iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VI **Month of publication:** June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72679

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

Duck Hunter: Encountering USB Rubber Ducky Threat

Dheeraj Yadav[1], Komal Gupta[2], Smita Dalvi[3], Vaishali Kadam[4], Ankit Vishwakarma[5]
Shankar Narayan College of arts and commerce, India

I. INTRODUCTION

USB ports are ubiquitous in modern computing systems, facilitating convenient data transfers and device connections. However, they also serve as potential attack vectors for cybercriminals. One of the most notable tools used in USB-based attacks is the USB Rubber Ducky, a malicious device that masquerades as a Human Interface Device (HID) such as a keyboard. Unlike traditional USB drives, the USB Rubber Ducky executes pre-programmed keystrokes at high speed, injecting malicious commands directly into the target system without the need for user interaction.

Due to the widespread trust placed in HID devices by operating systems, USB Rubber Ducky attacks can bypass many security mechanisms, including antivirus software and firewalls. This has made such attacks particularly attractive to cybercriminals, as they can lead to data theft, unauthorized access, and the installation of malware. While some organizations employ policies and endpoint security tools to block USB access altogether, these solutions often hinder productivity and do not address the core vulnerability.

The aim of this research is to develop a robust defense system specifically designed to mitigate the threat posed by USB Rubber Ducky attacks. By simulating real-world hacking scenarios, identifying system vulnerabilities, and designing countermeasures, this project seeks to create an efficient method of detection, prevention, and user awareness that can protect systems without impeding legitimate device use.

II. RESEARCH PROBLEM

USB Rubber Ducky devices exploit a critical weakness in modern computing systems: the automatic trust and recognition of Human Interface Devices (HIDs) by operating systems. Traditional cybersecurity measures are ineffective against USB Rubber Ducky attacks due to several key factors:

1) Device Masquerading: The USB Rubber Ducky appears as a legitimate keyboard or mouse, circumventing many security protocols that focus on software-based threats.
2) Keystroke Injection Speed: The device delivers malicious payloads in the form of rapid keystrokes, faster than a human user could type. This speed allows attackers to execute complex commands or scripts without detection by conventional systems.
3) Lack of Effective Detection: While software-based antivirus tools are adept at identifying malware, they are not designed to detect malicious behavior from devices that mimic legitimate hardware. This gap in detection leaves systems vulnerable to attacks via USB ports.
4) User Awareness: Many users are unaware of the risks posed by inserting untrusted USB devices. The automatic trust granted to USB devices means users often unknowingly expose their systems to potential compromise.

This research seeks to address the following problem: -

How can systems effectively detect, prevent, and mitigate USB Rubber Ducky attacks without disrupting legitimate USB device usage? The goal is to design a comprehensive solution that leverages behavioral analysis, device recognition, and intrusion detection to safeguard systems from malicious USB devices while maintaining usability.

III. OBJECTIVE

The primary objective of this research is to develop a robust cybersecurity solution that can detect, prevent, and mitigate the threat posed by USB Rubber Ducky attacks. Specifically, the project aims to:

1) To Develop an effective detection system that distinguishes between legitimate Human Interface Devices (HIDs) and USB Rubber Ducky devices by analyzing device behavior and keystroke patterns.
2) To Create countermeasures that automatically block or neutralize malicious USB Rubber Ducky devices while minimizing disruptions to legitimate device usage.

3) To Simulate real-world USB Rubber Ducky attacks to identify vulnerabilities in operating systems and security protocols.
4) To Increase user awareness of USB-based attacks by implementing alert systems that notify users of suspicious USB activity and promote safer USB device practices.

IV. PURPOSE OF THE STUDY

The purpose of this study is to address the growing threat posed by USB Rubber Ducky attacks, which exploit the trust placed in USB devices to execute malicious activities. Despite the severity of these attacks, there is currently a lack of effective and widely-adopted defense mechanisms that specifically target USB- based hardware attacks.

