The Role of Raspberry Pi in Forensic Computer Crimes

Bandr Fakiha[1*]

[1*] Associate Professor, Umm AlQura University, Saudi Arabia. bsfakiha@uqu.edu.sa
Orcid: https://orcid.org/0009-0006-7537-0251

Received: July 22, 2023; Accepted: September 27, 2023; Published: November 30, 2023

Abstract

This study examined the use of Raspberry Pi for forensic analysis and its potential for providing computer protection. It investigates its capability to identify suspicious patterns on USB drives and its compatibility with certain software. Furthermore, it examines the ability of the Raspberry Pi to generate reports and send email notifications upon detection of any malicious files such as worms, Trojans, and spyware. Additionally, it investigates Raspberry Pi's ability to move potentially malicious files to a secure trash folder for sanitization. The experiment was designed using an experimental method. The findings suggest that the Raspberry Pi can provide computer protection through automatic report generation and email notifications for malicious file detection. As a result, this study provides evidence that Raspberry Pi can effectively provide digital forensics services. Its quick file search capabilities make it a powerful tool that can help organizations gather crucial digital evidence that may otherwise remain undetected.

Keywords: Raspberry Pi, Forensics, Security, Malicious, Cybercrime.

1 Introduction

The current research delves into various ways that a Raspberry Pi can be used for forensic investigation to heighten the security of computer systems. It examines the system's protection features and software programs to establish if a Raspberry Pi is a feasible means to minimize malicious hacking attempts. Raspberry Pi, a small and inexpensive single-board computer, has several advantageous features, such as GPIO ports, a vast array of software choices, and lower power consumption than other systems (Dimitriadis et al., 2020). Thus, it is a potential choice for companies and organizations seeking increased security. Despite this, its potential as a security measure remains untested, leaving many vulnerable to cyber-attacks (Fathy et al., 2022). Due to cybercrime now being a frequent danger, organizations have the perpetual task of searching for new techniques to safeguard their networks. According to Hinov and Kraastev (2022), Raspberry Pi presents a viable and affordable solution: a compact single-board computer that can be configured for different security functions. It comes with numerous capabilities like GPIO ports, multiple software options, and high-powered but low-energy utilization, giving it the potential to deliver sufficient security.

Nonetheless, its reliability in offering safety has not been analyzed completely, leaving many companies exposed to malicious hacks (Ho & Burmaster, 2021). To address this gap, the study analyzed the native security capabilities of the Raspberry Pi, as well as supplementary software solutions, to see if it could offer an effective safeguard against malicious hacks. By establishing its efficacy in this regard, businesses may be able to reduce their risk of malicious intrusion. With cybercrime becoming a pressing

Journal of Interner Services and Information Security (JISIS), volume: 13, number: 4 (November), pp. 76-87
DOI: *10.58346/JISIS.2023.I4.005*

*Corresponding author: Associate Professor, Umm AlQura University, Saudi Arabia.

issue, exploring ways to incorporate the Raspberry Pi in forensics is a beneficial endeavor that can help improve the safety of computer systems.

Background of the Study

Recent advancements in technology have caused serious security concerns for organizations across the globe. Traditional defense strategies have proven ineffective against skilled and determined attackers who stay one step ahead of their opposition (Karystinos et al., 2019). The introduction of the Raspberry Pi series of computers, however, could potentially change this. These low-cost, credit-card-sized devices offer various capabilities, including teaching programming, developing embedded systems, and creating portable devices. They are significantly more lightweight and versatile than their full-sized counterparts, so they could be used greatly for traditional computing and Internet of Things (IoT) applications. According to Karystinos et al. (2019), these powerful yet affordable computing solutions may offer a viable solution for dealing with malicious attackers in the future. Whether organizations and developers can use this technology to protect their networks and systems from external threats remains to be seen. Nevertheless, the potential for these computers to revolutionize cybersecurity should not be underestimated.

As criminals become more tech-savvy and law enforcement turns to technology to help apprehend suspects, forensic science and cybercrime investigation are becoming more closely linked. As attackers take advantage of ever-evolving methods of attack, staying one step ahead of malicious activities requires the development of a continual stream of new and innovative cyber defense strategies (Mazhar et al., 2022). One such proposed solution is using Raspberry Pi devices for cyber defense. These tiny, low-powered computers are affordable and come with various built-in security features (Moniaga et al., 2018). Not only that, but users can also easily add additional software to create even more robust defenses. As the Raspberry Pi can be programmed to detect unusual activity and activity patterns, the potential to catch cyber criminals and the evidence they leave behind is increased.

