Fake Products Detection Using Machine Learning

Prof Shah.S.N[1], Mrs.Kokare.S.A[2], Rokade Dnyaneshwari[3], Avate Rutuja[4], Taware Sakshi[5]
[1]*HOD, Department of Computer Engineering, Sharadchandra Pawar college of Engineering and Technology Someshwarnagar, Pune, India*
[2]*Assistant Professor, Department of Computer Engineering, Sharadchandra Pawar college of Engineering and Technology Someshwarnagar, Pune, India*
[2,4,5] *Student, Department of Computer Engineering, Sharadchandra Pawar college of Engineering and Technology Someshwarnagar, Pune, India*

***Abstract*—The proliferation of counterfeit products and fraudulent branding presents significant challenges for consumers and businesses alike. The Fake Product & Fake Logo Identification System aims to address these challenges by leveraging advanced machine learning and computer vision techniques to accurately identify counterfeit items and logos. This system employs a combination of image recognition, pattern analysis, and AI-driven algorithms to detect discrepancies between genuine and fake products by analyzing subtle differences in logos, packaging, and design elements. By utilizing a comprehensive database of authentic product images and logos, the system compares and flags anomalies indicative of counterfeiting. The goal is to provide a reliable, scalable, and user-friendly solution that empowers consumers and businesses to combat the adverse effects of counterfeit products, enhancing trust and safety in the marketplace.**

***Index Terms*—Counterfeit items and logos, of image recognition, pattern analysis, and AI-driven algorithms.**

I. INTRODUCTION

In recent decades, portable computer systems have become increasingly popular due to their convenience and ability to simplify daily tasks. However, as these systems have evolved to offer more advanced features and powerful functionalities, security has emerged as a major concern. Cyber attackers often target portable systems to perform malicious actions such as data theft, disruption of business operations, or complete system compromise. One of the most difficult types of cyber attacks to detect is the business executive attack, which can bypass standard defenses like firewalls. Other common attacks include spear-phishing, eavesdropping, and distributed denial-of-service (DDoS). To counter these threats, intrusion detection systems (IDSs) are commonly used to provide protection from external intrusions. Despite the presence of such security mechanisms, many systems still rely on traditional login methods using a user ID and password. These are vulnerable to various threats, such as Trojan horse programs that capture login credentials or brute-force attacks that attempt countless password combinations. If attackers gain access, they can manipulate files, modify system configurations, or gain full system control. Currently, most host-based security solutions combine basic forms of known intrusion detection with network-based IDS techniques. Nevertheless, attacks using trusted IP addresses and sophisticated payloads can still bypass these systems. In some cases, even entities associated with well-recognized organizations may be difficult to trace or detect due to advanced obfuscation techniques. Computer forensics plays a crucial role in addressing such incidents. Its goal is to collect, preserve, and analyze digital evidence related to security breaches, treating computer systems much like crime scenes to reconstruct the events and uncover the truth.

II. METHODOLOGY

The Intelligent Insider Detection and Prevention System (IIDPS) framework is introduced in this section, along with a detailed breakdown of its components and their functions. By analyzing system calls (SCs), the IIDPS can identify a user's behavioral patterns, improving the system's accuracy in detecting potential attacks. To minimize response time, the IIDPS can be executed on a parallel computing system. This setup is particularly effective at mitigating insider threats by recognizing harmful user

actions and stopping attacks before they compromise the protected system. The IIDPS consists of a local computational grid and includes multiple components: three types of repositories (user log files, user profiles, and attacker profiles), a mining server, a detection server, a system call monitor (SC monitor), and a filtering module. Within the protected system, the SC monitor and filter are embedded as kernel-level modules. These components track and record system calls in the format (uid, pid, SC), where uid is the user ID, pid is the process ID, and SC is the system call submitted by the user. The user log file stores the sequence of SCs generated by each user, capturing their activity in chronological order. Using data mining techniques, the mining server analyzes this log data to uncover behavior patterns, which are then stored in the corresponding user profiles. The detection server plays a crucial role by comparing real-time user activities against the stored behavior patterns in both user and attacker profiles to detect suspicious behavior. If any malicious activity is identified, the detection server notifies the SC monitor and filter module, which then blocks the user's access to prevent further intrusions. To improve the system's efficiency, both the mining and detection servers operate within the local computational grid. Additionally, IIDPS assesses the similarity between the current SCs and known user profiles to detect cases where a user might be logging in with another user's credentials. A vital element of the SC monitor and filter is the class-limited-SC list, which restricts the use of certain system calls based on user roles. For example, a secretary might not be authorized to use specific privileged SCs. As a result, such restricted commands are blocked for unauthorized user groups, reinforcing system-level access control.

