Improving the Cybersecurity of Online Banking by the Integration of Artificial Intelligence-Powered Preventive Measures Against Keylogger Malware

Jasmine Chong Qi En
tp064426@mail.apu.edu.my

Abstract *– This research looks at how keyloggers malware will affect banks, especially online banking, by stealing confidential information from each client using the bank through recorded keystrokes (Shukla et al., 2023). It will cause financial losses and customers will lose trust in the bank itself. Human mistakes and social engineering tactics (Karadsheh et al., 2021) will often increase the chances of having keyloggers malware. The aim of this research is to see how often keyloggers attacks happen in banks and how it affects customers' trust towards online banking services. By implementing artificial intelligence powered preventive measures which it is a combination of artificial intelligence and machine learning technologies (Raparthi et al., 2020), the measurements can notice and respond to unusual behaviors caused by the keylogger malware and can develop more effective defense mechanisms to reduce the impact of attacks. Thus, online banking will have safer and smarter security systems, customers will have more confidence when using online banking services.*

Index Terms
keyloggers malware, online banking, artificial intelligence (AI), malware attacks, keyloggers attack

1. Introduction

Online banking is a service offered by a lot of banks nowadays, although it is convenient to most people in this digital era, it also exposes security issues like keylogger malware and other types of malwares, but the most popular malware that exists in online banking is keylogger malware. This malware records keystrokes to steal sensitive information which leads to several issues. Keyloggers malware is usually caused by weak passwords, security policies or even social engineering. By integrating artificial intelligence (AI), it can improve the overall security of online banking. There are different types of artificial intelligence powered preventive measures like Support Vector Machine (SVM) (Bansal et al., 2022), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long-Short Memory Network (LSTM) (Maz et al., 2024), Combinatorial-Based Fuzzy Inference System for Keylogger Detection (CaFISKLD) (Ayo et al., 2023) and etc., the benefits of implementing them can investigate and recognize attack patterns or data to develop detection strategies that are artificial intelligence based.

2. Problem Statement

The study shows that keylogger malware is considered one of the threats to the banking industry by recording keystrokes and capturing sensitive information of each client, leading to significant data breaches. These breaches undermine financial stability through revenue loss, increased operational costs, and potential legal liabilities while also affecting customer trust. The root causes of keylogger malware exploitation include human error and social engineering, such as phishing attacks that trick employees or customers into downloading malicious software (Marks, 2024), and a general lack of cybersecurity awareness. Other than that, weak security practices, such as weak password policies (H. Almulihi et al., 2022) and insufficiently secured systems, create vulnerabilities that keylogger malware can exploit, highlighting the need for security measures and comprehensive training programs within the banking sector. The potential for using machine learning algorithms like Linear Regression (Perwitasari, 2022), Logistic Regression (Gonaygunta, 2023) etc. to prevent keyloggers malware for banking industry, they can analyze software behavior and user interactions in real time which identify anomalies that has the presence of keyloggers by detecting unusual data access patterns or unauthorized transmissions or machine access (Singh et al., 2021). The usage of it is to enhance threat detection and response.

3. Research Aim

To see a reduction in the incidence of keylogger malware attacks in the banking sector and to minimize their impact on financial institutions and customers through improved security measures and protocols. These implementation and advancements will further strengthen digital defenses, which ensure a secure transaction environment and receive more trust from customers.

4. Research Objectives

I. To investigate the frequency and patterns of keylogger malware attacks in the banking industry and their effects on operational efficiency, financial performance, and customer trust. .

II. To develop and propose strategies for reducing the impact of keylogger malware which incorporates AI to enhance real-time detection and response capabilities.

III. To evaluate the impact of keylogger malware incidents on customer trust in online banking and investigate how keyloggers affect customer willingness to engage with online banking.

5. Research Questions

I. What are the most common types of keylogger malware attacks in the banking industry?
II. How does keylogger malware impact the financial efficiency of the bank?
III. How can AI be enhanced to detect keylogger malware attacks in real-time and what are the key features of an effective AI-powered preventive measures?
IV. How do keylogger malware incidents affect customer trust in online banking platforms and what are the factors that cause this?

6. Research Significance

The increase usage of online banking has brought a lot of convenience to users; however, it also has its own vulnerability. One of the vulnerabilities is that keylogger malware can steal user credential input when they key in their username and password (Jung et al., 2024). When attackers have information access to each stolen credential, it’s dangerous to them as users might lose their money and for the bank, they may lose the trust of their customers.

This research is significant as it explores how AI can be implemented in online banking systems and how it helps to reduce financial loss for the bank and increase user confidence. To obtain a safe and secure environment for the users, implementing specific and accurate AI algorithms is important as AI is considered a new technology. There are different kinds of AI algorithms that can be used to reduce the risk of keylogger malware like SVM, CaFISKLD and other algorithms can be used to reduce the happening of keyloggers.

