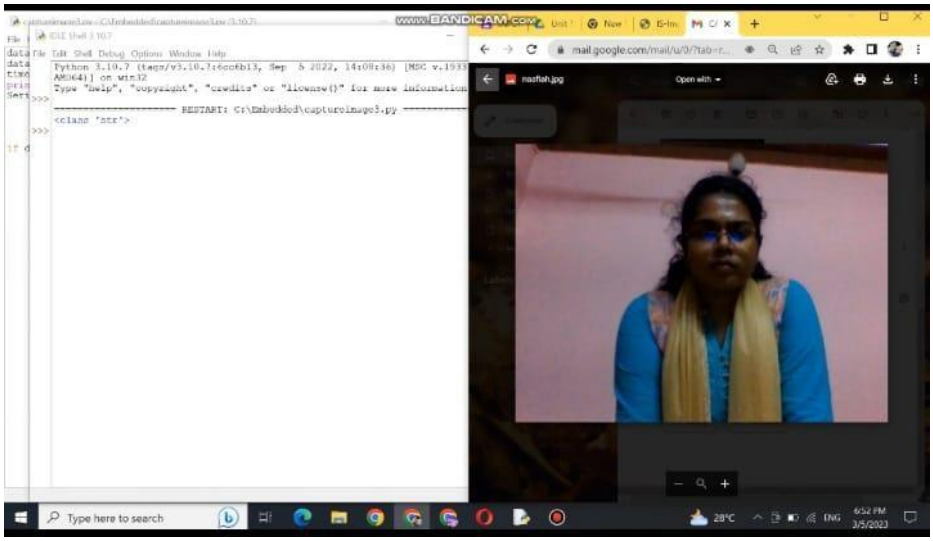

Figure 4. Implementation of Software

5. Conclusion

The research aims to combat shoplifting with a novel strategy that involves immediately notifying shop owner about the intrusions to prevent theft. A wireless sensing system that can detect human intruders and send real-time alerts to authorized parties accomplishes this.

Additionally, the system aids in stopping robbers from fleeing. However, new privacy and security issues have arisen as a result of the growing use of technology to link the real and virtual worlds. It is normal that these difficulties will be overcome in the future.

References

[1] G.Schirner,D.Erdogmus,K.ChowdhuryandT.Padir,TheFutureofHuman-in-the-LoopCyber-PhysicalSystems, inIEEE Computer, vol.46, no.1, pp. 36-45,2013.

[2] J. Fraga, and D. Powell, A Fault- And Intrusion-Tolerant File System, in proceedings ofIFIP3rdInternationalConferenceonComputerSecurity,Dublin,Ireland,pp.203-218,1985.

[3] S. Hossain, S. Etigowni, K. Davis, and S. Zonouz, Towards cyberphysical intrusiontolerance, in proceedings of the IEEE International Conference on Smart Grid Communications(SmartGridComm), Miami, FL, USA, pp. 139-144, 2015.

[4] S. Sowe, E. Simmon, K. Zettsu, F. de Vaulx and I. Bojanova. Cyber-Physical-HumanSystems: Putting People in the Loop, in IT Professional, vol. 18, no. 1, pp. 10-13, Jan.-Feb.2016.

[5] L. Lamport, R. Shostak, and M. Pease. The Byzantine Generals Problem, in ACMTransactionsonProgrammingLanguagesandSystems.vol.4,no.3,pp.382-401,Jan.-Feb.2016

[6] M.Castroand B.Liskov, Practical Byzantine fault-tolerance and proactive recovery, in ACM Transactions on Computer Systems (TOCS),vol.20, no.4, November2002.

[7] A. Sá, A.Freitas, and R.Macêdo, Adaptive request batching for byzantine replication, inOperatingSystems Review, vol.47, no. 1., pp.35-42, 2013

[8] J.KephartandD.Chess, The visionofautonomiccomputing,inIEEEComputer,vol.36,no. 1,pp. 41-50, 2003.

[9] A. Santos Sá, R, José, and A. Macêdo. QoS Self-configuring Failure Detectors forDistributed Systems. Frank Eliassen;;Rüdiger Kapitza. Distributed Applications and Interoperable Systems, 6115, Springer Lecture Notes in Computer Science, pp.126-140, 2010.

[10] R. Macêdo, A. Freitas, and A. Sá. Enhancing group communication with self-manageable behavior. Journal of Parallel and Distributed Computing.vol.73, no.4.pp.420-433,April2013.

[11] IOT Based Theft Detection using Raspberry Pi Umera Anjum, B. Babu Published 11 July 2017 Computer Science International Journal of Advance Research, Ideas and Innovations in Technology.

[12] IoT based Power Theft Detection R Giridhar Balakrishna, P Yogananda Reddy, M L N Vital International Journal of Innovations in Engineering and Technology (IJIET), Volume 8 Issue 3 June 2017

[13] IoT Based Energy Meter and Theft Detection 1Mamata N. Bonde, 2Roshni K.Patil, 3Utkarsh T. Mahajan, Shafiq Ansari4 , Hemraj V. Dhande5, International Journal of Innovations in Engineering and Science, Vol 4, No.10 ,2019.

[14] IoT Based Energy Metering And Theft Detection Srujana Uddanti1 , Christeena Joseph2,P.C.Kishoreraja3, International Journal of Pure and Applied Mathematics Volume 117 No. 9 2017, 47-51.

[15] Power Theft Detection and Alert System using IOT K.Kumaran, et. al. Vol. 12 No. 10 (2021).

Author's Biography

Mrs. S.P. REVATHY is an Assistant Professor with 4 years of teaching experience. She has published some research papers in national and international journals. Her area of research includes Image Processing, Mobile computing and Cloud Computing.

N.MADHI VATHANI an aspiring Engineering student who is pursuing my undergraduate degree from Velammal Engineering College. She is basically from the Information Technology department. She has done projects and attended symposiums. She has done an internship and got to learn many new things on technologies. She is very much interested in the Web development domain and loves to explore many new things. She likes to learn new technologies and gain knowledge from them.

NAAFIAHFATHIMA is an ambitious student pursuing her undergraduate degree in Information Technology at Velammal Engineering College. Shehasakeen interest in exploring various domains and is always excited to learn from new technologies and gain knowledge from them. She has completed various online certifications, including 2 NPTEL certifications, which have added value to her academic profile. She is always eager to participate in new opportunities and has a passion for seeking knowledge to enhance her skills.

A.MOHAMMEDILYAS is a dedicated undergraduate student pursuing Information Technology at Velammal Engineering College. He has completed an internship in webtechnologies, which has given him valuable industry exposure and practical skills. He is always enthusiastic about learning new things and is constantly seeking out opportunities to expand his knowledge. He has a passion for exploring new ideas and concepts in the field of IT and is dedicated to enhancing his skills to stay ahead in the rapidly evolving techindustry.