Security Threat Detection In Telecommunication Network In Compromised IoT Devices By Using Trustworthy Machine Learning

V. Aperame
Reg. No.: MS21909214
M.Sc. in IT
Specialized in Cyber Security

Supervisor: Dr. Prabath Lakmal Rupasinghe

October 2022

22 269 words

Department of Information Systems Engineering
Sri Lanka Institute of Information Technology

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

…….

Dr. Prabath Lakmal Rupasinghe (Supervisor)

Approved for MSc. Research Project:

……

Head/ Department Information Systems Engineering

Approved for MSc:

……...

Head – Graduate Studies

DECLARATION

"I declare that this is my own work and this dissertation does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to Sri Lanka Institute of Information Technology, the nonexclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books)."

Sign: …….....

Aperame Varatharaj

Date: ……..

ABSTRACT

Currently, Information Communication Technology (ICT) holds a significant part in the sphere. In IT, Cyber Security carry a massive position. Internet of Things (IoT) indicates to the vast number of tangible bodies which are affixed to the internet, by gathering and switching information with other apparatus and systems with the help of the internet. By using Machine Learning technique, the security threat detection is identified over the telecommunication network in compromised IoT devices. The Driver Anomaly Detection (DAD) Dataset is used for anomaly detection in IoT networks. Message Queue Telemetry Transport protocol (MQTT) is a messaging protocol which is based on Transmission Control Protocol (TCP) and utilized for to create communication between multiple devices. It is required to identify and distinguish the available threats presented in telecommunication network. This thesis gives an understanding about different security threats detection in telecommunication network using Machine Learning technique and explain about security constraints, issues presented.

By implementing Security Threat Detection System in an institute, it helps to assists analytical output concerning the imminent threats. Similarly, it aids to guarantee the fame of an association by launching faith among the workers. The above are the benefits obtained by a specific institution by consisting a Threat Detection System. Although there are existing Threat Detection Systems presented in the trade, but they are lacked in some instances like real time. So, in order to resolve all these problems, in this research as a result, ended up with a cost effective and ease of use comprehensive Threat Detection System in a telecommunication network in compromised IoT devices by using trustworthy machine learning.

ACKNOWLEDGEMENT

I would like to convey my deepest obligation to all those who provided me the support to complete this research successfully. An exceptional appreciation of gratitude to my supervisor Dr. Prabath Lakmal Rupasinghe for his contributions in stimulating suggestions and encouragements which helped me very much to coordinate my research domain. Whenever I need, my supervisor helps to resolve my doubts and give me the support in many ways, which helps me to accomplish my research in a successful manner. Also, I am heartily thankful to my supervisor to develop my knowledge, skills and attitude through this research.

I am also sincerely grateful to Dr. Anuradha Jayakody who is the head for Graduate Studies at SLIIT, for help me to complete my research in time without any delay during difficult period, by conducting lectures.

TABLE OF CONTENTS

List of Figures

List of Tables