1. Introduction

A website is a collection of pages that contain certain information and can be accessed by anyone, anytime, and anywhere. However, currently there are many problems that occur on a website, one of which is an attack on the web. For example, Cross-site Scripting, SQL Injection, DDoS Attack, and many attacks that occur on the website. Cross-Site Scripting or commonly abbreviated as XSS is an attack that injects code into HTML into web pages [1]. There are multiple methods for injecting JavaScript code into a victim's web application. Attackers frequently do this by inserting a script into one of the website's pages, causing the victim to download the script from the site. This scenario occurs when the web application accepts user input on its web pages, allowing the attacker to embed malicious JavaScript code that is reflected as executable code in the victim's browser [2]. Websites today face numerous challenges, among which web attacks like SQL Injection, DDoS, and also Cross-site scripting or XSS attacks are particularly prevalent. XSS, for instance, involves inserting malicious code, typically JavaScript, into web pages that are then executed in the user's browser. This type of attack occurs when a web application incorporates user input into its pages without adequate validation, enabling attackers to embed harmful scripts. These scripts can steal data, manipulate page content, or perform other malicious actions. The versatility of XSS attacks and the complexity of securing web applications against such vulnerabilities make it a significant threat to web security, necessitating robust measures to sanitize and validate user inputs to prevent these exploits [1][2].

Currently, there are many applications or systems that can help detect intrusions or attacks carried out by attackers, and some of these systems have been improved by incorporating Machine Learning, enabling them to detect attacks or intrusions more effectively [3][4]. Deep Learning an area within Machine Learning and Artificial Intelligence, has become a fundamental technology in the Industrial Revolution 4.0, providing enhanced abilities to analyze extensive datasets and detect patterns indicative of potential security risks [5][6]. A prominent architecture in this domain is Long Short-Term Memory (LSTM), a form of Recurrent Neural Network (RNN) that employs gradient-based learning techniques to address the difficulties of handling long-term dependencies in sequential data [7].

LSTM is particularly adept at addressing the error backflow problem, which is a common issue in traditional RNNs where gradients can diminish or explode, leading to poor learning efficiency [8]. By maintaining a constant error flow, LSTM networks can retain information over extended periods, making them highly effective for tasks such as time series prediction, anomaly detection, and, crucially, intrusion detection in cybersecurity. The integration of LSTM with ML algorithms enhances the system's ability to predict and respond to threats by learning from historical data, recognizing patterns of normal versus anomalous behavior, and adapting to new, unseen attack strategies, thus providing a robust defense mechanism against evolving cyber threats. This study aims to identify Cross-site Scripting (XSS) attacks using the Long Short-term Memory (LSTM) method to detect attacks from user input and to measure the accuracy, loss, precision, recall, and F1 score.