Intrusion Detection System using Autoencoder based Deep Neural Network for SME Cybersecurity

Khaizuran Aqhar Ubaidillah
Faculty of Computing
Universiti Malaysia Pahang,
Lebuhraya Tun Razak,
26600, Pekan, Pahang.
khzaqhar@gmail.com

Syifak Izhar Hisham
Faculty of Computing
Universiti Malaysia Pahang,
Lebuhraya Tun Razak,
26600, Pekan, Pahang.
syifakizhar@ump.edu.my

Ferda Ernawan
Faculty of Computing
Universiti Malaysia Pahang,
Lebuhraya Tun Razak,
26600, Pekan, Pahang.
ferda@ump.edu.my

Gran Badshah
College of Computer Science,
King Khalid University Abha,
Saudi Arabia
gdostan@kku.edu.sa

Edy Suharto
Department of Informatics,
Diponegoro University
Semarang, Indonesia
edy.suharto@gmail.com

2021 5th International Conference on Informatics and Computational Sciences (ICICoS) | 978-1-6654-3807-0/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICICOS53627.2021.9651851

***Abstract*— This paper proposes an intermediate solution using artificial intelligence to monitor any potential threat for SME, specifically in Malaysia. The proposed method uses Autoencoder based Deep Neural Network (AEDNN) trained with NSL-KDD dataset to efficiently detect possible cyber threats. This paper proposed AEDNN to detect automated threats cybersecurity and it does not intend to replace any existing security solutions. The proposed AEDNN is designed to detect any possible cyber threats accurately and consistently in the real-time network. The experimental results show that accurate results in the range between 96% to 99% specifically for SMEs in Malaysia.**

Keywords*— security, cyber threats, cybersecurity, network monitoring, detection system, deep neural network

I. INTRODUCTION

Cyber threats have rapidly grown with continuous difficulty and identification [1]. Nowadays, cyber threats become one of the most crucial factors that need to be considered for small and medium-sized enterprises (SME), small and medium-sized businesses (SMB), and also large companies in Malaysia. The large companies will not be focused on this study because they have fully-fledged Information Technology (IT) staff including experts that have broad network security skills to protect and ensure the company security.

Nowadays, SMEs have improved substantially in terms of their performance and efficiency by taking advantage of various opportunities by implementing the latest technologies such as digitalization of data management, cloud computing, etc [2]. Most SMEs have potentially become the target of cyber-attacks that can end up causing a lot of revenue loss, data breach, credentials stolen, and even destruction of the company itself. Based on the recent reports and statistics, roughly 80% of cyber-attacks are targeting companies and businesses globally, it consistently increases cyber-attack rate from the year 2016 towards 2019 in the intrusion and malware infection category in Malaysia. Most SMEs mainly focus on investing in the functionality of various contemporary technologies while putting their security as an afterthought. The problems which are specifically the issues of SMEs in Malaysia are becoming more vulnerable to cyber threats because of their lack of awareness, budget for a solution, or proper technical skills to handle it. Intrusion Detection System (IDS) can be categorized into two types of detection which are misuse detection and anomaly detection [3]. It shows that all security features mostly used signature-based detection which is less capable against advanced network threats. Moreover, IT staff is needed to be configured manually, so there will be possibilities that human errors might occur in the process and causing vulnerability towards the company's security.

This paper proposes Autoencoder based Deep Neural Network (AEDNN) to address the issues stated above. The approach is by creating an Artificial Intelligent system that can detect potential intrusion by monitoring and evaluating the traffic packets in real-time. If there are any potential cyber threats in the traffic, it can be detected. This solution can be integrated into any existing security systems such as Firewall, IPS, IDS, or SIEM in the network.

This paper is organized as follows. Section I presents the background of this research study. The related existing studies on cybersecurity using AI are discussed and analysed in Section II. Section III describes the proposed methodology including the proposed system, pre-processing, Deep Neural Network (DNN) design with autoencoder and the detailed AI architecture. Section IV shows the experimental results of the Autoencoder-based Deep Neural Network (AEDNN). Finally, Section 5 concludes this research work.

II. RELATED WORKS

The scheme by Larriva-Novo et al. [4] has done an extensive comparison in evaluating the most efficient approach towards obtaining the best performance in terms of detecting anomalies accuracy. The scheme proposed Feed Forward Neural Network (FFNN) and Recurrent Neural Network (RNN) as their AI models and categorized the dataset UNSW-NB15 by its characteristics into basic, content, traffic statistics, and direction-based. The scheme found out that the different models do not provide any significant differences in terms of accuracy. A group of data at a time and a smaller number of features can obtain an accurate prediction of the attack. Specifically, it was the FFNN with Adam optimizer and used Z-score as the normalization and linear rectifier as the activation function. The scheme achieved 98.8% accuracy with these specifications.