III. ALGORITHMS

A Convolutional Neural Network (CNN) is a type of machine learning model particularly effective for image-related tasks. In the context of product authentication, CNNs can be employed to analyze and classify logos and QR codes to determine whether a product is genuine or counterfeit. These models are known for their high accuracy, often achieving over 90% success in detecting fake products and logos.

IV. RESULT AND DISCUSSION

The developed system effectively detects fake products using a combination of QR code scanning and Convolutional Neural Networks (CNN) for logo analysis. The results demonstrate high accuracy in distinguishing between real and counterfeit items, especially when analyzing subtle differences in logos and packaging. The desktop application provides quick, real-time responses and is user-friendly, allowing both consumers and officials to easily verify product authenticity. However, the system is currently limited to products with QR codes and may occasionally face application crashes, indicating the need for further enhancement. Despite these limitations, the system proves valuable across industries like pharmaceuticals, fashion, and food, where counterfeit products are a major concern. With future improvements such as barcode integration and software optimization, the system has strong potential for broader adoption and impact.

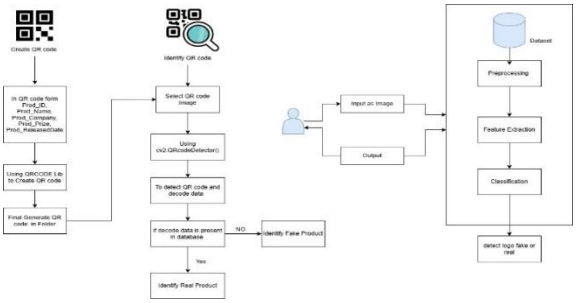
V. LITERATURE SURVEY

1. An Internal Intrusion Detection and Protection System Using Data Mining and Forensic Techniques *Authors: Fang-Yie Leu, Kun-Lin Tsai, Yi-Ting Hsiao, and Chao-Tung Yang* Traditional login methods, such as usernames and passwords, are still commonly used to verify user identities. However, these credentials are often shared among colleagues, making them a weak link in system security. This increases the risk of insider threats—legitimate users misusing their access from within the system. Since most existing security tools are designed to block external threats, detecting internal attacks becomes significantly more challenging.

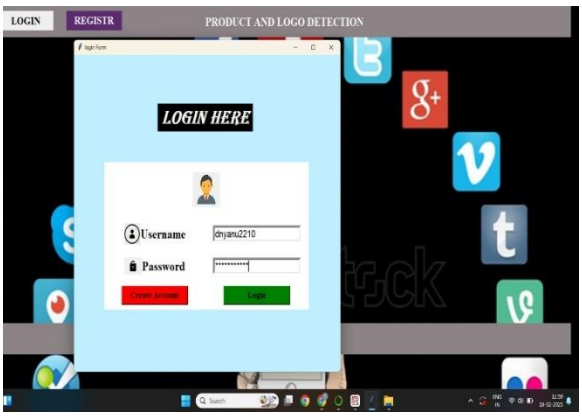
2. A System Architecture for the Detection of Insider Attacks in Big Data Systems *Author: Santosh Aditham Nagarajan Ranganathan*Big data platforms store massive amounts of user data in remote environments managed by service providers. This raises serious concerns about data privacy and security. One of the primary issues is the potential for insider threats from those who have access to the infrastructure itself. Despite its importance, the literature offers limited solutions focused on identifying such internal attacks.

