Nile Valley University Publications
Nile Journal for Science and Engineering (NJSE)
(ISSN:3122-5993)
Volume 02, No. 01, 2026
nilevalley.edu.sd

LOF-Based Anomaly Detection Approach for Mitigating DOS Attacks

Alaa Mustafa Mohamed[1] and Mirghani Ahmed Eltahir[2]

1 Faculty of Engineering, University of Science and Technology, Omdurman, Sudan
2 Faculty of Computer Sciences, Nile Valley University, Atbara, Sudan

Corresponding Author: Alaa00mu@gmail.com

Received: 3rd November, 2025 Accepted: 22nd December, 2025

Abstract:

This research was conducted using the Kali Linux operating system, which is a specialized platform in cyber security and penetration testing due to its powerful tools for network analysis and vulnerability detection. Open-source tools such as Wireshark and T Shark were employed to capture and analyze network traffic, enabling the researcher to study network data flows in detail and with precision. After data collection, the Local Outlier Factor (LOF) algorithm was implemented using Python and the scikit-learn library- one of the most prominent machine learning libraries for data analysis and anomaly detection. The study also referred to a set of modern academic sources and scientific papers discussing cybersecurity and data analysis, including works that examined the effectiveness of the LOF algorithm in detecting abnormal network activities.

Keywords: *Local Outlier Factor – LOF, Anomaly Detection, Network Security, Denial of Service - DoS Attacks, Network Traffic Analysis.*

نهج للكشف عن الشذوذ باستخدام معامل العزل المحلي (LOF) للتصدي لهجمات حجب الخدمه

الاء مصطفى محمد وميرغني احمد الطاهر

كلية الهندسة، جامعة العلوم والتقانة، امدرمان، السودان
كلية علوم الحاسوب، جامعة وادي النيل، عطبرة، السودان

المؤلف المرسل: Alaa00mu@gmail.com

تاريخ الاستلام: 3 نوفمبر، 2025م **تاريخ القبول: 22 ديسمبر2025م**

المستخلص:

تم إجراء هذا البحث باستخدام نظام التشغيل كالي لينكس، وهو منصة متخصصة في الأمن السيبراني واختبار الاختراق بسبب أدواته القوية لتحليل الشبكات واكتشاف الثغرات. تم استخدام أدوات مفتوحة المصدر مثل Wireshark و TShark لالتقاط وتحليل حركة مرور الشبكة، مما مكن الباحث من دراسة تدفقات بيانات الشبكة بالتفصيل وبدقة. بعد جمع البيانات، تم تنفيذ خوارزمية معامل العزل المحلي (LOF) باستخدام بايثون ومكتبة scikit-learn- وهي واحدة من أبرز مكتبات تعلم الآلة لتحليل البيانات واكتشاف الشذوذ. كما أشارت الدراسة إلى مجموعة من المصادر الأكاديمية الحديثة والأوراق العلمية التي تناقش الأمن السيبراني وتحليل البيانات، بما في ذلك الأعمال التي درست فعالية خوارزمية LOF في اكتشاف الأنشطة الشبكية غير الطبيعية.

كلمات مفتاحية: *معامل العزل المحلي ، كشف الشذوذ، أمن الشبكات ،هجمات حجب الخدمة، تحليل حركة الشبكة*