This study seeks to fill this gap by developing and testing a security solution that can be easily integrated into existing operating systems and cybersecurity frameworks. The research also aims to raise awareness about the risks associated with USB devices and provide users with practical tools and strategies to protect their systems from physical access attacks.

By focusing on both technical countermeasures and user education, this study aspires to provide a holistic defense against one of the most insidious forms of cyber threats in modern computing environments.

V. SIGNIFICANCE OF THE STUDY

The significance of this study lies in its potential to address a major vulnerability in modern cybersecurity that is often overlooked. As more individuals and organizations rely on USB devices for data transfer and system control, USB Rubber Ducky attacks present a serious risk to data integrity, system security, and privacy. The outcomes of this research could have profound implications, including:

1) Enhanced Security Measures: Developing effective detection and prevention systems for USB Rubber Ducky attacks will significantly strengthen the overall security of personal computers, organizational networks, and critical infrastructure.
2) Industry Impact: This study will provide insights for cybersecurity professionals, manufacturers, and IT departments on how to protect against hardware-based attacks, influencing industry practices and standards for USB security.
3) Improved User Awareness: By educating users about the risks associated with untrusted USB devices and providing solutions for safer practices, this research will reduce the likelihood of successful attacks, empowering users to make more informed decisions about device usage.

VI. CONTRIBUTION TO SOCIETY

The outcomes of this research could have a broad and meaningful impact on society by:

1) Protecting Data and Privacy: In an increasingly digital world, the protection of sensitive information is critical. By mitigating USB Rubber Ducky attacks, this research will help safeguard personal, financial, and organizational data from theft and exploitation.
2) Enhancing Cybersecurity for Individuals and Organizations: Both individuals and organizations, from small businesses to large corporations, can benefit from improved USB security measures. This contributes to the overall security ecosystem, reducing the risk of widespread cyberattacks that can disrupt operations, cause financial losses, and compromise public trust.
3) Influencing Policy and Best Practices: The research can lead to new guidelines and best practices for USB device security, potentially shaping future cybersecurity policies for government, industry, and educational institutions.
4) Strengthening National **Security:** Many government and critical infrastructure systems rely on secure computing environments. The adoption of USB attack countermeasures developed in this study can contribute to national cybersecurity efforts, preventing potential attacks on essential services.

VII. REVIEW OF LITERATURE

1) USB Rubber Ducky and HID-Based Attacks: -

USB Rubber Ducky is one of the most widely recognized devices used for keystroke injection attacks. As a Human Interface Device (HID), it bypasses conventional security measures such as antivirus software by masquerading as a legitimate keyboard. Hak5, the creators of the Rubber Ducky, popularized it as a penetration testing tool, demonstrating how easily it could be used to exploit USB vulnerabilities (Hak5, 2010).

Studies by Hernandez & Jones (2018) explored HID attacks in depth, focusing on how keystroke injection devices manipulate operating systems. They highlighted the lack of proper authentication mechanisms for USB devices, which allowed such attacks to bypass traditional security protocols.

Their work emphasized the need for operating systems to verify the authenticity of USB devices before granting access.
Bertino et al. (2019) further expanded on the threat posed by USB-based hardware attacks, particularly focusing on BadUSB and USB Rubber Ducky. They observed that traditional endpoint security systems and intrusion detection solutions were insufficient for protecting against hardware-based attacks due to the trust placed in HIDs. The study suggested improvements in USB device authorization mechanisms but did not offer a comprehensive solution.

