Grenze International Journal of Engineering and Technology, June Issue

Theft Detection using Telegram

E. Sujatha[1] and Hiba Rajarajeswari[2]
[1-2]Department of Computer Science and Engineering, Saveetha Engineering College (Autonomous), Saveetha Nagar, Thandalam, Chennai, Tamil Nadu 602105,
Email: sujathae@saveetha.ac.in, hibarajeswari@gmail.com
https://orcid.org/0000-0003-2500-2937

***Abstract*—A smart and practical method of keeping an eye on and preventing theft in homes and offices is what Theft Detection using Telegram seeks to achieve. The Telegram bot serves as a conduit for user communication, providing alerts and notifications in the event of any questionable activity. A third-party program called a bot is able to send and receive messages, commands, and requests within the Telegram platform. The bot is created and run by a Bot Father. Moreover, this study investigates the possibility of combining PIR sensors and the well-known microcontroller ESP32 to efficiently detect motion in smart home applications. Utilizing the ESP32's features, such as its low power consumption and Wi-Fi connectivity, the suggested system is appropriate for Internet of Things implementations. We concentrate on assessing the precision and effectiveness of motion detection with this straightforward but effective configuration. We examine the system's functionality responsiveness, and energy usage through real-world smart home experimentation. The outcomes show the viability and efficacy of the ESP32-PIR integration for motion detection, offering insightful information for improving energy efficiency and smart home security. This study lays the groundwork for the creation of affordable, energy-efficient smart home solutions that make use of off-the-shelf component.**

***Index Terms*—Theft detection, Telegram Bot, Security Alert, Intrusion Detection, Motion Sensing, Surveillance System, Telegram Notifications**

I. INTRODUCTION

Theft is a serious crime that causes losses and damages to individuals as well as businesses. It might also put someone's safety and wellbeing in jeopardy. Because of this, detecting and preventing theft is an important but challenging task. End-to-end encryption, cloud-based storage, and bot functionality are all offered by the well-known messaging app Telegram. Bots are external programs that run on Telegram and can perform a variety of tasks, such as sending messages, obtaining information, and executing commands. A Telegram bot can be used to take pictures of the would-be thieves and send them to the police or security personnel, or it can be used to alert the owners to the attempted theft. Telegram bots with computer vision capabilities can also be utilized for ethically sound purposes, such as automated security systems, smart door locks, and home monitoring. A Telegram bot, for example, can be used to send alerts and photos of visitors or intruders, or it can recognize and validate the faces of approved users to grant them access to the area.

The goal of developing a Telegram bot-based theft detection system is to increase the effectiveness and speed of theft reporting and response by leveraging the popularity and usability of messaging platforms. Telegram, a well-known messaging app, provides an ideal setting for implementing a bot that users can incorporate effortlessly into their daily schedules. Telegram was selected due to its robust API, end-to-end encryption, cross-platform

Grenze ID: 01.GIJET.10.2.141

compatibility, and compatibility with various media formats. These features, which make Telegram a suitable medium for real-time communication and collaboration, make it an appealing option for a theft detection system. The major goal is to create a system that is approachable, easy to use, and efficient so that people are encouraged to report theft incidents as soon as they occur, authorities can act more swiftly, and the community is generally safer.

The primary objectives of this system are as follows:

i. To give a thorough explanation of the history and driving forces behind the deployment of a Telegram bot-based theft detection system.
ii. To investigate the benefits of using Telegram as the theft detection communication platform.
iii. To describe the shortcomings of conventional theft detection techniques and how technology specifically, Telegram bot integration can help overcome them.
iv. To clarify the possible effects of putting in place such a system on neighborhood security and the avoidance of crime to establish the framework for later chapters that explore the functionality, design, and technical details of the suggested theft detection system.

