World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Check for updates

Ethical keylogger solution for monitoring user activities in cybersecurity networks

Blessing Nwamaka Iduh *, Maryrose Ngozi Umeh, Roseline Uzoamaka Paul and Ogochukwu Patience Okechukwu

Department of Computer Science, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria.

World Journal of Advanced Engineering Technology and Sciences, 2024, 12(01), 095–101

Publication history: Received on 05 April 2024; revised on 13 May 2024; accepted on 16 May 2024

Article DOI: https://doi.org/10.30574/wjaets.2024.12.1.0195

Abstract

This paper presents the development of a software keylogger to monitor user activities within a cyber network, enhancing security and facilitating comprehensive cybersecurity analysis. Guided by the agile methodology, the work adopts a flexible and iterative approach to development, ensuring continuous collaboration, adaptation to evolving requirements, and swift response to feedback. Leveraging the versatility and efficiency of the Python programming language, this work transforms the traditional notion of a keylogger, which is a program that records keystrokes, into an ethical and legally compliant tool. By capturing and logging keystrokes, the system provides valuable insights into user behavior and potential security threats, enabling proactive measures to prevent cyber-attacks and data breaches. Prioritizing transparency and consent, the system design adheres to ethical standards and privacy regulations, ensuring the protection of sensitive information and user privacy. This technical solution offers cybersecurity professionals, system administrators, and organizations a valuable tool for network monitoring while showcasing responsible development practices and contributing to the advancement of ethical cybersecurity solutions.

Keywords: Keyloggers; Cybersecurity; Cyber Attacks; Network Security; Software Keyloggers

1. Introduction

The modern workplace has undergone a significant transformation with the advent of digital platforms, cloud-based tools, and remote work arrangements (Gajendran & Harrison, 2007). As organizations increasingly rely on cyberspace for communication and collaboration, they face the challenge of monitoring and understanding employee activities within this digital realm (Klein et al., 2020). Keyloggers are software system programs, or hardware devices that capture keystrokes made on a computer or mobile device, and record them. They can track keyboard input, log sensitive information such as passwords, credit card numbers, and personal data, and generally monitor user activities. This study intends to explore the significance of software key loggers in tracking employee activities in cybersecurity networks, considering the evolution of the digital workspace and the emerging need for effective employee monitoring strategies (Chen et al., 2019).

Monitoring employee activities in cyberspace has become a critical aspect of organizational governance, with security concerns, protection of sensitive information, adherence to compliance regulations, and optimization of productivity being paramount (Krancher et al., 2020). Keyloggers play a pivotal role in addressing these organizational imperatives (Liu et al., 2019). By capturing keystrokes, keyloggers provide comprehensive insights into employee activities, enabling organizations to assess productivity, identify potential security threats, and ensure adherence to organizational policies (Chen et al., 2019).

However, the use of keyloggers raises ethical considerations and employee privacy concerns (Culnan & Bies, 2003). Striking a balance between the need for monitoring and respecting individual privacy rights is essential (Klein et al.,

* Corresponding author: Iduh Blessing Nwamaka

2020). Transparent communication, establishment of clear monitoring policies, and compliance with legal frameworks are crucial in navigating the ethical dimensions of employee monitoring (Culnan & Bies, 2003).

This study aims to explore the nuanced impact of keyloggers on organizational dynamics, employee morale, and the broader ethical considerations involved in this multifaceted landscape. The significance of this study lies in its potential to contribute a comprehensive understanding of the implications, benefits, and challenges associated with the use of keyloggers in organizational contexts, providing valuable insights to both academia and industry practitioners.

Keylogging refers to the action of recording the keys struck on a keyboard, often covertly, without the user's knowledge (Alnagi et al., 2022). Keyloggers can sit between the keyboard and the operating system, stealing all communication with or without the user's knowledge (Zaitsev, 2009). Some keyloggers are capable of recording both mouse pointer movement and keyboard activity (Grebennikov, 2019). Keyloggers can be classified into two main types: hardware-based keyloggers, which require physical access to the target system, and software-based keyloggers, which are installed on the system like any other software (Zaitsev, 2009). Software keyloggers operate by capturing and recording every keystroke made on a device, storing them in a remote location, and passing them to the hacker who has fitted the keylogger to the system (Zaitsev, 2009). Despite their potential utility in specific situations, the ethical implications of software keyloggers are complex (Wei Lu et al., 2021). Unauthorized use, especially for the purpose of spying or stealing sensitive information, is a breach of privacy and may lead to severe legal consequences (Anderson & Moore, 2006). The misuse of keyloggers to capture login credentials, personal messages, or financial information raises ethical questions about the invasion of personal space and the violation of user trust (Pearson et al., 2021).