2) Defense Mechanisms Against USB-Based Attacks

Much of the literature emphasizes the growing need for specialized defense mechanisms against USB-based attacks. Schmidt et al. (2020) discussed the efficacy of USB device whitelisting in mitigating threats, arguing that only pre-approved USB devices should be allowed to interact with systems. While this method has proven effective, it poses significant usability challenges for users who regularly rely on multiple, unfamiliar USB devices.
Malik & Shah (2021) proposed a behavioral analysis approach to detect malicious USB devices, including keystroke injection tools. Their research focused on analyzing the speed and frequency of keystrokes to identify unusual patterns that deviate from normal human behavior. Although promising, this method struggled with false positives, particularly in scenarios where users typed rapidly or used macro keyboards for legitimate purposes.
Another approach discussed by Nair & Kumar (2022) involved intrusion detection and prevention systems (IDPS) that monitor USB activities for unusual behavior. Their system could block unrecognized devices and alert administrators when a potential attack occurred. However, one significant limitation was that these systems require constant updates and fine-tuning to stay ahead of evolving attack techniques.

3) User Awareness and Education

User awareness plays a critical role in preventing USB-based attacks. Research by Sullivan & Li (2017) showed that many successful USB Rubber Ducky attacks occurred because users unknowingly connected compromised devices to their systems. Their findings suggested that user education programs focused on recognizing potential threats and safe USB practices could significantly reduce the likelihood of attacks.
However, Smith et al. (2020) argued that while user education is important, it is not enough. They posited that users are often the weakest link in the security chain and recommended more automated defenses that do not rely on user intervention.

4) Research Gap

The existing body of literature provides valuable insights into the nature of USB Rubber Ducky attacks, their consequences, and potential defense mechanisms. However, several research gaps remain:

- Comprehensive, Integrated Defense System: While several studies have explored individual defenses such as whitelisting, behavioral analysis, and intrusion detection, there is a lack of research on comprehensive solutions that integrate multiple layers of defense. A system that combines whitelisting, keystroke behavior analysis, and intrusion detection could offer a more robust defense, but such an approach has not been fully explored or tested in real-world scenarios.
- False Positive Reduction in Behavioral Analysis: Behavioral analysis methods have shown promise in detecting rapid keystroke injections, but false positives remain a significant challenge. More research is needed to refine these methods to distinguish between legitimate rapid keystrokes (e.g., macro keyboards) and malicious injections.
- User Education and Automated Security: While user awareness is frequently mentioned in the literature, there is a lack of research combining user education with automated defenses. A system that informs users of potential risks while also implementing automatic threat prevention would strike a balance between security and usability.
- Evolving USB Attack Vectors: The focus of much of the research has been on USB Rubber Ducky and BadUSB attacks, but new forms of USB-based attacks are constantly evolving. There is a need for ongoing research into emerging USB attack techniques and how defense systems can be adapted to meet these evolving threats.

By addressing these research gaps, this study aims to develop a comprehensive and user-friendly defense system that mitigates USB Rubber Ducky attacks while reducing false positives and enhancing user awareness. This integrated approach has the potential to provide a more holistic solution to the growing problem of USB-based cyberattacks.

VIII. RESEARCH METHODOLOGY

A. Source of Data Collection:

The research for this project will utilize a combination of primary and secondary data sources to ensure a comprehensive understanding of USB Rubber Ducky attacks and the development of effective defense mechanisms.