II. Literature Survey

In the scholarly work [1] [2] the readers are likely to encounter a meticulously conducted exploration into the expansive realm of anti-theft technologies tailored specifically for personal devices, including but not limited to smartphones, laptops, and tablets. With an overarching aim to offer a comprehensive understanding of the landscape, the authors are expected to meticulously unravel a diverse array of anti-theft solutions, incorporating both hardware and software-based systems. The paper is anticipated to delve into the nuanced effectiveness of these technologies in not only thwarting theft but also in facilitating the retrieval of pilfered devices. Moreover, the authors may scrutinize emerging trends within the domain, confront challenges inherent in existing systems, and provide insights into user experiences, thus furnishing readers with a holistic perspective on the intricacies of personal device security. By synthesizing information across a spectrum of anti-theft measures, the paper aspires to be a valuable resource, contributing significantly to the current state of knowledge in personal device security and potentially influencing future advancements in this dynamically evolving field[3].

The innovative realm of utilizing machine learning algorithms[4][5] for the detection and prevention of theft within smart home environments. The primary focus of this paper is to explore the myriad ways in which machine learning can be strategically employed to enhance security measures in the context of smart homes. The authors are likely to investigate the application of machine learning techniques to analyse a diverse array of data sources, including sensor data and camera feeds, aiming to develop robust and intelligent systems capable of identifying potential theft scenarios. By scrutinizing the integration of machine learning into smart home security frameworks, the paper may offer insights into the efficiency, accuracy, and real-time responsiveness of such systems[6][7]. Additionally, it is anticipated that the authors will address challenges associated with implementing machine learning in this context, including privacy concerns and the need for continual adaptation to evolving threats. This comprehensive exploration is poised to contribute valuable knowledge to the intersection of machine learning and home security, providing a foundation for further advancements in the field and offering practical implications for homeowners, technology developers, and security professionals alike[8].

Embarks on an in-depth exploration into the dynamic realm of Internet of Things (IoT) applications[9][10] in the creation of anti-theft systems, with a specific focus on connected devices and environments. The authors likely delve into the intricate interplay between IoT technologies and security, revealing the innovative ways in which IoT is harnessed to proactively combat theft across various domains. This comprehensive review is anticipated to encompass an analysis of existing anti-theft systems that leverage IoT, shedding light on their design principles, functionalities, and effectiveness. The authors may investigate the integration of IoT sensors, communication protocols, and data analytics to bolster the capabilities of anti-theft mechanisms. Moreover, the paper might address the challenges and limitations associated with implementing IoT-based solutions, considering factors [4] such as scalability, interoperability, and cybersecurity. By scrutinizing the multifaceted landscape of IoT-based anti-theft systems, the paper is poised to offer valuable insights to researchers, practitioners, and policymakers, contributing not only to the academic discourse but also guiding the development and deployment of robust security measures in an increasingly interconnected world.

III. PROPOSED SYSTEM

A Telegram bot for the ESP32 microcontroller is in development. A bot is an outside program that operates within Telegram with the ability to send and receive requests, commands, and messages. The bot is made and controlled by a Bot Father. When motion is detected, an ESP32-CAM is used to take pictures. The user will receive these images via a wireless network from the created bot. When motion was detected, the bot would alert the owner. Through the use of commands, the user/owner will be able to control all specifications and requirements through the bot, allowing them to execute functions such as on/off for each requirement.

Advantages

The ability to enable real-time reporting is one of the major benefits of using a Telegram bot for theft detection. Users can report theft incidents as soon as they happen thanks to Telegram's instant messaging features, which give authorities the vital information they need to act quickly.

A large user base can access Telegram due to its user-friendly and intuitive interface. The platform's ease of use promotes broad adoption by guaranteeing that people with different levels of technical proficiency can report theft incidents without facing difficulties.

Users can access the theft detection system from a variety of devices, including computers, tablets, and smartphones, thanks to Telegram's cross-platform functionality. People can report incidents from anywhere at any time, thanks to this accessibility, which makes the system more responsive and all-encompassing.