7. Overview of the Proposed System/Research

At target identification stage, the system will use tool like Keras (Dewis & Viana, 2022) to implement AI algorithms which it is a Python library that is suitable to monitor the system and identify targets that might be infected with keylogger malware that is injected by attackers, algorithms that can be used to analyze and user behavior are CNN, SVM and CaFISKLD. They can identify and analyse high-risk targets and present the results in image type and proceed to the next stage after completing identifying. (Kosarac et al., 2022) At the decision point stage, the AI algorithms that can be used for anomaly detection can be Isolation Forest algorithm (Chabchoub et al., 2022), it can identify target that has potential risk and whether there is a need for enhanced monitoring. If a target is identified as keylogger malware, the process will proceed to the next stage which is data capturing. If no, it will return to the target identification step and continue to monitor whether there is infected targets in the system. In the data capturing stage, the system will deploy behavioral analytics powered by AI (Farayola, 2024) to identify suspicious processes or unauthorized access to keyboard APIs or other input methods. In the data storage stage, AI algortihms will analyze data storage behaviour to detect and mark any weird or uncommon activies like unauthorized file creation by users that does not have access. During date exfiltration stage, AI algorithms like Random Forest and Gradient Boostign will analyze the system network traffic in real-time to identify and block unusual data transmission patterns which includes identifying encrypted transmissions to unknown destinations. (Afuwape et al., 2021) At data analysis stage, using text-matching algorithms (Cao et al., 2021) are able to automatically analyze security logs and data to search for specific patterns or string within log data and are able to extract information like IP addresses and etc. If the algorithms detect a data breach, they will generate alerts and initiate incident response procedures, else it will then continue with montoring. After detecting data breaches, security information and event management (SIEM) that is AI driven will then generate and prioritize alerts based on the their severity (MACANEATA, 2024). In the final stage, action on objectives, the security team will take action based on the AI generated alerts to stop the breach and prevent further damage.

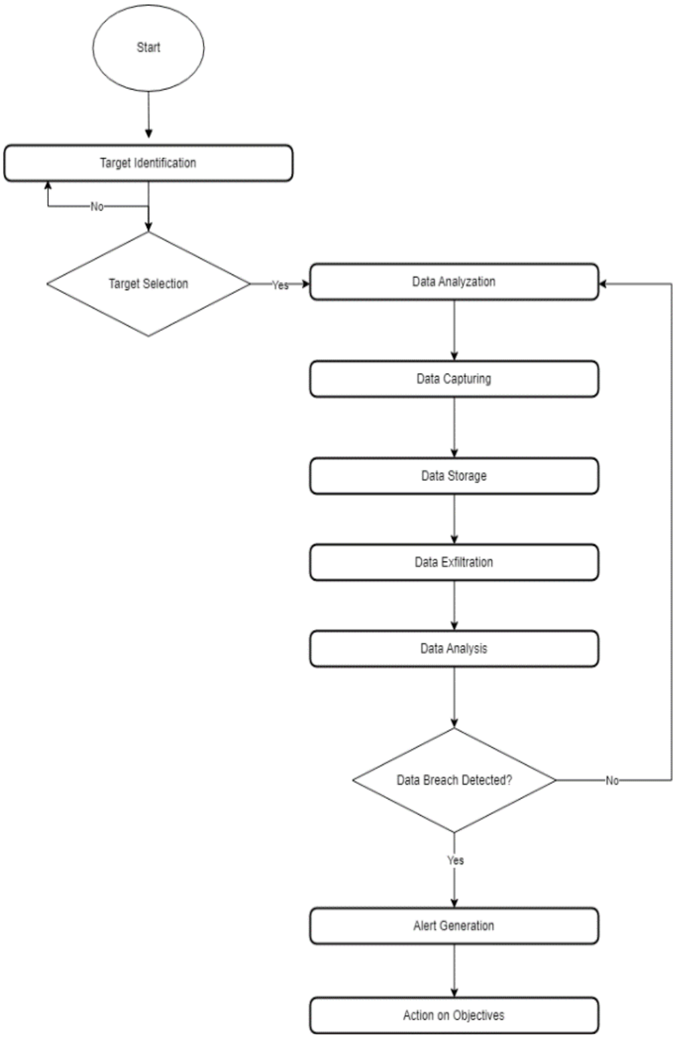

Figure 1: Implement Artificial Intelligence-Powered Preventive Measures Against Keylogger Malware

References

Marks, T. (2024, February 2). What are keyloggers and how can you protect yourself from them? *VPN Overview*. Retrieved from https://vpnoverview.com/internet-safety/malware/keyloggers/