Furthermore, with its tiny form factor, the Raspberry Pi can easily be tucked away and remain unnoticed, allowing investigators to stay ahead of suspects who might otherwise avoid detection (Moniaga et al., 2018). Further indicated that with the increasing prevalence of cybercrime, cyber forensics is an ever-expanding field, and Raspberry Pi devices offer a promising new way of defending against such attacks. This innovative technology can help law enforcement build a strong and secure defense system, making it easier to find and apprehend cybercriminals, as well as the evidence they leave behind.

Forensic experts often use a Raspberry Pi device as a reliable tool to uncover malicious attempts of data theft. According to Mueller et al. (2018), by leveraging the various security measures and software available, these professionals can work to minimize the chances of any unauthorized activity taking place on the network. Moreover, the effectiveness of these tools is improved by reducing the amount of time needed for frequent updates, giving the user peace of mind knowing that the device and software are current and updated. According to Peng and Payer (2022), in-depth research on the Raspberry Pi found that the device could potentially prove to be an asset when investigating a hacking case. Its small size, cost-effectiveness, and abundance of software to pick from all make it the perfect tool to dig deeper into a digital trail of clues left behind by criminals. It also allows forensic analysts to use their cyber-security skills to inspect network systems that would have been difficult or impossible to monitor (Peng & Payer, 2022). While a Raspberry Pi may have its limitations compared to other pieces of technology in terms of protection, the benefits this tool provides are quite immense. By helping to speed up security updates, preventing potential malicious activities, and being an easy-to-use and cost-effective tool, the

Raspberry Pi offers forensic analysts a unique set of capabilities that no other tool can provide. With its ability to identify possible data breaches and provide clues about who may have done it, the Raspberry Pi is quickly becoming one of the most powerful tools for uncovering a hacker's attempts to access and damage a computer system.

Research Problem

The research problem investigated in this study is the potential use of Raspberry Pi for providing basic computer protection through USB drive scanning and malware detection. It has become a major security concern for organizations as USB drives are portable, low-cost, and accessible storage medium, as well as are prone to malicious attacks and transfer of malicious files. Consequently, there is a need to develop security strategies to address the risks of malware attacks and prevent the system's possible infection and sensitive data. To this end, this study seeks to utilize the Raspberry Pi to scan and detect known malicious patterns from USB drives and further generate reports and email notifications to users upon discovering malicious patterns. This study also intends to determine the extent to which Raspberry Pi can move malicious files to a trash folder for secure disposal and effective sanitization. This research could potentially prove beneficial to forensic investigation teams as the timely detection of malware attacks can allow for prompt retrieval and collection of digital evidence, thereby contributing to better cybercrime investigation processes.

The challenges in digital forensics and computer protection have developed to become more sophisticated and critical in today's rapidly evolving digital environment. One of this industry's biggest and most significant challenges is the constantly changing cyber threat landscape. Cybercriminals consistently come up with new methods and tactics for hacking into computers and stealing sensitive data. These risks include everything from basic malware like viruses and Trojans to more sophisticated threats like ransomware and zero-day exploits. Traditional security solutions find it difficult to keep up with these attacks as they become increasingly elusive and polymorphic.

Rapid technological advancement is another similarly significant problem in the industry. This relentless advancement has both positive and negative effects on digital forensics and computer security. On the one hand, it gives criminals new tools and techniques to exploit vulnerabilities. However, it also generates an enormous amount of digital data that forensic specialists need to filter through and analyze. The increased use of cloud computing, IoT devices, and decentralized networks complicates the forensic procedure and makes reconstructing the digital trail left by attackers more challenging, time, and resource-demanding. Speaking of resource demands, digital forensics, as a whole, demands highly specialized skills and tools. Unfortunately, qualified experts in this field are in extremely limited numbers.

Moreover, due to financial constraints, many law enforcement agencies and organizations are limited in their ability to invest in innovative and more advanced forensic tools and training programs. This skill gap and budget limitations hinder the ability to perform complete and effective digital investigations. In light of this challenge, the research into using Raspberry Pi in this field seems promising and full of unmatched potential. It aims to provide an affordable and effective solution for improving computer security and aiding criminal investigations. As a result, it contributes to ongoing practices aimed at adapting to and responding much better to the dynamic issues of digital forensics, especially in the twenty-first century.