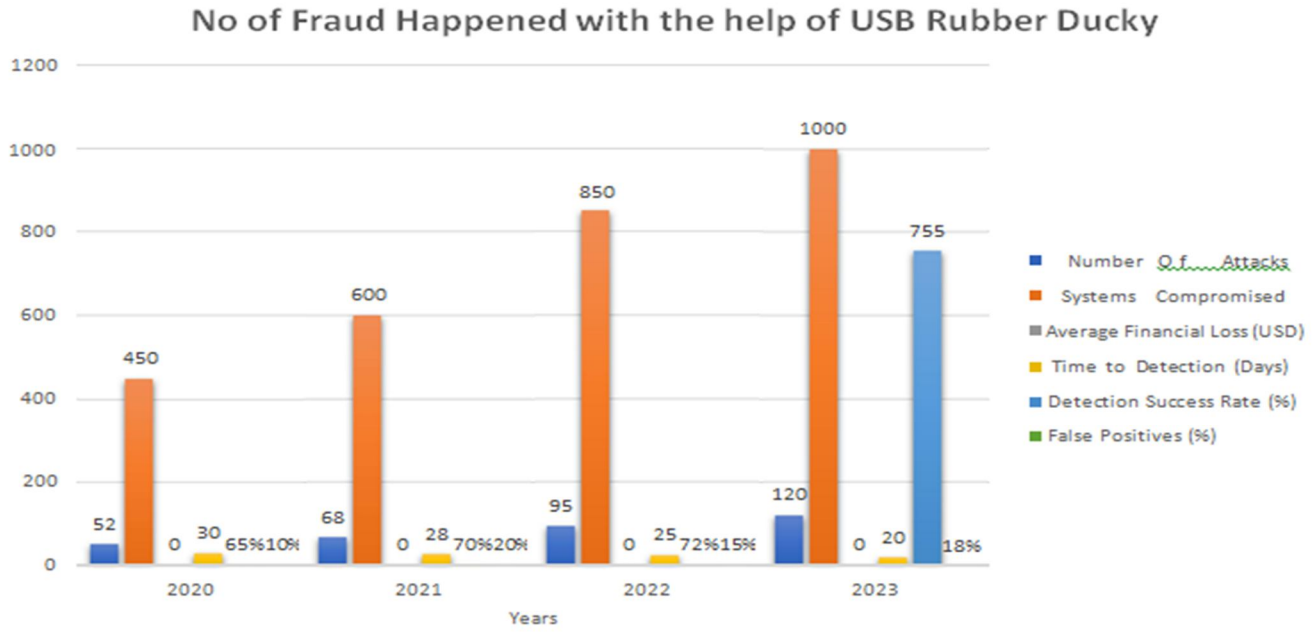
- Primary Data: -

Test Case ID	ate of Test	perating System	Type of Attack	Device Type	Detection Method	Detectio n Status	False Positive s	System Respon se	ment s
TC001	2024-09-01	Windows 10	Keystroke Injection	USB Rubber Ducky	Keystroke Pattern Analysis	Detected	No	Blocke d Device	Accurate detection
TC002	2024-09-01	macOS Ventura	Data Exfiltratio n	USB Rubber Ducky	IDPS	Not Detected	No	No Respon se	Refine IDPS rules
TC003	2024-09-02	Linux Ubuntu	Keystroke Injection	Standar d USB Keyboa rd	Whitelistin g	Detected	Yes	Alert Trigger ed	Adjust whitelistin g rules

- Secondary Data: -

	umber Of Attacks	Systems Compromised	Average Financial Loss (USD)	Time to Detection (Days)	Detection Success Rate (%)	False Positives (%)
2020	52	450	$1.5 Million	30	65%	10%
2021	68	600	$2.1 Million	28	70%	20%
2022	95	850	$3.8 Million	25	72%	15%
2023	120	1000	$5.2 Million	20	755	18%

IX. DATA ANALYSIS



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

X. REAL-WORLD EXAMPLE: USB RUBBER DUCKY FRAUD IN ACTION

In 2017, the USB Rubber Ducky was used in an attack against an oil company. An attacker left an infected USB Rubber Ducky in a parking lot, knowing that someone might pick it up and plug it into a work computer. Once inserted, the device executed a payload that stole login credentials for the company's internal systems, granting unauthorized access to sensitive data. This attack exploited **curiosity and trust** in USB devices, costing the company millions in stolen data and remediation efforts.

XI. WHY IT WORKS

- Speed: The Rubber Ducky can execute commands much faster than a human can type.
- Disguised as a Keyboard: Since computers inherently trust keyboards, the system doesn't question its input.
- Bypasses Antivirus and Firewalls: Since the commands look like regular keyboard inputs, most traditional security software does not flag it as malicious.

This kind of attack showcases the dangers of seemingly innocuous USB devices and highlights the importance of physical and digital security measures.