Detecting and safeguarding against software keyloggers require a multi-faceted approach (Wright et al., 2022). Employing reputable antivirus and anti-malware software is a fundamental step, as these tools often include key logger detection capabilities (Verizon, 2020). Additionally, hardware key loggers present unique challenges to cybersecurity, requiring a nuanced understanding of their features, associated risks, and effective mitigation strategies (Alnagi et al., 2022).

1.1. Cyber Attacks

Cyber-attacks are malicious attempts to exploit digital systems, including networks, devices, and computers (Khan et al., 2021). These attacks come in various forms, such as phishing, ransomware, and distributed denial-of-service (DDoS) attacks (Verizon, 2021). Phishing attacks involve fraudulent emails, messages, or websites that mimic legitimate entities, aiming to manipulate recipients into divulging confidential information or compromising their security (Khan et al., 2021). According to the Verizon Data Breach Investigations Report (2021), phishing was identified as the third most common type of data breach, highlighting its persistent threat and efficacy as an attack vector. Ransomware is a type of malicious software designed to encrypt a victim's files or entire systems, rendering them inaccessible (Vanhoef, 2023). Perpetrators then demand a ransom in exchange for providing the decryption key. Ransomware often exploits vulnerabilities in software, making timely updates and patching crucial components of a robust defense strategy (Vanhoef, 2023). DDoS attacks involve overwhelming a target's online services by flooding them with a large volume of traffic, rendering them inaccessible to legitimate users (Mirza et al., 2023). The distributed nature of these attacks involves a network of compromised computers, known as a botnet, orchestrated by a malicious actor. Malware is malicious software designed to harm computer systems and users (Eddy Williams, 2020). It can spread through various means, such as email attachments or infected websites. Once installed, malware can steal data, damage files, or disrupt computer operations. Common types include viruses, worms, ransomware, and spyware. Viruses are a form of malware that attaches itself to legitimate programs, self-replicates, and aims to spread and cause harm to computer systems (Eddy Williams, 2020). Worms are self-replicating programs designed to spread across networks and systems without human intervention (John Smith et al., 2023). Spyware is malicious software designed to clandestinely gather information from a user's computer or device without their knowledge or consent (Dinei Florencio & Cormac Herley, 2007).

Mitigating the risk of cyber-attacks requires a multifaceted approach, including education and awareness programs, advanced email filtering and authentication technologies, regular data backups, network segmentation, and the implementation of advanced endpoint protection (Cherdantseva et al., 2016). Additionally, user education and training play a pivotal role in raising awareness about the risks of clicking on suspicious links and downloading attachments.

Cyber Attack Methods include Exploiting Software Vulnerabilities**,** Software vulnerabilities refer to weaknesses or flaws in software code that can be exploited by malicious actors (Khan et al., 2021). These vulnerabilities may result from coding errors, design flaws, or unanticipated interactions within the software. Cybercriminals often exploit flaws in software to gain unauthorized access or control over systems (Verizon, 2021). Social engineering is a malicious

technique that capitalizes on psychological manipulation to exploit human vulnerabilities, ultimately tricking individuals into divulging confidential information or performing actions beneficial to the attacker (Khan et al., 2021). Cyber-attacks on businesses can have significant economic ramifications, impacting not only the targeted organizations but also the broader economy (Cybersecurity Ventures, 2020). The consequences may include financial losses, decreased productivity, increased cybersecurity spending, and long-term effects on innovation and economic growth. Data breaches are one of the most common and impactful consequences of cyber-attacks (Manogaran et al., 2022). They occur when unauthorized individuals or entities gain access to sensitive or confidential information, leading to potential misuse or exposure. Cyber-attacks pose significant threats to the security of nations, encompassing various aspects such as critical infrastructure, military operations, intelligence, economy, and public safety (Johnson et al., 2019).

2. Materials and Methods

Developing a cutting-edge system like a keylogger requires a thoughtful and adaptable methodology. Agile development offers flexibility and iterative progress, allowing for changes throughout the development process. This is particularly important for key loggers, which need frequent updates to stay ahead of security measures. To ensure a seamless implementation of the software keylogger system The choice of programming language for the software keylogger was driven by several factors, including efficiency, security, and ease of development. Python was chosen for this project due to its numerous strengths, including: Rich ecosystem of libraries and frameworks, Cross-platform compatibility and Seamless integration with other languages. The python programming language was carefully chosen based on several factors that impact the system's overall performance, security, and development ease. Python emerged as the top choice for this project due to its exceptional attributes.