H. Almulihi, A., Alassery, F., Irshad Khan, A., Shukla, S., Kumar Gupta, B., & Kumar, R. (2022). Analyzing the implications of healthcare data breaches through Computational Technique. *Intelligent Automation &amp; Soft Computing*, *32*(3), 1763–1779. https://doi.org/10.32604/iasc.2022.023460

Perwitasari, A. W. (2022). The effect of perceived usefulness and perceived easiness towards behavioral intention to use fintech by Indonesian msmes. *The Winners*, *23*(1), 1–9. https://doi.org/10.21512/tw.v23i1.7078

Shukla, V., Shukla, Y., & Patel, A. (2023). Examining the ethical implications and technical capabilities of key-logger software. 2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). https://doi.org/10.1109/icimia60377.2023.10425833

Gonaygunta, H. (2023). Machine learning algorithms for detection of cyber threats using logistic regression. *International Journal of Smart Sensor and Adhoc Network.*, 36–42. https://doi.org/10.47893/ijssan.2023.1229

Singh, A., Choudhary, P., singh, A. kumar, & tyagi, D. kumar. (2021). Keylogger detection and prevention. *Journal of Physics: Conference Series*, *2007*(1), 012005. https://doi.org/10.1088/1742-6596/2007/1/012005

Bansal, M., Goyal, A., & Choudhary, A. (2022). A comparative analysis of k-nearest neighbour, genetic, support vector machine, decision tree, and long short-term memory algorithms in machine learning. *Decision Analytics Journal*, *3*, 100071. https://doi.org/10.1016/j.dajour.2022.100071

Maz, Y. A., Anbar, M., Manickam, S., Rihan, S. D., Alabsi, B. A., & Dorgham, O. M. (2024). Majority voting ensemble classifier for detecting keylogging attack on internet of things. IEEE Access, 12, 19860–19871. https://doi.org/10.1109/access.2024.3362232

Karadsheh, L., Alryalat, H., Alqatawna, J., Alhawari, S. F., & Jarrah, M. A. (2021). The impact of social engineer attack phases on improved security countermeasures. International Journal of Digital Crime and Forensics, 14(1), 1–26. https://doi.org/10.4018/ijdcf.286762

Ayo, F. E., Awotunde, J. B., Olalekan, O. A., Imoize, A. L., Li, C.-T., & Lee, C.-C. (2023). CBFISKD: A combinatorial-based fuzzy inference system for keylogger detection. Mathematics, 11(8), 1899. https://doi.org/10.3390/math11081899

Raparthi, M., Dodda, S. B., & Maruthi, S. (2020). Examining the use of artificial intelligence to enhance security measures in computer hardware, including the detection of hardware-based vulnerabilities and attacks. *European Economic Letters*. https://doi.org/10.52783/eel.v10i1.991

Jung, W., Hong, S., & Lee, K. (2024). Mouse Data Attack Technique using machine learning in image-based user authentication: Based on a defense technique using the WM_INPUT message. *Electronics*, *13*(4), 710. https://doi.org/10.3390/electronics13040710

Dewis, M., & Viana, T. (2022). Phish responder: A hybrid machine learning approach to detect phishing and spam emails. *Applied System Innovation*, *5*(4), 73. https://doi.org/10.3390/asi5040073

Kosarac, A., Cep, R., Trochta, M., Knezev, M., Zivkovic, A., Mladjenovic, C., & Antic, A. (2022). Thermal behavior modeling based on BP neural network in Keras framework for motorized machine tool spindles. *Materials*, *15*(21), 7782. https://doi.org/10.3390/ma15217782

Chabchoub, Y., Togbe, M. U., Boly, A., & Chiky, R. (2022). An in-depth study and improvement of Isolation Forest. *IEEE Access*, *10*, 10219–10237. https://doi.org/10.1109/access.2022.3144425

Farayola, O. A. (2024). Revolutionizing banking security: Integrating Artificial Intelligence, Blockchain, and business intelligence for Enhanced Cybersecurity. *Finance &amp; Accounting Research Journal*, *6*(4), 501–514. https://doi.org/10.51594/farj.v6i4.990

Afuwape, A. A., Xu, Y., Anajemba, J. H., & Srivastava, G. (2021). Performance evaluation of secured network traffic classification using a machine learning approach. *Computer Standards &amp; Interfaces, 78,* 103545. https://doi.org/10.1016/j.csi.2021.103545

Cao, K., Chen, C., Baltes, S., Treude, C., & Chen, X. (2021). Automated query reformulation for efficient search based on query logs from stack overflow. *2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE)*. https://doi.org/10.1109/icse43902.2021.00116

MACANEATA, C. (2024). Overview of security information and event management systems. *Informatica Economica*, *28*(1/2024), 15–24. https://doi.org/10.24818/issn14531305/28.1.2024.02