

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

Do Not Copy, Lead City University, Nigeria

Dedication

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

Do Not Copy, Lead City University, Nigeria

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 siblings, 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.

Do Not Copy Lead City University, Nigeria

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

Certification	2
Dedication	3
Acknowledgements	4
Abstract	5
CHAPTER ONE	Error! Bookmark not defined.
Introduction	Error! Bookmark not defined.
1.1 Background of The Study	Error! Bookmark not defined.
1.2. Statement of the Problem	Error! Bookmark not defined.
1.3 Aim and Objectives of the Study	Error! Bookmark not defined.
1.4 Scope and Limitations	Error! Bookmark not defined.
1.5 Organization of the Thesis	Error! Bookmark not defined.
1.6 Definition of Terms	Error! Bookmark not defined.
Chapter Two	Error! Bookmark not defined.
Literature Review	Error! Bookmark not defined.
2.1. Conceptual Review	Error! Bookmark not defined.
2.2. Machine Learning and Cybersecurity	Error! Bookmark not defined.
2.3. Neuro Fuzzy Systems	Error! Bookmark not defined.
2.4. Predictive Modelling in Cybersecurity	Error! Bookmark not defined.
2.5. Feature Engineering for Keylogging Detection	Error! Bookmark not defined.
2.6. Datasets and Evaluation Metrics	Error! Bookmark not defined.
2.7. Neuro Fuzzy Hybrid Models in Security	Error! Bookmark not defined.
2.8. Real-time Detection and Response	Error! Bookmark not defined.
2.9. Human-Centric Security Approaches in Cybersecurity	Error! Bookmark not defined.
2.10 Comparative Analysis of Neuro-fuzzy models with Other Techniques	Error! Bookmark not defined.
2.11. Adversarial Attacks and Robustness of Neuro-fuzzy Systems	Error! Bookmark not defined.
2.12 Related Works	Error! Bookmark not defined.
CHAPTER THREE	Error! Bookmark not defined.
Methodology	Error! Bookmark not defined.
3.1 Methodology	Error! Bookmark not defined.

3.2	The System Model	Error! Bookmark not defined.
3.2.1	Detailed Analysis of the Model	Error! Bookmark not defined.
3.3	The Detailed Model	Error! Bookmark not defined.
3.3.1	Data Collection	Error! Bookmark not defined.
3.3.2	Data Preprocessing	Error! Bookmark not defined.
3.3.3	Fuzzy Logic Component	Error! Bookmark not defined.
3.3.4	Neuro-Network Component	Error! Bookmark not defined.
3.3.5	Training and Validation	Error! Bookmark not defined.
3.3.6	Mitigation Strategy	Error! Bookmark not defined.
3.3.7	Evaluation	Error! Bookmark not defined.
3.4	Metrics for Performance Evaluation of the Model	Error! Bookmark not defined.
3.4.1	Accuracy	Error! Bookmark not defined.
3.4.2	Precision	Error! Bookmark not defined.
3.5	Implementation requirements	Error! Bookmark not defined.
3.6	R-Studio	Error! Bookmark not defined.
3.7	Justification for Choice of Programming Language	Error! Bookmark not defined.
Chapter Four		Error! Bookmark not defined.
Design And Implementation		Error! Bookmark not defined.
4.1	Design	Error! Bookmark not defined.
4.2	Research design	Error! Bookmark not defined.
4.2.1	Use-Case	Error! Bookmark not defined.
4.2.2	Activity diagram	Error! Bookmark not defined.
4.2.3	Sequence diagram	Error! Bookmark not defined.
4.3	Implementation phase of the model	Error! Bookmark not defined.
4.3.1	Defining the input variable (crisp values)	Error! Bookmark not defined.
4.3.2	Defining the output variable	Error! Bookmark not defined.
4.3.3	Inputting of data interface	Error! Bookmark not defined.
4.3.4	Outputting of data interface	Error! Bookmark not defined.
4.4	Result discussion.	Error! Bookmark not defined.
4.5	Predicted whether is keylogger or Benign output	Error! Bookmark not defined.
4.6	Implications of Mean Squared Error (MSE)	Error! Bookmark not defined.
4.7	Comparing the Result with ANN	Error! Bookmark not defined.
CHAPTER FIVE		Error! Bookmark not defined.

Conclusion

5.1 Summary

5.2 Conclusion

5.3 Recommendations

5.4 Contribution to Knowledge

5.5 Future Work

Bibliography

List of Appendices

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Error! Bookmark not defined.

Do Not Copy, Lead City University, Nigeria

List of Figures

Figure 1: Neuro-fuzzy hybrid system	Error! Bookmark not defined.
Figure 2.1 Neuro-fuzzy system	Error! Bookmark not defined.
Figure 3.1 System model	Error! Bookmark not defined.
Figure 3.2: Snippet of the raw data	45
Figure 3.6 R-studio screen	52
Figure 4.1 HYFIS model system	
Error! Bookmark not defined.	
Figure 4.2 Use-case diagram of the proposed system	57
Figure 4.3 Activity diagram of the proposed system	58
Figure 4.4 Sequence diagram of the proposed system	59
Figure 4.5 Importing of the data from the file storage	64
Figure 4.6 Checking and removing of missing values	65
Figure 4.7 Removing of column that are not a factor in the prediction	65
Figure 4.8 Removal of the output	66
Figure 4.9 Splitting of the data into training and testing sets	66
Figure 4.10 Display of input of the testing data	67
Figure 4.11 Display of output of the testing data	67
Figure 4.12 The HYFIS Model and the parameter needed for the prediction	68
Figure 4.13 The prediction of the class of attack given only the input	68
Figure 4.14 The conversion of decimal to whole numbers	69
Figure 4.16 The calculation of MSE the closer to zero the more the accuracy	Error! Bookmark not defined.
Figure 4.17 The comparison of the original and predicted data set	Error! Bookmark not defined.
Figure 4.18 The characteristics of a fuzzy rule-based system(FRBS) model	Error! Bookmark not defined.
Figure 4.19 The MSE and the original and predicted output	Error! Bookmark not defined.