شبكة المعلومات الجامعية

التوثيق الالكتروني والميكروفيلم

HANAA ALY

شبكة المعلومات الجامعية
التوثيق الإلكتروني والميكروفيلم

جامعة عين شمس

التوثيق الإلكتروني والميكروفيلم

قسم

نقسم بالله العظيم أن المادة التي تم توثيقها وتسجيلها
علي هذه الأقراص المدمجة قد أعدت دون أية تغيرات

يجب أن

تحفظ هذه الأقراص المدمجة بعيدا عن الغبار

HANAA ALY

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Computer Engineering and Systems Department

Secure coding for the Internet of Things (IoT)

A Thesis submitted in partial fulfillment of the requirements of
Masters in Electrical Engineering
(Computer and Systems Engineering)
by

Silvia Wahballa Soliman
Bachelor of Science
(Computer Engineering and Systems Department)
Faculty of Engineering, Ain Shams University, 2013

Supervised By

Prof. Dr. Ayman Mohammed Bahaa Eldin
Prof. Mohammed Ali Sobh

Date: 2021

AIN SHAMS UNIVERSITY
FACULTY OF ENGINEERING
Computer Engineering and Systems

Secure Coding for the Internet of Things (IoT)

Examiners' Committee

Name and affiliation **Signature**

Prof. Dr. AbdelNasser Hussein Reyad Zayed ....
Computer Engineering and Systems Department
Faculty of Engineering, Menoufia University.

Prof. Dr. Mohammed Mahmoud Taher ....
Computer Engineering and Systems Department
Faculty of Engineering, Ain Shams University.

Prof. Dr. Ayman Mohammed Bahaa Eldin ....
Computer Engineering and Systems Department
Faculty of Engineering, Ain Shams University.

Prof.Mohammed Ali Sobh ....
Computer Engineering and Systems Department
Faculty of Engineering, Ain Shams University.

Date:2021

Statement

This thesis is submitted as a partial fulfilment of Masters of science in Electrical Engineering, Faculty of Engineering, Ain Shams University. The author carried out the work contained in this thesis, and no part of it has been submitted for a degree or a qualification at any other research institution.

Silvia Wahballa Soliman

Signature

....

Date: 2021

Researcher Data

Name: Silvia Wahballa Soliman

Date of Birth: 29/08/1991

Place of Birth: Cairo, Egypt

Last academic degree: Bachelor Degree

Field of specialization: Computer and Systems Engineering

University issued the degree : Ain Shams University

Date of issued degree : 2013

Current job : Senior Technical Training Analyst at Archer Integrated Risk Management - an RSA company

Thesis Summary

Key words: Secure, coding, IoT, Internet Of Things, IoT, Malware, Machine Learning, Deep Learning, Dataset, attack, UNSW-NB15, Network Intrusion Detection, NIDS, Hierarchical

Internet is not only about humans accessing the Internet through their mobile phones or laptops but it’s extended to a plenty of devices like refrigerators, air conditioners, cars, light bulbs...etc. Therefore we have IoT. Currently IoT is a very important scope of research since it’s connecting the whole world together.

IoT has wide Economic, Industrial, Health benefits and many more. IoT devices are easy accessible and widely used, this caused many security challenges. One of the most challenging security problems in IoT is Network attacks like: worms, exploits, DoS ...etc. Therefore, a Network Intrusion Detection System is extremely important for a more secured IoT eco-system. From the most proven to be effective methods for malware detection recently is Machine learning.

That’s why in this thesis we present a cascaded NIDS in IoT using machine learning algorithms. The main purpose behind this research is presenting a NIDS that gives a good accuracy with good complexity. It detects the normal/abnormal traffic and if the traffic is abnormal then it will identify the type of abnormal traffic. Cascading was prefered for less complexity and better accuracy. We used in this research of the most recent and comprehensive data set in the latest 5 years which is UNSW-NB15 data set which contains a lot of modern IoT attacks. The experiment performed showed that Random Forest is the best algorithm for either binary (with accuracy 99.6%) or multi-class classification (with accuracy 90%). Also we used feature reduction to reduce the UNSW-NB15 features from 47 to 15 features.

Acknowledgment

I would like to express my deep gratitude to my supervisors prof.Ayman Bahaa eldin and dr.Mohammed Sobh for their help and support during the thesis work. Also my mom, dad and husband for always having my back during this long journey as well as dr. Taraggy Mohiy who helped me a lot and supported me with her knowledge.

Silvia Wahballa Soliman
Computer Engineering and Systems
Faculty of Engineering
Ain Shams University
Cairo, Egypt
2021

Contents

Contents xi

List of Figures xv

List of Tables xvi

1 Introduction 1

1.1 Introduction . . . 1
1.2 Motivation and Challenges . . . 2
1.2.1 IoT attack levels: . . . 2
1.2.2 Major security issues . . . 3
1.2.3 Network Intrusions in IoT . . . 4
1.2.4 Market Need . . . 4
1.2.5 Well known attacks in IoT . . . 5
1.2.5.1 Backdoors . . . 5
1.2.5.2 Worms . . . 5
1.2.5.3 DoS . . . 5
1.2.5.4 Exploit . . . 6
1.2.5.5 Reconnaissance . . . 6
1.2.5.6 Shellcode . . . 6
1.2.5.7 Analysis . . . 6
1.2.6 Motivation Summary . . . 7
1.3 Publications resulted from this research . . . 8
1.4 Aim of Research . . . 8
1.5 Thesis Contribution . . . 8
1.6 Thesis Outline . . . 9

2 Background 10

2.1 Network Intrusion Detection Systems . . . 10
2.2 Feature Reduction . . . 10
2.2.1 Feature Reduction using Random Forest . . . 11
2.3 Cross Validation . . . 11
2.4 Classification . . . 12
2.4.1 SVM . . . 12
2.4.2 DT . . . 13
2.4.3 K-Nearest Neighbor . . . 13
2.4.4 RF . . . 14
2.4.5 Artificial Neural Networks . . . 14