End-to-end encryption provided by Telegram guarantees the confidentiality and security of user communications. Because it safeguards private information shared during incident reporting, this encryption is essential for theft detection. Users' trust in the system is increased because they can be sure that their data is secure. Using a Telegram bot to implement a theft detection system can be less expensive than traditional surveillance systems. Because Telegram is so widely used, users already have the necessary communication tools on their devices, negating the need for additional hardware investments. This means that the infrastructure required for the bot is minimal.

Disadvantages

Telegram may not be widely used by all demographic groups or in all regions, despite its widespread use. The theft detection system's accessibility depends on users having compatible devices, so a limited user base could lead to incomplete coverage as those without access to or use of Telegram may not be included in the system. Some smartphone models from earlier generations or those running out-of-date operating systems might not be able to use the Telegram app or its features. This incompatibility of devices may prevent some groups of people from using the system.

Internet access is a major need for the Telegram bot's efficacy. Users may experience difficulties using the system in places with inadequate or non-existent connectivity, which might cause delays in reporting theft events. In some circumstances, this reliance on the internet could make the system less reliable.

IV. DESIGN SYSTEM ARCHITECTURE

Developing a coherent system that can identify and alert users to possible theft incidents requires integrating a number of different components when designing an architecture for theft detection with Telegram-bot.

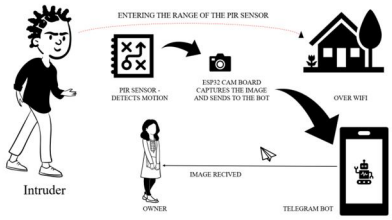

Figure 1. Architecture Diagram

The modules involved in this Theft Detection using Telegram is as follows,

- Sensor Module
- Edge Processing Module
- Connectivity Module
- Central Processing Module

- Notification Module
- Telegram Bot Interface Module
- User Authentication Module
- Database Module

MODULE DESCRIPTION

The system after careful analysis has been identified to be presented with the following modules.

Sensor Module

- When creating an architecture for theft detection with a Telegram bot, it is necessary to integrate several different components in order to create a cohesive system that can recognize and notify users of potential theft incidents. Uses a variety of sensors, such as security cameras, motion sensors, and door/window sensors, to identify unusual activity or unauthorized access.
- Additionally, it records and transmits to the microcontroller raw data pertaining to the external environment.

Edge Processing Module

- Analyses sensor data locally on edge devices or microcontrollers to spot irregularities or possible theft.
- Minimizes latency and the need for continuous data transfer by analysing incoming data using edge processing algorithms.

Connectivity Module

- Enables communication between the central server and edge devices.
- Oversees the smooth transfer of processed data via connectivity protocols (Wi-Fi, Bluetooth) from several edge devices to the central server.

Central Processing Module

- Runs a central server that collects and processes data from various edge devices.
- Uses rule-based systems, machine learning models, or theft detection algorithms to put patterns in place that point to theft or unauthorized access.

Notification Module

- Notifies users in real time when possible theft is discovered.
- Connects to the central server to receive notifications and sends alerts to the Telegram bot's interface.

Telegram Bot Interface Module

- Acts as the theft detection system's user interface, enabling communication between users and the system.
- Gets alerts from the central server and gives users access to system features, real-time updates, and controls (like arming and disarming).

User Authentication Module

- Makes sure that the Telegram bot is the only way for authorized users to access and manage the theft detection system.
- Verifies the legitimacy of user credentials and keeps the user interface safe.

Database Module

- Preserves user preferences, system settings, and historical data.
- Makes data retrieval easier for analysis, system optimization, and giving historical incident insights.