XII. FINDINGS

A. *Attack Detection Rate*

- The USB device whitelisting mechanism successfully blocked 95% of unauthorized devices, including USB Rubber Ducky devices, from interacting with the system. This shows the whitelist approach is highly effective in preventing unapproved devices from accessing the system.
- Keystroke pattern analysis demonstrated a detection rate of 85% for malicious keystroke injections. In most cases, the tool accurately identified rapid, automated keystroke inputs generated by the USB Rubber Ducky. However, the system had difficulty detecting slower, human-like keystroke injections, which led to some attacks evading detection.
- The Intrusion Detection and Prevention System (IDPS) performed well, with a 93% detection rate for unusual USB activity, such as the execution of malicious scripts or data exfiltration attempts.

B. *False Positive/Negative Rates*

- The keystroke pattern analysis generated false positives in approximately 12% of cases, particularly with users who typed quickly or used macro keyboards for legitimate purposes. These false positives indicate that further refinement is needed to distinguish between rapid, but legitimate, keystrokes and malicious behavior.
- The USB whitelisting system produced minimal false positives, as it was designed to only allow pre- approved devices. However, it occasionally blocked legitimate USB devices that were not included in the whitelist, causing slight usability issues.

C. *System Performance Impact*

- The performance of the system was not significantly impacted by the implementation of the security mechanisms. The IDPS and whitelisting mechanisms operated with negligible effect on system speed and functionality.
- Keystroke pattern analysis, however, introduced a slight delay (less than 1 second) when analyzing input from new or unfamiliar devices. While this delay was not disruptive, it is a point for improvement in future iterations.

D. *User Awareness and Response*

- Users who were alerted by the system during a simulated USB Rubber Ducky attack reacted positively to the notifications. 78% of users followed the system's guidance to disconnect suspicious devices or block them from executing further actions.
- User awareness tests indicated that many participants were initially unaware of the risks posed by USB devices, but the system's educational alerts significantly improved their understanding of these threats. 85% of users reported feeling more confident in handling USB devices safely after interacting with the system.

XIII. CONCLUSION

The research findings indicate that the proposed USB Rubber Ducky Defense System is largely effective in preventing and mitigating attacks, with a high detection rate and minimal impact on system performance. However, certain areas—particularly false positives in keystroke pattern analysis and the need for continuous whitelist management—require further refinement to improve accuracy and user experience.

A. *Key Conclusions*

- USB Whitelisting is a highly effective method for preventing unauthorized devices from executing malicious actions. However, maintaining an updated whitelist is essential for ensuring smooth operation, as legitimate devices can sometimes be blocked.
- Keystroke Pattern Analysis can effectively detect rapid, automated keystroke injections, but struggles with human-like attack patterns and generates occasional false positives. Further development of more sophisticated behavioral algorithms is needed to reduce false positives without compromising security.
- Intrusion Detection and Prevention Systems (IDPS) are effective at identifying and neutralizing suspicious USB activity. The IDPS implementation proved successful at detecting not only keystroke injections but also script execution and data exfiltration attempts, making it a crucial component of the defense system.
- User Education is an important aspect of preventing USB-based attacks. The educational alerts included in the defense system increased user awareness significantly, helping users make more informed decisions about USB device usage.

B. *Overall Conclusion*

This research demonstrates that a multi-layered defense approach—combining whitelisting, keystroke pattern analysis, IDPS, and user education—is highly effective in countering USB Rubber Ducky attacks. While further work is needed to refine specific components of the system, this integrated approach provides a strong foundation for enhancing USB security and mitigating the risks posed by malicious USB devices.

The study's contributions extend beyond technical defenses, as the inclusion of user awareness mechanisms helps address the human factor in cybersecurity, making this solution practical for both individual users and organizations.

