Available *online* at : http://jnte.ft.unand.ac.id/

Jurnal Nasional Teknik Elektro

| ISSN (Print) 2302-2949 | ISSN (Online) 2407-7267 |

INTRODUCTION

New cybersecurity risks have emerged because of the organizations of deploying Internet of Things (IoT) devices in information technology environments [1], [2]. These emerging risks have the capacity to undermine fundamental principles such as operational ecosystem security, efficiency, mobility, and safety [3]. The advent of novel threat vectors not only impacts the technological aspects of our lives but also poses risks to our financial and physical well-being. The potential for attacks has raised concerns regarding online privacy, social networks, businesses, and critical infrastructure [4]. In a short period of time, it has the potential to cause harm to the hardware system as well [5]. This phenomenon is anticipated to extend globally, driven by the imperative need to implement security measures across a broader and more critical spectrum of fields than ever before. However, this is only the initial phase of an increasingly advanced era of digitalization.

The Internet of Things (IoT) comprises interconnected smart devices, enabling them to collect and exchange information seamlessly [6]. In most cases, IoT systems are composed of three primary components: IoT devices, network elements, and the acquisition of sensory data [7]. One fundamental attribute of IoT devices is they are continually active [8], [9]. Amidst such rapid advancements, the substantial volume of statistics presents new challenges for the development of information security [10]. This progress must align with the emergence of increasingly advanced threats, such as exploits and vulnerabilities within global data networks and numerous technical and security challenges [11]. Among those challenges, one notable concern is the occurrence of anomalous network dataflow, commonly referred to as network intrusion or breach.

Intrusion refers to the deliberate attempts to a sequence of unexpected activities, whether originating locally or globally, that undermine the confidentiality, integrity, or availability of a network [12]. There are various avenues through which these attacks can be carried out, including exploiting vulnerabilities in applications, protocols, and web applications. The presence of malicious applications on interconnected devices within an IoT network further compounds the problem. The larger the IoT network, the greater the potential for vulnerabilities, as attackers can target any device connected to the network to gain unauthorized access. The increase of use of IoT-based systems amplifies the risk of these attacks, potentially leading to profound societal impacts [13]. The application of an Intrusion Detection System (IDS) is one of several approaches to overcome this problem.

Considering the increasing demand and the necessity to address future complex threats, the implementation of Machine Learning (ML) techniques can serve as a solution to amplify an IDS. Numerous research studies have applied ML-based approaches for intrusion detection [14]. Authors in [15] conducted research that extensively explores the malicious use of machine learning which aiming to undermine user privacy, system stability, and service integrity, while also enhancing techniques related to intrusion and obfuscation. Nonetheless, network traffic has grown increasingly intricate and subject to dynamic changes, while cyber-attacks continue to evolve daily. It implies that new standardized patterns or unknown attacks have the potential to deviate from the patterns learned from the initial training data [16], leading to numerous errors during the actual process of the detection of the attack detection system. To address this challenge, it is imperative to develop a methodology which capable to identify the real-time errors when detecting cyber-attacks and dynamically adjust the attack detection system based on the prevailing attack conditions.

There were numerous research studies focused on the application of ML methods in IDS [17]. Authors in [11] proposes an intrusion decision system using the Random Forest Bagging, Gradient Boosting, and XGB classifier and it has an accuracy value of 94.3%, 92% and 94.3%. In 2022, an experiment with ensemble learning bagging on IOT conducted to detect a multi-classification and attained 96.2% on N-BaIoT data set [18]. These studies setting a new standard and paving the way for future researchers to strive into this field by developed remarkable results and scores. However, most of these research efforts primarily relied on the combination of traditional ML techniques and outdated datasets for training and validation purposes. To bridge this gap, this study suggests the implementation of more advanced ML methods, specifically Random Forest, Decision Tree, and Logistic Regression algorithm using Ensemble Learning Technique. These methods will be applied to a newly curated dataset comprising comprehensive descriptions of intrusions.

https://doi.org/10.25077/xxxxx