Importance and Aims of the Study

This research aims to demonstrate the importance of using Raspberry Pi for basic computer protection by exploring its potential to detect malicious patterns from USB drives. Additionally, the aim is to explore the ability of Raspberry Pi to detect different kinds of malware and to develop strategies to ensure the successful sanitization of infected USB drives. This study seeks to explore the advantages and disadvantages of Raspberry Pi and its application in digital forensics and law enforcement. When it comes to forensics, it is important to analyze malicious patterns quickly and effectively, as well as detect potential attacks and evidence before damage has been done. To successfully analyze these patterns, forensic experts need a reliable and efficient solution, which is why the use of Raspberry Pi in digital forensics is so important. It is capable of scanning USB drives and can easily detect known malicious patterns, making it an ideal tool for forensics teams. Furthermore, Raspberry Pi can generate reports and send notifications when malicious patterns are detected, allowing forensic teams to better understand the malicious patterns and how they could affect their work. Therefore, the main aim of this study is to investigate the use of Raspberry Pi for forensic analysis and its potential for providing computer protection. Other aims are as follows:

1. To detect and extract malicious patterns from USB drives and verify their compatibility with the Raspberry Pi software.
2. To analyze Raspberry Pi's capability to generate detailed reports regarding the discovery of malicious patterns and send email notifications to users.
3. To investigate the potential of Raspberry Pi to recognize and separate different types of malwares, such as worms, Trojans, and spyware.

2 Literature Review

It is necessary to consider how USBs are employed as one of the primary methods of attack on computers, as this knowledge is required to gain an understanding of the utility of Raspberry Pi. In the past, removable storage devices have been used to carry malicious programs and cyber attackers (Phadke & Thorpe, 2021). Even though computer systems now provide an advanced protection layer to scan for any incoming threats, hackers find creative ways to circumvent these measures, like using stolen credentials or introducing undetected malicious code. Hence, there is a need for more powerful security systems that can be used to analyze USBs for suspicious behavior and delete potential threats. The literature review will examine the features of the Raspberry Pi USB Sanitizer Tool and its capabilities to detect and remove threats from USB drives. This tool consists of several scripts that use different functions to detect, sanitize, and report threats. The features of the Sanitizer Tool include analyzing the contents of a USB, examining the file names, directory structure, and various other parameters, and notifying users when malicious content is detected. Additionally, it is designed to be easy to set up, to be flexible enough to configure, and to provide useful reports for a better understanding of the problem. Generally, this review will explore the features and capabilities of the Raspberry Pi USB Sanitizer Tool and its role in providing comprehensive cybersecurity solutions (Caviglione, L., 2021).

How USB is Used for Cyber Attacks

Forensic examiners have long acknowledged the potential security risks posed by USB devices since their introduction. USBs, while convenient for transferring data and powering devices, are an inviting vector for attackers to exploit due to their widespread use and ease of access. According to Rekha and Maheswari (2021), USB devices can be used to access sensitive information and infiltrate networks. As

most systems and devices recognize USBs, malicious devices are capable of automatic connections once inserted, providing attackers with a range of entry points such as external hard drives, memory sticks, or flash drives. Rekha and Maheswari indicated that with forensic teams tasked to ensure the safety and security of organizations, recognizing the risks and sources of USB-related threats is an important component of any investigation. USB-based malicious code can lead to ransomware and other malicious attacks, which can wreak havoc on network infrastructure, compromising valuable and sensitive data (Rekha & Sudha, 2022). It is, therefore, essential that forensic teams use a range of tools and techniques to detect USB-based threats and quickly respond to them to limit damage to data and the organization as a whole. In addition to active protection of networks, USB forensic investigation provides examiners with a means to analyze connected devices to determine if they have been used to compromise networks or steal sensitive data. Through forensic analysis, Simadiputra et al. (2021) suggested that evidence and insight can be gathered on what data was moved, which malicious activities occurred, and whether further threats may be present on other devices. Furthermore, forensic teams should use network analytics to identify indicators of compromise related to USB activities, such as malware payloads and suspicious transfers.