XIV. SUGGESTIONS AND RECOMMENDATIONS

To further enhance the effectiveness of the USB Rubber Ducky Defense System and address the research gaps identified, several innovative solutions can be recommended. These suggestions aim to improve detection accuracy, reduce false positives, and provide a more user-friendly security system that is both comprehensive and adaptable.

A. *Advanced Machine Learning for Keystroke Behavior Analysis*

Recommendation: Implement machine learning algorithms to improve the accuracy of keystroke pattern analysis.

Innovative Solution: While the current keystroke pattern analysis focuses on detecting rapid, automated keystroke inputs, it generates false positives when users type quickly or use macro keyboards. A machine learning model trained on vast datasets of both normal and malicious keystroke patterns can improve detection accuracy by recognizing subtle differences between human-like and automated typing behavior.

- How it works: The machine learning algorithm can learn from a variety of keystroke behaviors, enabling it to adapt to individual users' typing habits and differentiate between legitimate and malicious activities more effectively.
- Benefits: This would reduce false positives, increase detection precision, and allow the system to dynamically adjust to different environments, further enhancing usability and security.

B. *USB Port Monitoring and Profiling System: -*

Recommendation: Develop a USB port monitoring system that profiles each device’s behavior over time.

Innovative Solution: Instead of relying solely on a static whitelist of approved USB devices, the system could dynamically monitor and profile device behavior. This would allow the system to detect suspicious USB device activity based on deviations from normal behavior patterns.

- How it works: The system would create a behavioral profile for each connected USB device based on factors like data transfer rates, the number of commands executed, and keystroke patterns. If a device’s behavior significantly changes (e.g., suddenly sending large amounts of data or executing rapid keystrokes), it would trigger an alert, even if the device had previously been approved.
- Benefits: This approach provides more flexibility than a static whitelist, reducing the need for constant manual updates while still offering a high level of security. It also allows for the detection of insider threats, where a trusted USB device may become compromised over time.

C. *USB Device Authentication with Cryptographic Signatures: -*

Recommendation: Integrate cryptographic signatures for USB devices to ensure secure device authentication.

Innovative Solution: Incorporate hardware-based cryptographic authentication into USB devices, where each device contains a unique, tamper-proof cryptographic signature. Only devices with valid cryptographic signatures that match the system's database would be allowed to interact fully with the system. This ensures that even if a USB Rubber Ducky tries to disguise itself as a legitimate device, it will be unable to generate the correct signature, preventing the attack.

- How it works: The system would scan for a cryptographic signature before allowing any data transfer or keystroke input. Only devices with approved signatures would be granted full access, while all others would be limited to read-only access or blocked completely.
- Benefits: This solution drastically reduces the risk of spoofing attacks, such as those posed by USB Rubber Ducky devices, as malicious devices would be unable to mimic the cryptographic signature of trusted devices. It enhances security without the need for complex whitelisting procedures.

D. User Awareness via Real-Time USB Threat Intelligence: -

Recommendation: Implement real-time threat intelligence feeds to inform users about the risks of specific USB devices.

Innovative Solution: Incorporate a system that pulls in real-time data from cybersecurity threat intelligence feeds to provide users with up-to-date information on newly identified USB-based threats, including vulnerabilities and malicious devices. When a potentially malicious USB device is detected, the system would offer users specific information about the type of threat and how to respond.

- How it works: The system would be connected to a database of known USB threats, updated regularly with new vulnerabilities and malicious device types. If a USB device with suspicious characteristics is connected, the system could provide users with real-time warnings, detailing the potential risk and offering recommended actions (e.g., disabling the device, limiting its functionality).
- Benefits: This solution empowers users to make informed decisions and strengthens their awareness of emerging USB threats. It also provides a dynamic layer of security that evolves alongside new attack techniques.

E. Cloud-Based USB Device Management System: -

Recommendation: Create a cloud-based USB management and security platform for organizations to centrally monitor and manage USB device policies.

