A Secure Framework for Detecting “Fake News in Social Media Networks”

K.S.P. Nonis
(Reg. No.: MS21910418)

A THESIS
SUBMITTED TO
SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
(CYBER SECURUTY)

November 2024

I certify that I have read this thesis (draft) and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Anuradha Jayakody

Approved for MSc. Research Project:

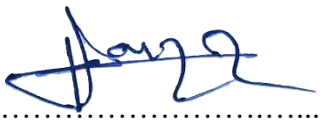
MSc. Programme Co-ordinator, SLIIT

Approved for MSc:

Head of Graduate Studies, FoC, SLIIT

DECLARATION

This is to certify that the work is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources). The work has not previously been submitted in any form to the Sri Lanka Institute of Information Technology or to any other institution for assessment for any other purpose.

Sign:  .....

K.S.P. Nonis

Date: ……11th November 2024…

ABSTRACT

A Secure Framework for Detecting “Fake News in Social Media Networks”

Sanjeeva Nonis
MSc. in Information Technology (Cyber Security)
Supervisor: Prof Anuradha Jayakody
November 2024

In today's digital era, the proliferation of fake news poses significant challenges to societal trust, political stability, and public perception. This study develops a comprehensive framework for enhancing fake news detection, leveraging advanced machine learning techniques, privacy-preserving methods, and dynamic threat modeling. Key objectives include improving detection accuracy, ensuring user data privacy, and adapting to evolving misinformation tactics. By integrating ensemble learning methods such as Random Forests and Gradient Boosting, along with Natural Language Processing (NLP) techniques, the framework offers superior performance in identifying fake news. Additionally, privacy-preserving techniques like differential privacy and federated learning help address growing concerns over user data confidentiality. The research highlights the importance of ensuring compatibility with major social media platforms to maximize effectiveness and scalability. Comprehensive performance evaluations underscore the robustness of the proposed system. Recommendations include fostering collaboration among stakeholders, strengthening user engagement in evaluation processes, and advancing the framework's adaptability to dynamic misinformation tactics. This research contributes significantly to the ongoing fight against misinformation, promoting a more informed and resilient society through an efficient, privacy-focused detection system.

ACKNOWLEDGEMENT

While at Sri Lanka Institute of Information Technology, I have benefited from having great advisors who seem to agree about very little. Prof. Anuradha Jayakody was a great mentor, providing advice, constant constructive criticism of my ideas and writing, access to his web of contacts and friends, and the freedom to work on my own projects on his research account's time.

I would like to express my grateful gratitude to my principal supervisor Prof. Anuradha Jayakody for all his guidance, input, advice, and encouragement throughout the research. Many thanks also to Dr. Prasanna S. Haddella, Dr Harinda Fernado, Mr Amila Senarathne and Mr Kavinga Yapa Abeywardena.

I would like also like to thank Mr Sudharshana Gunawardena – Chairman ITN, Mrs Sanjivani Epa – General Manager ITN and all the staff of the ITN Engineering Division and IET Sri Lanka Network for fullest support, practical information and suggestions.

I also wish to thank all my MSc colleagues; I am grateful for all these unforgettable moments spent with you.

Finally, My Wife Anuradha, Two Sons Sanjula and Anjula and my mother for their never-ending support.

Table of Contents

List of Figure

List of Table