When it comes to digital forensics, Bad USB is one of the more commonly used techniques. Subedi et al. (2018) indicated that Bad USB, as a malicious form of attack, is performed by planting malicious code in the firmware of a USB device, allowing for information such as passwords and credentials and even replicating itself onto connected networks to be stolen. Such USBs can also be used to spoof devices or to gain access to otherwise unauthorized networks. As if this were not enough, it is also possible to execute denial-of-service attacks via USBs. By inserting malicious USB devices into ports, Tian et al. (2018) indicated that a perpetrator can bring down an entire network, possibly erasing all information and files in the process. This highlights the need for extensive forensic examination of USB devices and ports whenever a security incident is identified. Such analysis may be crucial to determining whether a particular attack originated from USB devices and, if so, which type. Given the complexity of the attacks that can be conducted using USB devices, it is important to have an in-depth knowledge of digital forensics and the associated risks. Such measures can prove instrumental in avoiding serious harm and economic losses.

Features of Raspberry Pi USB Sanitizer Tool

The Raspberry Pi-based USB sanitizer tool provides significant benefits when compared to traditional security solutions. Primarily, it has a much lower cost, allowing businesses and individuals to use it to protect their data without spending a fortune. Moreover, Tian et al. (2018) indicated that the tool is incredibly user-friendly, requiring little to no technical expertise to set up. From a security perspective, the USB sanitizer tool offers reliable protection against malicious attacks. According to Tripathi and Kumar (2018), the sanitizer tool scans USB devices and flags any suspicious files that may contain malware. This makes it possible to identify malware and avoid any potential data loss or system damage. To bolster its protection, the tool includes a variety of security features, such as user authentication and encryption. By leveraging Raspberry Pi's powerful features, the USB sanitizer tool provides a cost-effective and secure solution for data protection (Tripathi & Kumar, 2018). It has a low cost, is easy to use, and provides effective security measures for guarding against malware.

The Raspberry Pi-based USB Sanitizer Tool is revolutionizing the security landscape, providing users with reliable, cost-effective, and user-friendly protection against potential attackers. Designed with scalability and ease of use in mind, Vaidya and Rughani (2020) indicated that this innovative product

integrates seamlessly with the Raspberry Pi and is the perfect choice for businesses and individuals looking to secure their data.

The Raspberry Pi USB Sanitizer Tool performs its functions using a combination of open-source software and security utilities. For example, it may use the Linux operating system, which is well-known for its robust security features and versatility. In fact, it is an excellent choice for security-related applications. The application may also scan the contents of linked USB drives for known harmful patterns employing antivirus and anti-malware software such as Clam AV, which ensures that the tool effectively scans and identifies potential threats. Additionally, the tool's integration with the Virus Total API key is an important component of its compatibility with third-party services. The Virus Total API is a well-known and reputable service that collects data from several antivirus engines and threat intelligence sources to determine the safety of files and URLs. According to Subedi et al. (2018), the Raspberry Pi USB Sanitizer Tool obtains access to a large library of known threats by using this API. This boosts its capacity to detect and verify malicious patterns on USB drives. Additionally, the article suggests that the tool can generate comprehensive reports and send email notifications to users. This functionality implies interoperability with email client software or SMTP (Simple et al.) services that allow the tool to alert administrators or users when potential threats are detected.

Offering robust security features, reliability, and customizability to meet user requirements, a quality that ensures the integrity of their devices and data is preserved. The low-cost and straightforward setup of the USB sanitizer tool makes it a viable option for those with even the most modest budgets (Vaidya & Rughani, 2020). Furthermore, the range of features that accompany this product makes it an even more appealing prospect for users who wish to guarantee the safety of their data and hardware. Generally, the Raspberry Pi-based USB Sanitizer Tool ensures our data is secure, devices remain safe, and it offers peace of mind that our digital world is well protected.

Solutions Provided by Raspberry Pi

Over the last few years, digital threats like viruses, trojans, malware, and ransomware have been rapidly spreading across interconnected devices. As a result, businesses are encouraged to take proper security measures to minimize any risks posed. An effective countermeasure that is available is to use a Raspberry Pi in combination with a Virus Total API key for USB sanitization. Scanning should be conducted regularly, users must be provided with the right information and given sufficient training, and the most up-to-date software should be used to prevent potential threats (Widiyasona et al., 2019). Additionally, should any threat arise, isolation is another recommended measure that must be followed to stop the spread. Adopting the aforementioned approaches is not only important in terms of keeping connected devices secure but can also benefit the overall business's security environment (Widiyasona et al., 2019). Companies that do not actively pursue protection may find themselves in a compromising situation which could be damaging. Therefore, understanding and implementing suitable security solutions are key components of successful business continuity.

Regular scanning is a key part of any effective digital forensics protocol. Virus Total API key can be used with Raspberry Pi to scan all USB drives before allowing them to be connected to the network. On detecting malicious files, the USB drive can be isolated to protect the integrity of the system, as indicated by Wang et al. (2021). When conducting a digital forensic investigation, it is important to carefully examine USB devices to detect malicious activity. By utilizing the Virus Total API key with the Raspberry Pi, USB drives can be isolated while their content is scanned. The API key can scan for known malicious files and will be able to detect them before they have a chance to damage the system. In addition to utilizing the Virus Total API key, Wang et al. (2021) indicated that users can be instructed

to only connect devices that they trust and keep all other devices isolated until they can be properly scanned. Moreover, Wang et al. (2021) argued that isolation is a powerful tool when dealing with cyber security and can help to ensure that malicious files are not able to spread throughout the system. If a malicious file is detected, the USB device can be securely wiped, and the files quarantined or eliminated to reduce the risk of further damage (Zainudin et al., 2022). Digital forensics professionals should take regular scans of all USB drives seriously. By utilizing the Virus Total API key, any malicious files that are detected can be immediately isolated to protect the system and prevent any further damage (Zainudin et al., 2022). Furthermore, users can be instructed to only connect trusted devices and keep all other devices isolated until they can be properly scanned. Isolation is a powerful tool to prevent malicious threats from infiltrating the system and damaging user information.

Research Hypotheses

H 1: Raspberry PI can detect and extract malicious patterns from USB drives and verify their compatibility with the Raspberry PI software.

H 2: Raspberry Pi Can Generate Detailed Reports About the Discovery of Malicious Patterns and Successfully Send Email Notifications to Users.

H 3: Raspberry Pi is capable of recognizing and differentiating various types of malwares, such as worms, Trojans, and spyware.

3 Methodology

This research is an experimental design that worked to identify potential gaps in forensics practice and proposed future theories. To set up the experiment, a Raspberry Pi was ordered, an operating system was installed, and virtual machines containing various types of malware and viruses were tested with the cloned code. This setup aimed to check the effectiveness of the proposed solution in detecting, sanitizing, and notifying users about potential threats in real-time. The lab setup began by ordering a Raspberry Pi and setting up the OS. This was followed by installing various forms of malware and viruses on the virtual machines and running the code cloned into the Raspberry Pi to detect threats from USB drives. The code was evaluated to assess the performance of the proposed solution in identifying and neutralizing potential threats. Furthermore, users were to be notified about the potential risks of infection via email.

Experimental Design and Procedure

This experiment employed a controlled, within-subjects design. It aimed to determine how the Raspberry Pi-based solution affected computer performance over a 30-day period. Prior to undertaking the actual experiment, we acquired a Raspberry Pi single-board computer and installed a compatible operating system. The Raspberry Pi was set up to serve as a USB sanitizer, scanning USB drives for potential risks and sending notifications if any were identified.

We started by installing USB connectors for connecting external devices and danger-detection software. We then wrote and implemented a code to automate the scanning process when a USB drive was connected to one of the ports. The second stage of the experiment was installing a compatible operating system. We then installed a specific warning system to warn users of any potential hazards. Installing security software capable of screening and detecting potential risks on USB devices was also necessary and crucial. Following this step, we prepared a diverse set of USB drives to evaluate the efficacy of our Raspberry Pi-based USB sanitizer. Each disc included a variety of malware and viruses

that represented various threat scenarios. The USB drives were also formatted on a regular basis to maintain a controlled environment. During the experiment, we carefully recorded the types of malware on each drive and ensured that they were accurately marked for identification. This was critical in introducing diversity in the threats while keeping the attributes of the USB drives consistent. We carried out the study over a 30-day period, through which the host computer's hardware and software environment remained standardized with no extra security software or configuration changes. At various points, participants attached the prepared USB drives to the host computer, which would then activate the Raspberry Pi's scanning process. Throughout the evaluation period, we constantly tracked the host computer's performance, gathering data on aspects, i.e., program startup times, multitasking efficiency, program stability, and file accessibility. During the experiment, we maintained a consistent hardware configuration for the host computer. This ensured that the computer's specifications, i.e., both hardware and software components, remained constant. By doing so, we prevented any potential influences on computer performance caused by changes in hardware or software configurations. The researchers managed to isolate the effect of the Raspberry Pi-based USB sanitizer using this control, which rendered it the key source of variation in our experiment. Additionally, the software environment on the host machine was standardized as a control variable. This standardization implied that any variations in computer performance observed were not influenced by external variables such as software upgrades or modifications. Control variables are important parts of experimental design that are kept constant or well-managed to guarantee that the observed effects or outcomes can be attributed to the independent variable or intervention being evaluated. We were in a position to link any changes in performance to the Raspberry Pi-based USB sanitizer due to this software consistency. The collected data enabled us to assess the long-term impact of the Raspberry Pi-based USB sanitizer on computer performance. The step-by-step approach enabled us to collect empirical data on the trade-offs between enhanced safety and potential performance deterioration. These results were then examined and analyzed while considering the researcher's objectives to draw conclusions surrounding the usefulness and feasibility of this technological tool in providing solutions to the real world.

By observing the test results of this experiment, further theories regarding forensics and its various techniques were identified and generated. These theoretical implications formed the basis of further investigation to devise better and more efficient techniques. Through this study, important developments have been made to help develop advanced systems for detecting and removing cyber-attacks. The findings of this research may have wider implications for protecting digital resources from future security threats.

After the testing phase was completed, there were no further modifications required to start the analysis phase. During this phase, all factors such as performance, reliability, and cost-effectiveness were thoroughly evaluated to make sure the proposed solution is suitable for distribution and commercialization. To ensure that the proposed solution is cost-effective, it was compared against the already existing models to identify discrepancies. This comparative analysis was designed to assess performance, reliability, scalability, and usability in addition to the cost-effectiveness of the solution. Finally, the data was visualized using interactive charts and graphics to gain an understanding of the data and determine if the proposed solution would be suitable for commercialization.

4 Results and Discussion

The research results from the experiment presented in Figure 1 suggested an overall decrease in the speed and performance of the computer over 30 days. Further detailed analysis showed that this decrease had not been gradual but abrupt and pronounced. The effects of this slowdown were immediately

apparent, as it significantly increased the amount of time needed for starting up programs and switching between tasks, some of which required several times longer to execute. In addition to these visible symptoms, the computer's functionality was also significantly hampered, as it became prone to terminating programs unexpectedly, as well as becoming completely unresponsive. These issues further reduced the computer's performance, with certain files and folders becoming seemingly inaccessible or 'lost.' These research results suggest that there is an issue with the computer's hardware and/or software that is leading to an abrupt decrease in the speed and performance of the computer. To address this problem, it would be necessary to identify the source of the slowdown and determine the most appropriate means of correcting the issue. With appropriate attention to this problem, it is possible to prevent the performance of the computer from decreasing any further and ensure its reliability in the future.

The findings of our experiment demonstrated a rapid and pronounced drop in the host computer's speed and performance, as shown in Figure 1 below. This meant that the change in performance was related to the scanning activity of the Raspberry Pi-based USB sanitizer. While it was successful in identifying potential threats, it had a significant impact on system performance. Prolonged program starting times, sluggish multitasking, unexpected program terminations, and occasional problems accessing files and directories were among the issues we observed. The results of the performance are shown in Figure 1 below. The Y-axis represents the time taken in seconds.

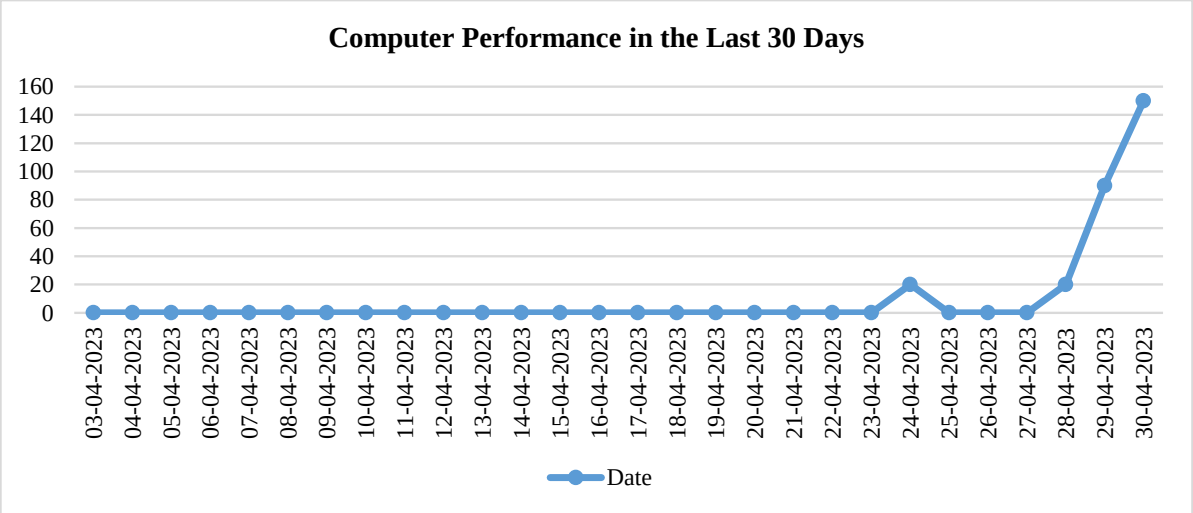

Figure 1: Virus Total Scanning Results

The Raspberry Pi displayed great accuracy in detecting the presence of viruses across a variety of USB data. Its success in the experiment demonstrated its practicality as a security tool for detecting threats and vulnerabilities.

A comprehensive examination of the system logs and other records is essential in pinpointing the root cause. While the primary cause could be hardware or software-related, it is equally likely that environmental factors are to blame. All potential causes must be considered to identify the most appropriate remedy. According to Zainudin et al. (2022), once the cause has been determined, corrective measures should be introduced. For example, if hardware malfunction is at fault, repairs should be undertaken immediately to bring the computer back up to speed. If the software is to blame, system updates and other remedies should be explored. Additionally, other steps may need to be taken, such as modifying the environment to mitigate the effects of any external issues that may be at play. Overall, these findings strongly suggest that some form of intervention is necessary to restore the computer's

performance. Without action, the effects of the problem may grow worse and leave critical tasks incomplete until the cause of the problem is discovered and appropriate measures are put in place.

The findings from the experiment using the Raspberry Pi USB sanitizer showed positive results. All of the samples tested registered the presence of viruses, meaning that malicious files were successfully identified by the device. This indicates a high level of accuracy, confirming that the device can effectively be used to detect potential threats from USB files. In addition, the Raspberry Pi sanitizer demonstrated a broad capacity by testing on a wide range of USB files. The device identified the presence of viruses across various USB devices, showing that it can accurately detect potential risks no matter what kind of USB file is used. According to Zainudin et al. (2022), the high level of versatility gives the sanitizer the capability to perform its tasks quickly and effectively. The results from the experiment confirm that the Raspberry Pi USB sanitizer is effective in identifying malicious files and protecting the user from potential threats. The device demonstrated its accuracy and versatility, ensuring the safety of USB files and giving the user peace of mind. As a result, this experiment has shown the success of the Raspberry Pi USB sanitizer and its potential as an important tool in security.

5 Conclusion and Recommendation

The research demonstrates that the Raspberry Pi is an effective tool for providing basic computer protection by scanning and detecting malicious patterns from USB drives. Its detection capabilities make it an invaluable tool in guarding against potential malicious threats and could prove invaluable to both individuals and businesses. Moreover, the research indicates that the Raspberry Pi could be used for a range of other cybersecurity purposes, such as malware and ransomware detection, which can be of great value in providing increased protection. The findings from this research imply that the Raspberry Pi is a viable option for basic computer protection and malware detection. Additionally, it is a relatively low-cost tool that can be utilized to protect computer systems and networks from potential threats. To increase the effectiveness of the Raspberry Pi, it is suggested that further research be conducted on how to further improve the detection capabilities and extend the security measures. Based on the findings from this research, it is recommended that a security protocol, such as one that specifies rules and policies, should be in place when connecting USB devices. Moreover, implementing automated measures, such as a script that can move malicious files to a trash folder, helps secure a computer's data. Generally, the research has demonstrated that the Raspberry Pi is an effective tool for providing basic computer protection and malware detection. Utilizing the recommendations mentioned above could further strengthen security measures and protect a computer's data from malicious intrusions.

References

[1] Caviglione, L., Wendzel, S., Mileva, A., & Vrhovec, S. (2021). Guest Editorial: Multidisciplinary Solutions to Modern Cybersecurity Challenges. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *12*(4), 1-3.

[2] Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I-Digital forensics framework for reviewing and investigating cyber-attacks. *Array*, *5*.

[3] Fathy, A., Atitallah, A.B., Yousri, D., Rezk, H., & Al-Dhaifallah, M. (2022). A new implementation of the MPPT based raspberry Pi embedded board for partially shaded photovoltaic system. *Energy Reports*, *8*, 5603-5619.

[4] Hinov, N., & Krastev, F. (2022). Identification, Vulnerability Research and Cybersecurity of Raspberry Pi Devices. *In IEEE 8th International Conference on Energy Efficiency and Agricultural Engineering (EE&AE)*, 1-6.

[5] Ho, S.M., & Burmester, M. (2021). Cyber Forensics on Internet of Things: Slicing and Dicing Raspberry Pi. *International Journal of Cyber Forensics and Advanced Threat Investigations*, *2*(1), 29-49.

[6] Karystinos, E., Andreatos, A., & Douligeris, C. (2019). Spyduino: Arduino as a HID exploiting the Bad USB vulnerability. *In IEEE 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 279-283.

[7] Mazhar, M.S., Saleem, Y., Almogren, A., Arshad, J., Jaffery, M.H., Rehman, A.U., & Hamam, H. (2022). Forensic analysis on internet of things (IoT) device using machine-to-machine (M2M) framework. *Electronics*, *11*(7), 1-23.

[8] Moniaga, J.V., Manalu, S.R., Hadipurnawan, D.A., & Sahidi, F. (2018). Diagnostics vehicle's condition using obd-ii and raspberry pi technology: study literature. *In Journal of Physics: Conference Series*, 978(1). IOP Publishing.

[9] Mueller, T., Zimmer, E., & de Nittis, L. (2019). Using context and provenance to defend against usb-borne attacks. *In Proceedings of the 14th International Conference on Availability, Reliability and Security*, 1-9.

[10] Peng, H., & Payer, M. (2020). {USBFuzz}: A Framework for Fuzzing {USB} Drivers by Device Emulation. *In 29th USENIX Security Symposium (USENIX Security 20)*, 2559-2575.

[11] Phadke, P., & Thorpe, C. (2021). Analysis of API Driven Application to Detect Smishing Attacks. In *European Conference on Cyber Warfare and Security*, 588. Academic Conferences International Limited.

[12] Rekha, G., & Maheswari, B.U. (2021). Raspberry Pi Forensic Investigation and Evidence Preservation using Blockchain. *In IEEE International Conference on Forensics, Analytics, Big Data, Security (FABS)*, *1*, 1-5.

[13] Rekha, G., & Sudha, T. (2022). A Study on Iot Forensic Investigation in the New Age of Intelligent Crimes. *Mathematical Statistician and Engineering Applications*, *71*(4), 3274-3281.

[14] Simadiputra, V., & Surantha, N. (2021). Rasefiberry: Secure and efficient Raspberry-Pi based gateway for smarthome IoT architecture. *Bulletin of Electrical Engineering and Informatics*, *10*(2), 1035-1045.

[15] Subedi, K.P., Budhathoki, D.R., & Dasgupta, D. (2018). Forensic analysis of ransomware families using static and dynamic analysis. *In IEEE Security and Privacy Workshops (SPW)*, 180-185.

[16] Tian, J., Scaife, N., Kumar, D., Bailey, M., Bates, A., & Butler, K. (2018). SoK:" Plug & Pray" today–understanding USB insecurity in versions 1 through C. *In IEEE Symposium on Security and Privacy (SP)*, 1032-1047.

[17] Tripathi, S., & Kumar, R. (2018). Raspberry pi as an intrusion detection system, a honeypot and a packet analyzer. *In IEEE International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*, 80-85.

[18] Vaidya, N.S., & Rughani, P.H. (2020). A forensic study of Tor usage on the Raspberry Pi platform using open-source tools. *Computer Fraud & Security*, *2020*(6), 13-19.

[19] Wang, Z., Xie, W., Wang, B., Tao, J., & Wang, E. (2021). A survey on recent advanced research of CPS security. *Applied Sciences*, *11*(9), 3751.

[20] Widiyasono, N., Putra, I. K. G. D., Giriantari, I. A. D., & Sudarma, M. (2019). IoT forensic: Optimizing Raspberry Pi for investigation on the smart home network. *In IOP Conference Series: Materials Science and Engineering*, *550*(1). IOP Publishing.

[21] Zainudin, Z. I. B., San, L. Y., & Abdulla, R. (2022). Smart hand sanitizer dispenser. *Journal of Applied Technology and Innovation (e-ISSN: 2600-7304)*, *6*(1), 10.

Author Biography

Bandr Fakiha

Associate Professor at Department of Medical Health Services, Dean of Faculty of Health Sciences, Umm Al-Qura University. Saudi Arabia. Interesting in cybercrime, cybersecurity and forensic computer applications.