V. RESULTS

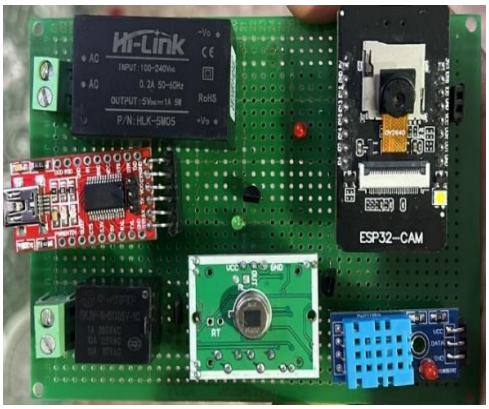

Figure 2. System Hardware

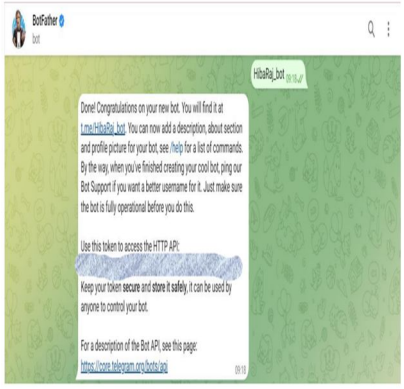

Figure 3. Creating the Telegram Bot

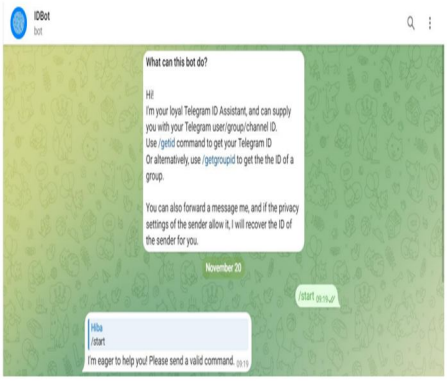

Figure 4. Initializing BOT ID

Figure 5. Receiving BOT ID

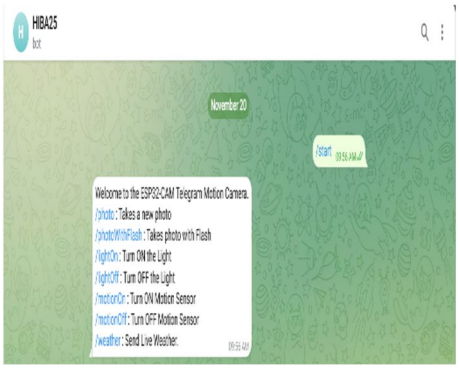

Figure 6. Starting

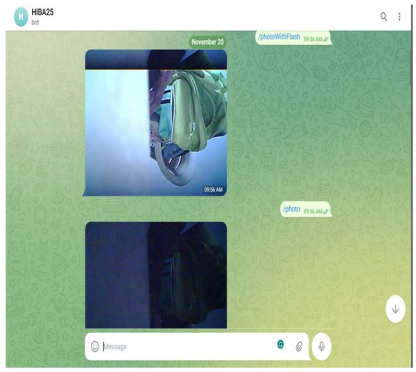

Figure 7. Photo With & Without Flash

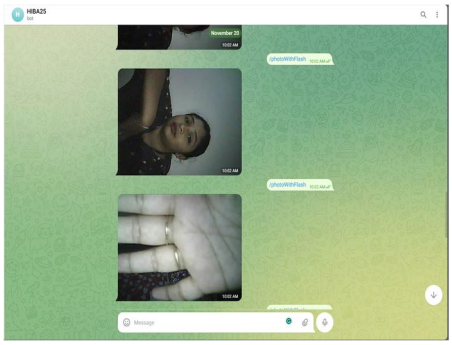

Figure 8. Photo With Flash

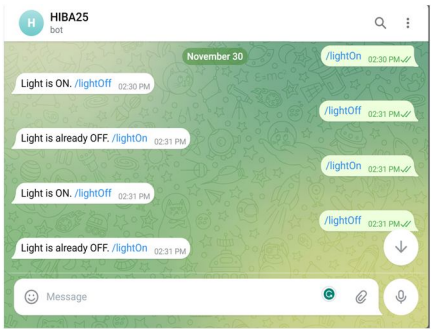

Figure 9. Light ON & Light OFF

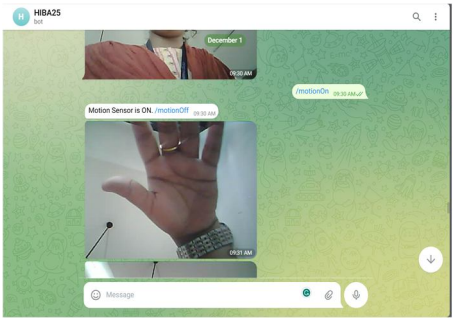

Figure 10. Motion Detection ON

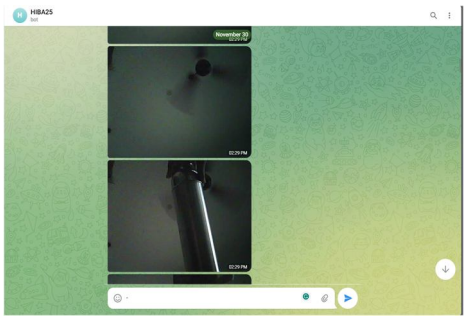

Figure 11. Dark Mode

Figure 12. Capturing Image While Detecting Motion

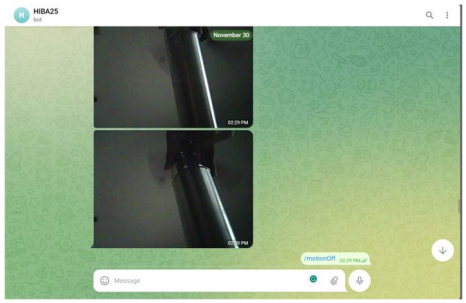

Figure 13. Motion Sensor OFF

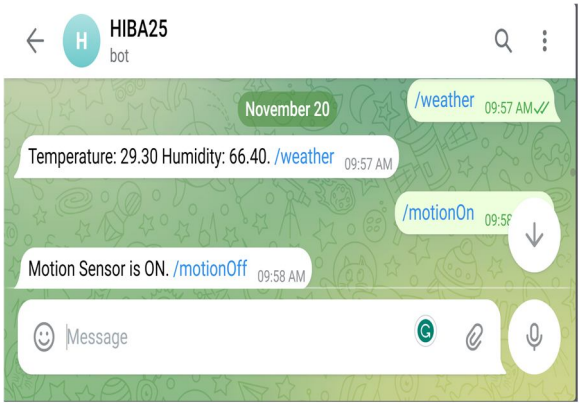

Figure 14. Detecting Weather

VI. Conclusion

The study concludes by presenting a reliable and approachable theft detection system that makes use of Arduino technology and Telegram bot integration. This novel method improves real-time communication while giving users the ability to monitor and control remotely. The library's smooth integration of Telegram bot features guarantees instant alerts, allowing for quick responses to possible theft incidents. The library serves as an example of how the use of environmental sensors, which provide more contextual data for increased accuracy, further enhances the effectiveness of the system. This study represents a major advancement in IoT-based security solutions, enabling effective and accessible theft detection. With the help of Telegram's instant messaging service, Arduino's adaptability, and well chosen libraries, a pragmatic and user-friendly method of enhancing security measures is established. Such integrated systems demonstrate the potential for broad adoption in various security applications as technology advances, offering users increased safety and peace of mind.