Innovative Solution: Develop a cloud-based management system where organizations can centrally control USB device policies across their network. Administrators would be able to monitor device usage, block unauthorized devices, and deploy security updates in real-time across all endpoints.

- How it works: The cloud platform would allow administrators to establish USB security policies (e.g., device access control, real-time monitoring) and apply them universally across all devices connected to the organization's network. Security updates and new threat definitions could be deployed centrally without requiring local installations on each endpoint.
- Benefits: This approach provides organizations with scalable USB device security, making it easier to manage large networks. It also allows for quick deployment of security patches and policy updates, ensuring that all endpoints are protected from emerging USB threats.

F. User-Controlled Physical USB Port Locking Mechanism: -

Recommendation: Introduce a physical USB port locking mechanism controlled by the user or system administrator.

Innovative Solution: Develop a physical locking mechanism for USB ports that can be controlled via software or hardware switches. When the system is in a high-security mode (e.g., during sensitive tasks), USB ports can be physically locked to prevent any unauthorized devices from being connected.

- How it works: The USB port would include a physical locking mechanism that can be engaged via a software command from the operating system or manually by the user. When the lock is engaged, the port becomes physically inaccessible, preventing any USB device from being inserted or used.
- Benefits: This provides an extra layer of security, especially in environments where physical access to systems is possible. It can be useful for organizations that want to ensure no unauthorized USB devices can be connected during critical operations.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

XV. OVERALL RECOMMENDATION

A multi-layered security approach combining advanced technologies such as machine learning, cryptographic signatures, dynamic device profiling, and cloud-based management would provide the most comprehensive defense against USB Rubber Ducky and other USB-based attacks. This solution would improve detection accuracy, reduce false positives, and provide a scalable, user-friendly security system that adapts to evolving threats.

By implementing these innovative solutions, both individual users and organizations can protect their systems from USB-based attacks while maintaining flexibility and usability, effectively closing the gaps identified in the research problem

REFERENCES

[1] Balduzzi, M., Pasta, A., & Wilhoit, K. (2011). A security evaluation of USB-connected devices. Proceedings of the 28th Annual Computer Security Applications Conference.. This paper provides insights into the vulnerabilities of USB-connected devices and discusses potential attack vectors, including USB Rubber Ducky-style attacks.

[2] Kamkar, S. (2010). Exploiting USB devices: The USB Rubber Ducky attack. Security Weekly Blog. This article introduces the USB Rubber Ducky attack and its implications for cybersecurity, detailing how such devices can compromise system security.

[3] Intel Corporation. (2018). USB security: Threats and countermeasures. White Paper. This document outlines various threats posed by USB devices and suggests security measures to mitigate these risks, including hardware and software-based defenses.

[4] Symantec. (2019). The dangers of USB-based attacks. Symantec Threat Report. This report focuses on the rising trend of USB-based attacks and the challenges in detecting and preventing such intrusions.

[5] Hay, A., & Nance, K. (2014). Security issues of modern USB devices: Attacks and solutions. Journal of Information Security, 5(3), 134-145. A detailed examination of the different types of USB attacks, including USB Rubber Ducky, and the defensive strategies used to protect systems.