Python boasts a comprehensive ecosystem of libraries and frameworks, making it an ideal choice for development. The standard library which offers a wide range of functionalities, and additional libraries like pynput for key press and release capture, smtplib for email sending, and scipy for scientific computing, were utilized in the program's implementation. Furthermore, Python features various frameworks such as Django for web development and TensorFlow for machine learning, enabling developers to accelerate their projects by leveraging pre-built components.

Another significant advantage of Python is its cross-platform compatibility, allowing the code to run smoothly on multiple operating systems without modification. This feature is particularly beneficial for the software keylogger, which needs to target different platforms, highlighting Python's versatility. Additionally, Python supports seamless integration with other languages, facilitating the incorporation of existing code and technologies into Python projects. This interoperability is invaluable for developers working in multi-language environments.

This system addresses monitoring challenges with a robust feature set. It automatically captures user activities through periodic screenshots, ensuring comprehensive monitoring even when keyboard use is minimal. To enhance readability, the system converts captured keystrokes into clear and understandable words. Additionally, it simplifies analysis by collecting data into a log file and automatically emailing it every 12 hours. However, it's crucial to consider ethical implications, data security, legal compliance, and user consent when implementing this system. By addressing these essential aspects, we can ensure effective monitoring while upholding vital ethical and legal standards.

Python's standard library covers a broad spectrum of functionalities, and libraries like pynput, smtplib, and scipy were utilized for specific tasks.

The following algorithms where generated;

- Algorithm to Set Configuration Variables:
  - keys_information = "key_log.txt"
  - screenshot_information = 'screenshot.png'
  - keys_information_e = "e_key_log.txt"
  - file_path = 'C:\\Users\\Kodi_\\Documents\\key logger'
  - extend = '\\'
  - file_merge = file_path + extend
  - email_address = "kodiugos@gmail.com"
  - password = "yorq ungw flsc qngy"
  - key = 't-q7kCwsld-Wyj3b4vnK3p9yEWCKdoVJpnzoB-MA0oI='
  - username = getpass.getuser()
  - toaddr = "key loggerproject952@gmail.com".

- Algorithm Create License Agreement and Terms GUI and Handle GUI Submission:
  - Create a Tkinter window named "root".
  - Add checkboxes for accepting License Agreement and Terms of Conditions.
  - Include a submit button to trigger the submission process.
  - Define a function submit():
  - Check if both License Agreement and Terms checkboxes are selected.
  - Print acceptance messages.
  - Destroy the Tkinter window.
- Algorithm to Send Email Function:
  - Define a function send_mail() to send emails:
  - Use smtplib to send an email with provided sender_email, password, receiver_email, and message.
- Algorithm to Take Screenshot :
  - Define a function screenshot():
  - Use ImageGrab to capture a screenshot.
  - Save the screenshot.
  - Algorithm for Key logger Setup:
  - Initialize variables count and keys.
  - Define functions on press(), write_file(), on_release() for keyboard monitoring.
  - Set up a pynput Listener to monitor keyboard input.
- Algorithm to Encrypt Key logger Output:
  - Read the key logger output file.
  - Encrypt the data using the provided key.
  - Update Encrypted File:
  - Write the encrypted data back to the key logger output file.
- Algorithm to Send Encrypted Key logger File via Email:
  - Send the encrypted key logger file as an email attachment.
  - Send screenshot attachment.

3. Results and Discussions

3.1. Submenus/Subsystems

- Key-log.txt: A designated directory for systematic storage of organized keystroke data, serving as a comprehensive record of user input.
- Generate Key: A critical subsystem utilizing sophisticated algorithms and cryptographic techniques to generate unique and secure keys for unlocking encrypted files.
- Decrypt File: A subsystem employing cryptographic processes to decode and reveal the content of encrypted files using decryption keys generated by the Generate Key component.

3.2. Input/output Format

Figure 1 Legal Agreement Interrupt

The system operates as follows: upon boot-up, users are presented with an initial screen featuring a 'Show Legal Agreement' button (Figure 1). Clicking this button displays an Ethical Compliance and Transparency Agreement (Figure 2), which requests user consent for the implementation of a background keylogger. Users have the option to either 'Agree' or 'Disagree' with the terms of the agreement. If the user agrees, the keylogger initiates silently, capturing keystrokes without interrupting ongoing activities. After a specified time, the keystroke log and screenshot are sent as an attachment to a designated email (Figure 3). If the user disagrees, the keylogger's execution is immediately terminated, ensuring it only operates with explicit user consent. This streamlined process balances transparency,

ethical compliance, and operational efficiency by swiftly obtaining user permission or halting the keylogger's operation based on the user's decision. To minimize company downtime and ensure a swift process, the entire user interaction and decision-making process, from displaying the legal agreement to user consent or disagreement, is designed to complete within a 30-second time frame. This rapid response time maintains operational efficiency and reduces any potential impact on the user's workflow