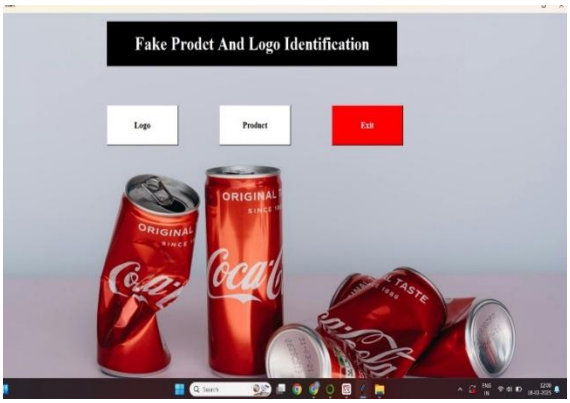
3. Detecting Collaborative Insider Attacks in Information Systems *Authors: Khanh Viet, Brajendra Panda, Yi Hu* Ensuring data confidentiality, integrity, and availability is vital in securing information systems. While much focus is placed on preventing external threats, internal attacks—especially those involving multiple insiders working together—are often overlooked. This paper explores the dynamics of collaborative insider threats by examining system interactions and mapping out how sensitive data might be illicitly transferred.

VI. SYSTEM ARCHITECTURE



VII. RESULT





VIII. ADVANTAGES

1) High Accuracy and Efficiency

ML models can analyze large datasets and identify subtle patterns or anomalies that may indicate counterfeit products.

Reduces human error and increases reliability over manual inspection.

2) Real-Time Detection

Once trained, ML models can detect fake products instantly in real-time scenarios—whether in e-commerce platforms, barcode/QR scanning apps, or supply chain systems.

3) Scalability

Machine learning systems can easily scale to monitor thousands or millions of products across multiple categories and marketplaces without a drop in performance.

4) Automation of Repetitive Tasks

Tasks like image comparison, text analysis of product descriptions, and serial number verification can be fully automated.

5) Continuous Improvement

ML models can learn from new data and get smarter over time, improving detection capabilities with more exposure to real-world cases.

IX. CONCLUSION

Numerous tools are available for the detection of counterfeit goods, but they just photograph the barcode. This study's goal is to suggest a method for build a tool that would record the image of the product QR code and process it using ML and QR code technique to determine whether a product is genuine or fraudulent. This programmed will demonstrate portability and simple to use It will be very beneficial.

REFERENCES

[1] G. Liu, C. Wu, Y. Chen. In their 2022 study presented at the 20th International Conference on Mobile Ad-Hoc and Sensor Networks, the authors introduced a scalable and secure method for product identification that does not rely on blockchain technology.

[2] K. Gupta, A. Singh, R. Verma This 2022 research, featured at the 14th IEEE International Conference on Services Computing, proposes a secure and efficient mechanism for verifying products within supply chains, utilizing verifiable credentials to ensure integrity.

[3] S. Chen, J. Li, X. Wang. Presented at the 25th International Conference on Neural Information Processing (2022), this paper outlines a deep learning-based approach that combines multiple data types to detect counterfeit goods in e-commerce platforms.

[4] R. Sharma, N. Patel, S. Singh at the 16th International Conference on Cryptology and Network Security (2022), the authors offered a privacy-focused product authentication solution for supply chains that does not involve blockchain, maintaining confidentiality without compromising efficiency.

[5] J. Lee, K. Park, Y. Kim During the 12th IEEE International Conference on Cyber Security and Privacy (2023), this team proposed a decentralized method for counterfeit product detection using a distributed ledger system, avoiding blockchain while enhancing security and performance.

[6] Y. Zhang, C. Yang, K. Huang, Y. Li In their publication in *IEEE Transactions on Network Science and Engineering*, the authors introduced an intrusion detection framework for industrial IOT systems based on graph neural networks, improving threat identification through structured data representation.

[7] M. Mohy-eddine, A. Guezzaz, S. Benkirane, M. Azrour This study, featured in *Journal of Computer Virology and Hacking Techniques*, suggests an intrusion detection model leveraging ensemble learning, aimed at edge computing environments in the industrial IoT.

[8] M. Nuaimi, L. C. Fourati, B. B. Hamed Published in the *Journal of Network and Computer Applications*, the authors conducted a thorough review of intelligent intrusion detection techniques specifically tailored for industrial IoT ecosystems.

[9] M. Tanveer, S. Shabala. In a chapter from *Plant Nutrition and Food Security in the Era of Climate Change*, the researchers examined the interactions between essential and nonessential nutrients, discussing how these relationships can impact global food security.

[10] Q. Wang, X. Zhu, Y. Ni, L. Gu, H. Zhu. This review article in *Internet of Things* explores the integration of blockchain technology with both general and industrial IoT, highlighting benefits, limitations, and future research directions.