IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 4, July-August 2025

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Facto0072: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204034

SpyUSB: Securing USB Drives Against Malware Injection and Data Exfiltration

P. Masanamoorthy[1], Mrs. P. Shenbagam[2]

PG Scholar, Department of Master of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India

Assistant Professor, Department of Computer Applications, RVS College of Engineering, Dindigul, Tamil Nadu, India

ABSTRACT: USB flash drives are frequently used to store data, especially private or sensitive company information. The primary goal of current defense measures to safeguard those data is to stop data theft that occurs when a USB device is plugged into a host machine that has malware on it. This study identifies a threat: hackers can create spy USB flash sticks that can transmit data covertly across wireless networks without setting off host computer security measures. In order to illustrate the danger of covert data theft, we present SpyUSB, a USB flash drive that has been implanted with backscatter-based data theft gear. SpyUSB gathers information from the physical layer of communication between the host computer and the SpyUSB device, which is visible to the host computer's security features. SpyUSB creates a stealthy wireless channel by using backscatter communication. Additionally, utilizing a small energy reservoir, we investigate the possibility of covert data theft when the SpyUSB device is unplugged from the host computer. Our test demonstrates that SpyUSB can reach a maximum transmission bandwidth of 1,600 kbps. It can standby for more than six hours or send data continuously for 1.9 hours after being disconnected from a computer.

I. INTRODUCTION

USB flash drives, the most widely used portable data storage device, enable storage for everyday and professional tasks including additional backups and computer file transfers. Such devices may store sensitive data, including national security information, as well as private information about specific individuals. For instance, 460,000 residents' names, addresses, dates of birth, and tax payments were among the private data that a Japanese officer had kept [1]. In a similar vein, a USB flash drive has the security information and itinerary of British Queen Elizabeth's visit to Heathrow Airport [2]. There would be serious security risks if data is stolen or leaked from such USB flash devices. Although data encryption [3], [4] may lessen the impact of data theft, the encrypted data can still be decrypted using cryptanalytic techniques such brute-force attacks. Thus, preventing data theft from USB flash devices is the primary countermeasure. The majority of defense tactics are designed to stop data theft when malware on a host computer accesses a USB drive that is plugged in. The compromised host uses wireless local area networks (LANs) or even air-gapped networks to transmit and leak relevant data in the background. Five, six, seven, eight, nine, and ten. However, host systems can be remarkably equipped with sophisticated protection mechanisms to thwart malware attacks. [11], [12]. Access control techniques can be used by many systems to prevent unwanted access to certain USB flash drives [13], [14], [15], and [16], significantly reducing the possibility of data leakage. This study identifies a threat: USB flash drives have the ability to wirelessly leak data on their own without triggering host computer security measures. To transfer the stored data in a secret manner, we conceal a radio frequency (RF) transmitter inside a USB drive.

II. EXISTING SYSTEM

Traditionally, farmers have employed various methods to repel animals from their crops and livestock. While these methods may lack the sophistication of modern AI-based systems, they have been effective in certain contexts. Here is an overview of existing animal repelling techniques Erecting physical barriers like fences and walls is a common method to prevent animals from entering crop fields. These barriers act as a deterrent and provide a visible boundary. Farmers often use chemical repellents sprayed on crops to deter animals. These can include substances with strong odours or tastes that animals find unpleasant. Scarecrows have been a traditional method of deterring birds. They are human-like figures placed in fields to create the illusion of a human presence, scaring away birds. Animals such as dogs, donkeys, or llamas are sometimes employed as guard animals. Their presence helps deter smaller animals or predators from entering the area.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Facto0072: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204034

Loud noises, such as clanging pots or using devices that emit startling sounds, can be effective in scaring animals. Additionally, bright lights at night may disrupt nocturnal animals.

III. PROPOSED SYSTEM

This project presents an integrated system aimed at addressing wildlife-related challenges in agriculture by combining advanced AI technologies with targeted ultrasound emissions and farmer alert mechanisms. The system utilizes Temporal Convolutional Network (TCN) and WildNet for accurate detection and recognition of animal species, coupled with species-specific ultrasound emissions for repelling identified animals. Additionally, the system incorporates an alert system to notify farmers via SMS when potential threats are detected. The TCN and WildNet form the core of the computer vision module, offering real-time video analysis for accurate detection and recognition of animal species. This component processes high-resolution imagery captured by cameras deployed in agricultural areas, enhancing the system's ability to identify and classify wildlife accurately. The Ultrasound Emission module integrates species-specific ultrasound devices into the system. Upon identification of a threat by the computer vision module, the corresponding ultrasound emission is triggered, aiming to repel the detected species. Careful design ensures effectiveness against targeted species while minimizing impact on non-targeted entities. The alert system responds to potential threats by initiating notifications to farmers. Using SMS alerts, pre-registered farmers receive real-time information about the identified species and potential risks. This immediate and personalized communication enhances the farmers' ability to respond promptly to wildlife intrusions.

IV. SYSTEM ARCHITECTURE

The system architecture of the Animal Repellent System is designed to provide real-time detection and deterrence of wildlife intrusions in agricultural fields. It begins with live video input captured through surveillance cameras placed in the fields. These frames undergo preprocessing and segmentation to extract essential features required for analysis. The processed data is then fed into a Convolutional Neural Network (WildNet) for animal classification, while a Temporal Convolutional Network (TCN) is used to analyze sequential frames, improving accuracy in intrusion prediction. Upon identifying an animal, the system matches the detected species with its database and triggers a species-specific ultrasound signal to repel the animal in a humane manner. Concurrently, an alert system sends SMS notifications to farmers with details of the intrusion. The edge computing unit controls both the repellent device and alert mechanism, ensuring low-latency operation. All detection events and responses are logged in a centralized database for monitoring and analysis. A user-friendly web interface allows farmers to view real-time updates, configure settings, and manually activate deterrents when needed.

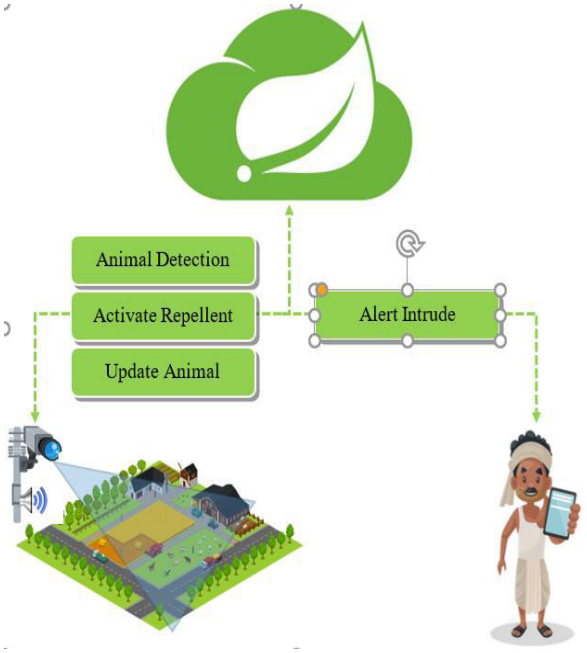

fig.4.1 Architectural diagram

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Facto0072: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204034

V. RESULTS

This section presents the outcomes and functional results of the proposed system titled "Reducing Latency and Storage Costs in Cloud Applications Using Advanced Data Management."The project was implemented and tested with simulated datasets and cloud-like environments to demonstrate its ability to manage redundant data, reduce storage costs, and enhance data access performance.

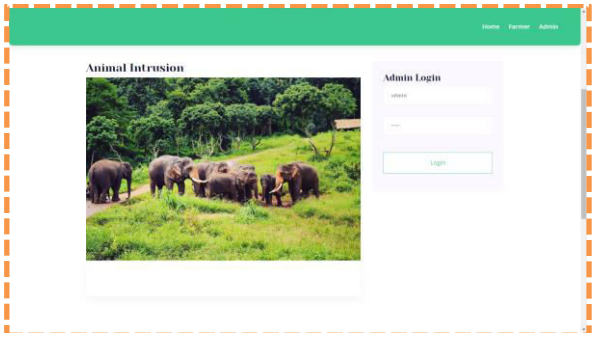

Fig 5.1: Animal File Upload Interface

The Animal Repellent System features a dual-interface design tailored to the distinct roles of administrators and farmers. The **Admin Interface** offers advanced controls, allowing administrators to securely log in, upload wildlife image datasets, and initiate the training of the WildNet model using configurable parameters. They can deploy trained models to edge devices, configure species-specific ultrasound frequencies, and update models as needed. A map-based dashboard enables real-time visualization of repellent zones and device locations across different fields.

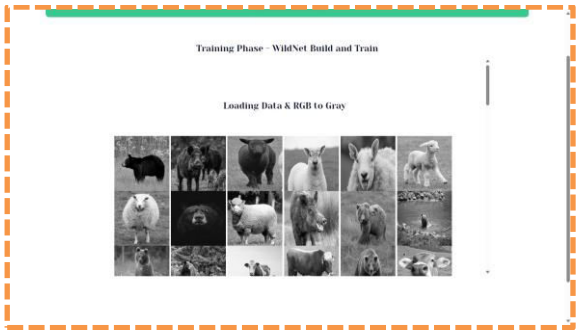

Fig 5.2: Loading Data RGB Gray

After cleanup, the system processes the uploaded files to detect and remove duplicate entries. This is done using fuzzy matching algorithms, which analyze file content, naming similarities, and metadata structures. Unlike exact matching, fuzzy matching detects duplicates even when filenames are slightly different but the content is identical. This helps prevent redundant storage and improves space utilization.