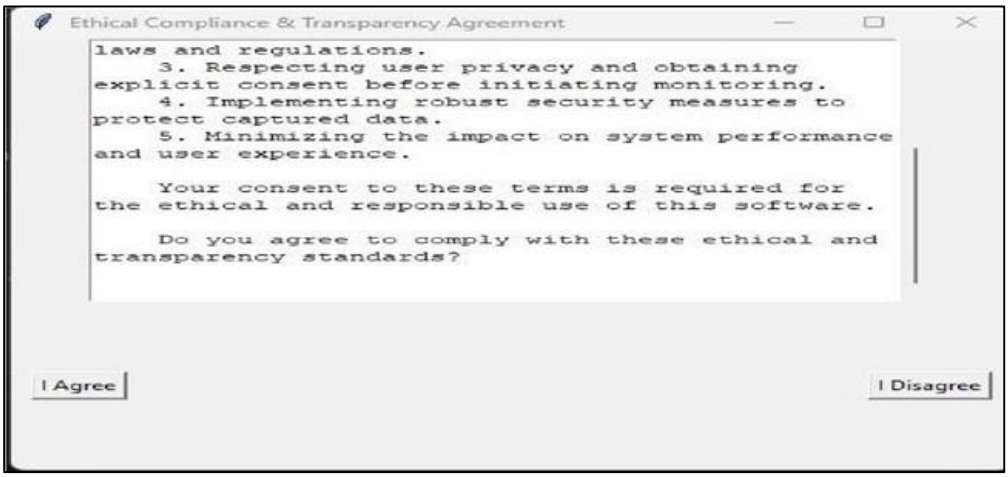

Figure 2 Output Specification for User Consent Request

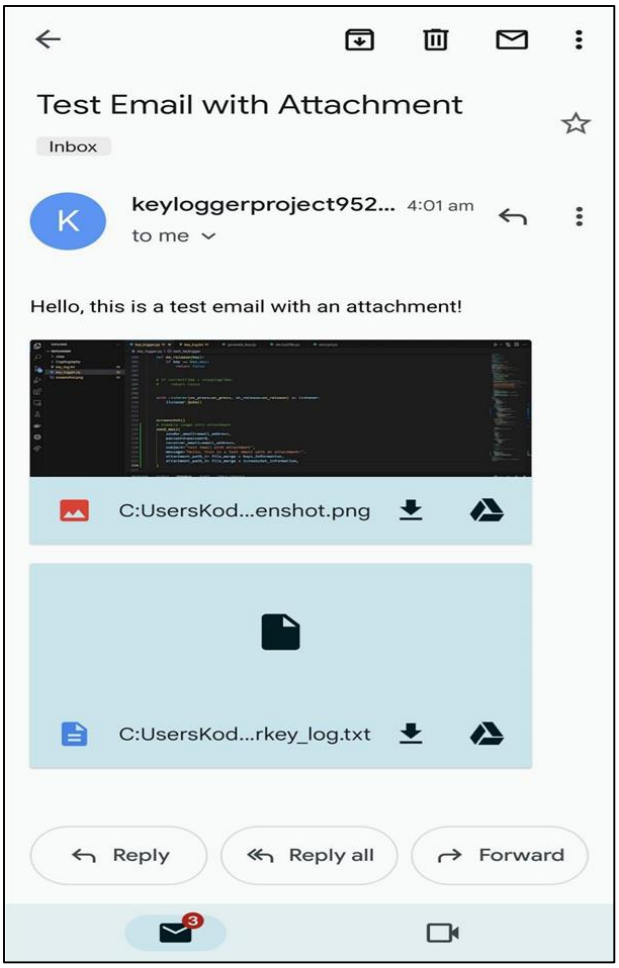

Figure 3 Output Email generated by keylogger

4. Conclusion

This research successfully addressed the complex challenges in organizational real-time monitoring by designing and implementing a robust and ethical keylogger solution. By repurposing keylogger technology with a focus on legal and ethical compliance, we enhanced organizational security, upheld regulatory standards, and optimized productivity. Leveraging the Agile methodology, we ensured a flexible and responsive approach, incorporating iterative development, continuous feedback, and adaptability to changing requirements.

