based Predictive Model for Keylogging Attack Mitigation

Mariam Ayobami GBADEGESIN
LCU/PG/002431

Being a MSc Thesis Submitted to the Department of Computer Science, Faculty of Natural and Applied Sciences, Lead City University, Ibadan, Oyo State, Nigeria

In Partial Fulfilment of the Requirements for the Award of Master of Science Degree (MSc) in Computer Science

2023

Certification

This is to certify that Mariam Ayobami GBADEGESIN with matriculation number LCU/PG/002431 carried out this research work titled "Neuro-fuzzy Based Predictive Model for Keylogging Attack Mitigation" in the Department of Computer Science, Faculty of Natural and Applied Sciences, Lead City University, Ibadan, Oyo state, for the award of Master Degree (MSc) in Computer Science and that this has not been previously submitted.

Prof S. O Akinola
(Supervisor)

Date

Dr Wilson Sakpere
(Head of Department)

Date

Dedication

This research work is dedicated to Almighty God for his mercies and grace in abundance upon my life and to my family members.

Acknowledgements

I would like to express my deepest gratitude to my thesis supervisor Prof Akinola for his untiring guidance and motivation in making this research work a huge success. I wish to specially thank him for being very patient and helpful to me throughout the development process of the system.

My special thanks go to My Head of Department, Dr Wilson Sakpere for his sincere critique and provision of directions on how best to approach this thesis work.

My sincere thanks go members of staff of computer science department, Lead City University Ibadan whose individual contributions influenced my final submissions in this research work.

I want to register my special thanks and gratitude to my best friend and husband, Mr Akeem Lawal for his unending prayers, support and understanding during the course of this thesis work. To my children and My Parents and my sibblings, thank you so much for your support and prayers.

Finally, my thanks go to my friends who have given me full support, without which I would not have completed this thesis work.

Abstract

In the ever-evolving landscape of cybersecurity, the relentless progression of cyber threats presents an ongoing challenge to the integrity of sensitive data and user credentials. Among these threats, keylogging malware has emerged as a particularly insidious vector, adept at covertly infiltrating systems, stealing login credentials, and exfiltrating valuable information. This research is driven by the imperative need to confront this menacing adversary. By delving into the subtle intricacies of human keystroke dynamics, we have engineered a groundbreaking and intelligent predictive model aimed at the early and reliable detection of keylogging attacks. The innovative character of this model stems from its amalgamation of two powerful techniques: adaptive neural networks and fuzzy logic inference. This research develops a Neuro-fuzzy predictive model using keystroke dynamics to reliably detect and mitigate ongoing keylogging threats. The model's training process was conducted using a diverse dataset comprising over three hundred thousand keystroke samples, sourced from both simulated users and actual keyloggers. Impressively, baseline neural networks exhibited a detection accuracy rate of 99.1%. Building upon this solid foundation, the specialized Neuro-fuzzy model further elevated precision, achieving a remarkable 99.62% accuracy. This enhancement primarily stemmed from the model's ability to distinguish between human and automated keystroke patterns, significantly reducing false positives. These results demonstrate that an adaptive Neuro-fuzzy model can reliably predict keylogging attacks in real-time based on anomalous keystroke dynamics before significant credentials or data are exfiltrated. The adaptive model provides a robust predictive solution to a rapidly evolving risk that continues to bypass traditional reactive defenses.

Keywords: Neuro-fuzzy, Neuro-fuzzy model, keylogging, keylogging threats
Total word count: 250 words

Table of Contents

List of Figures