Fig 5.3: Build and Train Interface

| ISSN: 2394-2975 | www.ijarety.in| | Impact Facto0072: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204034

The **Build and Train Interface** is a critical component of the Animal Repellent System that enables administrators to develop and refine the WildNet deep learning model for accurate animal detection. Through this interface, administrators can easily upload labeled datasets, typically collected from platforms like Kaggle, and visualize them to assess image quality and distribution. The interface supports comprehensive data preprocessing steps such as grayscale conversion, resizing, noise reduction, and binarization, which enhance the dataset's readiness for training. It also facilitates animal segmentation and feature extraction using techniques like RPN and GLCM, ensuring precise isolation of animal characteristics.

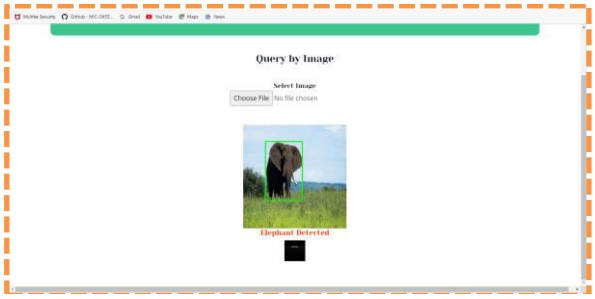

Fig 5.4: Upload and choose File

The **Upload and Choose File** feature allows administrators to easily upload wildlife image datasets into the system.

VI. CONCLUSION

The proposed Animal Repellent System effectively addresses the growing challenge of wildlife intrusion in agricultural fields using a combination of advanced technologies such as edge computing, computer vision, and deep learning. By leveraging the WildNet Convolutional Neural Network and Temporal Convolutional Networks (TCN), the system achieves high accuracy in detecting and classifying animal species in real-time. The integration of species-specific ultrasound emissions ensures humane and targeted repulsion, minimizing harm to both crops and wildlife. Additionally, the alert mechanism empowers farmers with timely notifications, allowing proactive responses to potential threats. The system's intuitive user interface and automation capabilities reduce manual intervention, enhance scalability, and support sustainable farming practices. Through extensive testing, the system demonstrated a recognition accuracy of up to 98%, confirming its reliability and practicality. Overall, this project contributes to the advancement of smart agriculture by offering a robust, ethical, and eco-friendly solution for mitigating human-wildlife conflicts, thereby promoting both food security and biodiversity conservation. SpyUSB, a USB flash stick with a hidden spy to steal data, is presented in this study. The spy can be used in both plug-in and unplug modes. Depending on whether it connects to a computer, it selects a mode to steal data. Despite being blocked by a strong concrete wall, SpyUSB has a transmission distance of 10.75 meters and a throughput of 1,600 kbps. With the help of a rechargeable battery, the USB flash drive can continue to function for six hours after being.

VII. FUTURE ENHANCEMENTS

While the proposed spyUSB system demonstrates a significant advancement in securing USB storage devices against malware injection and data exfiltration, there are numerous avenues for future enhancement and expansion. One of the key areas to explore is the improvement of real-time detection capabilities. This could involve developing lightweight and optimized versions of the deep neural network models that are capable of functioning efficiently on low-resource or edge computing environments, thus enabling faster response times without compromising detection accuracy. Another promising direction is extending the system's compatibility to support a broader range of operating systems, including macOS and various Linux distributions, thereby increasing its practical applicability in heterogeneous IT environments. Furthermore, incorporating adaptive learning mechanisms such as online learning or reinforcement learning could allow the model to dynamically adjust to new and evolving malware threats, including zero-day attacks, without the need for frequent retraining.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Facto0072: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 4, July - August 2025 ||

DOI:10.15680/IJARETY.2025.1204034

REFERENCES

1. M. De Clercq, A. Vats, and A. Biel, "Agriculture 4.0: The Future of Farming Technology," World Government Summit, 2018, pp. 11–13.
2. Y. Liu, X. Ma, L. Shu, G. P. Hancke, and A. M. Abu-Mahfouz, "From Industry 4.0 to Agriculture 4.0: Current Status, Enabling Technologies, and Research Challenges," IEEE Transactions on Industrial Informatics, vol. 17, no. 6, pp. 432–4334, June 2021.
3. M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming," IEEE Access, vol. 7, pp. 156237–156271, 2019.
4. K. Kirkpatrick, "Technologizing Agriculture," Communications of the ACM, vol. 62, no. 2, pp. 14–16, Jan. 2019.
5. A. Farooq, J. Hu, and X. Jia, "Analysis of Spectral Bands and Spatial Resolutions for Weed Classification via Deep Convolutional Neural Network," IEEE Geoscience and Remote Sensing Letters, vol. 16, no. 2, pp. 183–187, Feb. 2018.
6. M. Apollonio, S. Ciuti, L. Pedrotti, and P. Banti, "Ungulates and Their Management in Italy," European Ungulates and Their Management in the 21st Century, Cambridge University Press, 2010, pp. 475–505.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com