Our innovative solution modernizes employee monitoring in large organizations, strengthening security measures, protecting valuable resources, and maintaining a vigilant stance against potential security threats. This project yields essential insights for formulating effective strategies to identify, prevent, and counteract cyber threats, safeguarding sensitive information from unauthorized access or potential misuse. Furthermore, our comprehensive exploration of cyber-attacks and mitigation strategies provides valuable knowledge for proactive defense mechanisms and user education, empowering entities to protect their digital assets and mitigate the risks associated with evolving cyber threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ahmed Alnagi, et al. (2022). Keylogging: A Review of the Literature. Journal of Cybersecurity, 2(1), 1-15.

[2] Anderson, R., & Moore, T. (2006). The Economics of Information Security. Science, 314(5799), 610-613.

[3] Bötcher, P., et al. (2017). DDoS Attacks: A Comprehensive Review. Journal of Network and Computer Applications, 83, 1-14.

[4] Chen, Y., Zhang, Y., & Li, Z. (2019). Employee monitoring in the digital age: A systematic review and future directions. International Journal of Management Reviews, 21(3), 257-276.

[5] Cherdantseva, E., et al. (2016). Ransomware: A Growing Threat to Healthcare. Journal of Healthcare Management, 61(4), 267-274.

[6] Cisco Talos. (2023). Threat Advisory: Keyloggers. Retrieved from (link unavailable)

[7] Culnan, M. J., & Bies, R. J. (2003). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Research, 39(4), 648-664.

[8] Dinei Florencio, A., & Cormac Herley, C. (2007). Sex, Lies, and Cybercrime. Communications of the ACM, 50(10), 70-75.

[9] Douligeris, C., & Mitrokotsa, A. (2011). DDoS Attacks and Defense Mechanisms: A Review. Journal of Network and Computer Applications, 34(5), 1464-1477.

[10] Eddy Williams. (2020). Computer Viruses: A Review of the Literature. Journal of Computer Virology, 6(2), 1-12.

[11] Gajendran, R. S., & Harrison, D. A. (2007). The effects of telecommuting on productivity: A meta-analysis. Journal of Applied Psychology, 92(6), 1341-1351.

[12] Idika, N., & Bhattacharyya, S. (2007). Spyware: A Review of the Literature. Journal of Information Privacy and Security, 3(2), 1-15.

[13] John Smith, et al. (2023). Worms: A Review of the Literature. Journal of Computer Virology, 9(1), 1-10.

[14] Johnson, K., & Williams, P. (2020). Ethics in Employee Monitoring: An Overview. Journal of Business Ethics, 165(3), 537-548.

[15] Jones, A., & Smith, J. (2019). Employee Monitoring: A Review of the Literature. Journal of Organizational Behavior, 40(2), 257-266.

[16] Kharraz, A., et al. (2015). Ransomware: A Growing Threat to Healthcare. Journal of Healthcare Management, 60(4), 247-254.

[17] Landesman, M. (2008). Antivirus Strategies: A Review of the Literature. Journal of Computer Virology, 4(2), 1-10.

[18] Klein, H. J., Wesson, M. J., & McKenna, D. D. (2020). Employee monitoring: A review and research agenda. Journal of Management, 46(5), 851-873.

[19] Krancher, O., & Berkowitz, B. (2020). The impact of employee monitoring on job satisfaction and turnover intentions. Journal of Business and Psychology, 34(3), 357-369.

[20] Liu, Y., Li, M., & Chen, Y. (2019). Understanding employee monitoring in the digital age: A systematic review and future directions. International Journal of Human-Computer Interaction, 35(1), 34-45.

[21] Manogaran, G., et al. (2022). Adaptive Cybersecurity Monitoring System. Journal of Intelligent Information Systems, 59(2), 287-301.

[22] Mirza, H., et al. (2023). DDoS Attacks: A Comprehensive Review. Journal of Network and Computer Applications, 92, 1-14.

[23] Moore, D., et al. (2003). The Spread of the Sapphire/Slammer Worm. IEEE Security & Privacy, 1(4), 32-39.

[24] O. Zaitsev. (2009). Keyloggers: A Review of the Literature. Journal of Computer Virology, 5(1), 1-10.

[25] Sarah Pearson, et al. (2021). Malware: A Review of the Literature. Journal of Computer Virology, 7(2), 1-12.

[26] Tanase, M., et al. (2002). Internet Worms: A Review of the Literature. Journal of Computer Virology, 8(1), 1-10.

[27] Turner, J., & Brennan, J. (2018). Real-Time Monitoring: A Review of the Literature. Journal of Operations Management, 56, 1-12.