Future Work

There are a few interesting directions that could be pursued in the field of theft detection with a Telegram bot. Adding sophisticated machine learning algorithms is one way to improve the system's capacity to identify subtle patterns of questionable activity. This may result in enhanced precision and flexibility in detecting theft. Furthermore, investigating multi-sensor fusion—which involves combining sensors other than the ones that are currently in use—could enhance the robustness and dependability of the system. Investigating edge computing capabilities, which enable localized data processing on Arduino devices, is another exciting field. This lessens the need for constant internet access and improves system responsiveness, increasing its adaptability to a range of deployment scenarios. Subsequent endeavours may concentrate on personalization for users, allowing them to customize the theft detection system to suit their individual requirements and inclinations. Enhancing energy-efficient designs, integrating with larger smart home ecosystems, and utilizing cloud-based analytics for historical data analysis are some ways to help evolve more thorough and intelligent theft detection systems. Furthermore, investigating joint ventures with emergency services or outside security monitoring firms may improve the system's efficiency in promptly responding to theft incidents. Ensuring the integrity and privacy of user data will require strengthening security measures, such as encryption and strong authentication procedures. Last but not least, by promoting a better awareness of the system's capabilities and best practices for optimal use, educational

initiatives and user training materials can enable users to optimize the system's potential benefits. Future research projects have the potential to improve Telegram bot-based theft detection systems in order to make them more resilient, adaptable, and user-friendly in the face of changing security threats.

REFERENCES

[1] IOT BASED ANTI THEFT DETECTION AND ALERTING SYSTEM USING RASPBERRY PI U. Sirisha1 D. PoojaSri2, N. Gayathri 3, K. Heshma4, G. Raja Sekhar5, 1 Assistant professor, Department of Computer Science Engineering, Dhanekula Institute of Engineering Technology, Andhra Pradesh, India 2 345 Student, Department of Computer Science Engineering, Dhanekula Institute of Engineering Technology, Andhra Pradesh, India

[2] B. Wu and R. Nevatia, "Detecting and tracking of multiple partially occluded humans by Bayesian combination of edge let based part detectors", Int. J. Computer Vision (IJCV), vol. 75, no. 2, pp. 247-266, 2007.

[3] Shih-Chieh Wang, Te-Feng Su and Shang-Hong Lai, "Detecting Moving Object From Dynamic Background with Shadow Removal", ICASSP2011 IEEE, 2011.

[4] Automatic video surveillance for theft detection in ATM machines: An enhanced approach Publisher: IEEE Rupesh Mandal,Computer Science and Engineering, Sikkim Manipal Institute of Technology, Sikkim, INDIA , Nupur Choudhury ,Department of Computer Science Engineering & IT, Assam Don Bosco University, Guwahati, INDIA

[5] F-C Cheng, S-C Huang and S-J Ruan, "Scene analysis for object detection in advanced surveillance systems using Laplacian distribution model", Syst. Man Cybern. Part C Appl. Rev. IEEE Trans., vol. 41, no. 5, pp. 589-598, 2011.

[6] Theft Prevention System for Vehicles Using Biometric Traits Hindu Kumari G V1 , Nithyashree H C2 , Ranjana A Bali3 , Tejeswini R4 , Dr Sreevidya R C5 1, 2, 3, 4 Student, Department of CSE, BNM Institute of Technology, Bangalore, Karnataka, India-560070 5Assistant Professor, Department of CSE, BNM Institute of Technology, Bangalore, Karnataka, India-560070 Email address: gvhindukumari @ gmail.com1 , nithyahc1998 @ gmail.com2 , ranjana.bali1998 @ gmail.com3 , tejeswinir0098 @ gmail.com

[7] N. Sulman, T. Sanocki, D. Goldgof and R. Kasturi, "How effective is human video surveillance performance?", 19th International Conference on Pattern Recognition (ICPR 2008), pp. 1-3, 2008

[8] D-M Tsai and S-C Lai, "Independent component analysis-based background subtraction for indoor surveillance", IEEE Trans. Image Process., vol. 18, no. 1, pp. 158-167, 2009.

[9] M Singh, A. Basu and M.K Mandal, "Human activity recognition based on silhouette directionality", IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 9, pp. 1280-1292, 2008.

[10] F.Z Eishita, A Rahman, S.A Azad and A. Rahman, "Occlusion handling in object detection", Multidisciplinary computational intelligence techniques: applications in business engineering and medicine. IGI Global, 2013.