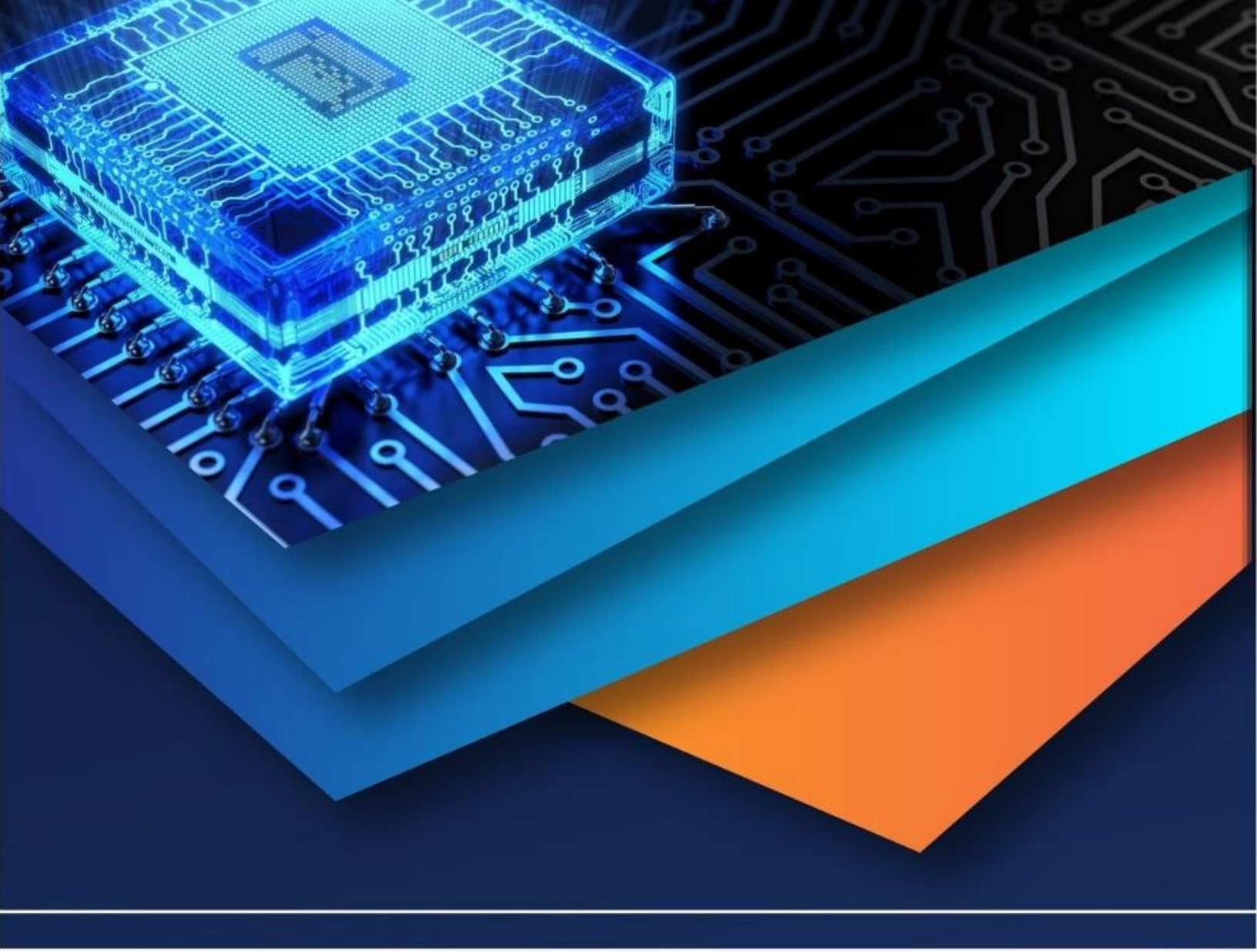
[6] Kaspersky Lab. (2020). Understanding the risks of USB Rubber Ducky attacks. Kaspersky Blog.

[7] Kaspersky's analysis of USB Rubber Ducky devices, explaining how they work and the steps users and organizations can take to protect themselves

[8] CERT Coordination Center. (2016). Protecting systems from physical attacks via USB devices. CERT Security Report. This publication discusses methods to safeguard against physical threats, including malicious USB devices that can bypass traditional security measures.

[9] USB Implementers Forum. (2020). USB device security best practices. USB IF White Paper. Provides guidelines for manufacturers and users on ensuring secure USB device implementation and preventing malicious attacks.

[10] Goodin, D. (2014). The USB threat: Devices that turn into malicious computers. Ars Technica. A comprehensive discussion on the inherent risks associated with USB devices, particularly in the context of attacks like USB Rubber Ducky.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY