DOI:10.3969/j.issn.1003-5060.2026.02.004

基于特征融合的 SQL 注入多分类检测

姜珍珍[1], 杨彬彬[2], 薛 峰[3]

(1.合肥工业大学 计算机与信息学院,安徽 合肥 230601; 2.安徽三实软件科技有限公司,安徽 合肥 230601; 3.合肥工业大学 软件学院,安徽 合肥 230601)

摘 要:SQL 注入攻击是一种常见的网络安全威胁,因此检测 SQL 注入成为网络安全领域的一项重要研究内容。传统 SQL 注入检测方法存在准确性低、无法确定 SQL 注入攻击的具体类型等问题,文章提出一种基于特征融合的 SQL 注入攻击多分类检测方法(feature fusion-based multi-class SQL injection detection,FMC-SID)。实验结果表明,该方法不仅达到了 99.99%的准确率,而且能够确定 SQL 注入攻击的具体类型,为安全人员提供更加具体的 SQL 注入攻击的描述信息和意图,以制定更有针对性的应对措施,提高网络安全的防护能力。

关键词:SQL 注入检测;网络安全;多分类;特征融合;深度学习;SQL 标准化

中图分类号:TP391.41 **文献标志码**:A **文章编号**:1003-5060(2026)02-0167-07

Feature fusion-based multi-class SQL injection detection

JIANG Zhenzhen[1], YANG Binbin[2], XUE Feng[3]

(1. School of Computer Science and Information Engineering, Hefei University of Technology, Hefei 230601, China; 2. Anhui Sanshi Software Technology Co., Ltd., Hefei 230601, China; 3. School of Software, Hefei University of Technology, Hefei 230601, China)

Abstract: Structured query language(SQL) injection attack is a common network security threat, so detecting SQL injection has become an important research topic in the field of network security. Traditional SQL injection detection methods have problems such as low accuracy and inability to determine the specific type of SQL injection attack. Therefore, this paper proposes a feature fusion-based multi-class SQL injection detection(FMC-SID) method. The experimental results show that this method not only achieves an accuracy of 99.99%, but also identifies the specific type of SQL injection attack, which can provide security personnel with more specific description and intention of SQL injection attack, enabling them to develop more targeted countermeasures and improve network security protection capabilities.

Key words: structured query language(SQL) injection detection; network security; multi-class classification; feature fusion; deep learning; SQL normalization

0 引 言

随着用户对 Web 应用程序的依赖程度不断增加,后端数据库中存储的敏感个人信息数量也随之增长,因此数据库的高价值性使其成为黑客攻击的主要目标。黑客采用 SQL 注入攻击手段窃取数据库中的信息,因此检测和预防 SQL 注入攻击十分重要。然而由于很多 Web 应用程序在开发过程中缺乏对安全性问题的充分考虑,导致黑客可以通过恶意输入(SQL 注入)执行对数据

收稿日期:2023-08-24;**修回日期**:2023-09-18

基金项目:国家自然科学基金资助项目(62272143)

作者简介:姜珍珍(1998—),女,安徽安庆人,合肥工业大学硕士生;

薛 峰(1978—),男,安徽六安人,博士,合肥工业大学教授,博士生导师,通信作者,E-mail:feng.xue@hfut.edu.cn.

库的攻击,进而对网站和用户造成巨大的危害。SQL 注入攻击的威胁不仅限于破坏数据的完整性,还可能涉及身份验证、授权、保密等安全问题,因此已成为 Web 应用程序安全性的头号攻击手段[1]。

为保护 Web 应用程序免受 SQL 注入攻击,安全人员通常采用入侵检测系统[2]或 Web 应用程序防火墙[3],这 2 种安全机制通常采用基于规则的方法检测 SQL 注入攻击。这种规则的检测方法不仅需要大量的专家配置,还可能会漏掉一些未知的、新型的攻击,并且容易被攻击者通过编码等变异技术规避,导致安全机制被攻破。

采用机器学习的方法检测 SQL 注入攻击可以弥补上述方法的不足。该方法无需预设规则,可自动学习攻击特征,并结合查询语句的语法与语义信息提升检测准确率。文献[4]通过对比实验,初步验证机器学习在此任务中的优势。然而,现有研究多聚焦于二分类问题(判断是否为攻击),虽有助于提升系统安全性,却难以实现对不同 SQL 注入攻击类型的精准识别和细分。

本文针对以上问题提出一种基于特征融合的 SQL 注入攻击多分类检测方法(feature fusion-based multi-class SQL injection detection,FMC-SID)。首先为 SQL 注入攻击负载标注类型,如错误注入、时间注入、联合注入、布尔注入和堆叠注入等;然后使用标准化方法处理这些 SQL 注入攻击负载,并将原始负载与标准化之后的负载进行特征融合;最后使用融合后的特征作为卷积神经网络的输入进行训练,并预测分类 SQL 注入攻击负载的具体类型。

1 相关工作

传统的 SQL 注入检测方法主要依赖规则集匹配,通过预定义规则识别查询语句中的特定攻击模式。该方法实现简单,但规则集需人工维护,难以检测变异或经过掩盖的攻击[5]。此外,该方法依赖复杂的正则表达式进行编译与解析,检测过程耗时较长。为提升效率,文献[6]提出一种基于签名的检测方法,通过提取 SQL 查询的指纹特征并与预存指纹库进行快速比对,以实现高效判断。

为了克服基于规则集匹配方法的不足,基于机器学习的 SQL 注入检测方法逐步成为研究热点。文献[7-8]采用机器学习、深度学习的方法检测 SQL 注入,初步证明机器学习方法在该领域的有效性;文献[4]采用机器学习方法识别 HTTP 查询字符串中的注入特性,并对比多层感知机、递归神经网络(recurrent neural network,RNN)[9]以及长短期记忆网络(long short-term memory,LSTM)[10]等多种分类模型的性能;文献[11]将 SQL 查询语句建模为令牌图,并使用节点的中心度度量训练支持向量机(support vertor machine,SVM)[12]以检测 SQL 注入;文献[13]对用户 URL 访问日志中的数据进行统计研究,基于统计结果设计几种不同的特征训练多层感知机实现 SQL 注入的检测;文献[14]提出基于 LSTM 的 SQL 注入攻击检测方法和一种基于数据传输通道的注入样本生成方法;文献[15]从包含恶意注入的查询中总结特征,并使用这些特征训练集成分类算法以检测查询是否为恶意;文献[16]提出针对 NoSQL 数据库的注入攻击检测,最终分类算法能识别出 97.6%的注入攻击。

2 数据准备

在构建数据集前,本文进行数据标注、增强等预处理工作。所构建的数据集(SQLInjData)包含布尔、时间、错误、联合、堆叠注入等多种 SQL 攻击负载以及正常用户输入,数据来源于 Kaggle 平台并已进行整合与去重。针对其中数量较少的堆叠注入类型,本文通过数据增强技术扩充其样本数量。

2.1 数据标注

文献[17]总结分析目前已知类型的 SQL 注入攻击负载的特征,本文依据此分类标准对数据集 SQLInjData 中的 SQL 注入攻击负载进行类型标注,类型描述见表 1 所列。

表 1 SQL 注入攻击负载类型描述

类型	描述
Boolean(b)	攻击者通过在查询中注入含布尔逻辑的条件窃取数据库中的数据
Time(t)	攻击者在查询中注入时间函数,通过观察数据库是否延迟响应获取数据库信息
Error(e)	攻击者在查询中注入导致语法错误的语句,利用数据库在执行这些错误的语句时服务器返回的错误消息获得数据库信息
Union(u)	攻击者在原查询后添加 Union 关键字和恶意的 Select 查询语句,并使其与原始查询一起执行
Stack(s)	攻击者在原查询后添加查询分隔符和任意的恶意查询语句,并使其与原始查询一起执行
False(f)	用户正常输入

SQLInjData 中还有攻击者使用十六进制、ASCII、Unicode 字符重新编码攻击字符串的变异 SQL 负载，为了正确标注变异 SQL 负载的攻击类型，本文在为其标注类型之前先对其解码。

2.2　数据增强

本文的数据增强主要针对样本数很少的堆叠注入攻击负载，堆叠注入就是试图在原查询后面添加恶意 SQL 命令，因此堆叠注入的数据增强采用如下 2 种方法。

1）基于堆叠注入负载结构的变换。以堆叠注入负载’;drop table users;- -为例，如果攻击者输入该负载到 pass 字段中，应用程序生成查询：

select info from users where login=‘admin’ and pass=‘’;drop table users;- -’ and pin=‘’，那么此时 pass 字段被用户输入的单引号闭合，攻击者最后输入的注释符会闭合后面所有原本需要用户填写验证的字段（如 pin 字段），而攻击者输入的分号就分隔开 2 条 SQL 语句，数据库会依次执行原始 SQL 语句和攻击者在分号之后输入的 SQL 语句，此时由于攻击者的恶意注入会导致数据库中的 users 表被删除。由此可见，堆叠注入结构主要包含：① 单引号，用于闭合字段；② 分号及恶意 SQL 语句，用于执行攻击；③ 注释符，用于注释原查询剩余部分。

堆叠注入的增强可以通过在保持其结构不变的基础上适当变换：① 在单引号前面添加具体验证字段 admin’，或者在单引号后面添加永真表式’or 1=1 让原查询语句闭合以达到绕过验证的效果；② 在第 2 部分添加多个；drop table users 结构，让数据库同时执行多条恶意 SQL 语句；③ 第 3 部分可以替换注释符。

2）基于 SQL 命令内部结构的变换。除了在堆叠注入结构方面进行数据增强，也可以从改变所添加 SQL 语句的内部结构入手，将 Drop 语句换成其他类型的 SQL 语句；在所添加 SQL 语句的某个字段里面添加通配符，如可以将 select 变换成 selec%t 或 s * elect、改变语句中 where 字段后面的条件等。

3　本文方法

本文提出的基于特征融合的 SQL 注入多分类检测方法 FMC-SID 结构由标准化特征融合模块、特征提取模块、网络鉴别器 3 个模块组成，如图 1 所示。

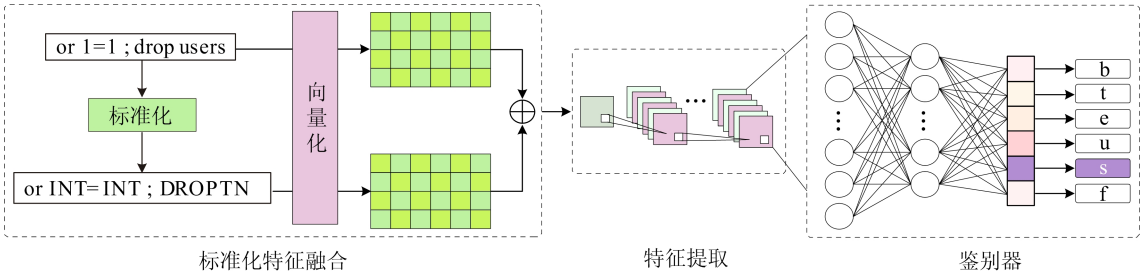


图 1　FCM-SID 结构

标准化特征融合模块先将原始 SQL 注入攻击负载转换为标准形式的 SQL 负载，接着对原始 SQL 负载和标准化形式的 SQL 负载进行向量化，并使用特征融合技术将这 2 组向量数据相加得到融合后的向量数据。特征提取模块采用全卷积结构对融合后的向量数据进行特征提取操作，并通过改变卷积结构的卷积核配置来提取丰富的高维度特征。鉴别器模块采用线性结构对这些高维度特征进行类型鉴别。

为了充分利用这些高维度的特性信息，鉴别器采用线性结构，该结构每个单元都能从提取的特征中获取到完整的特征信息，从而提高鉴别的准确率。

3.1　标准化特征融合模块

3.1.1　标准化处理

SQL 注入攻击负载的形式多变，攻击者可以构造各种变异的负载来实现各种不同的恶意操作，如通过重新编码负载的方式以规避常规的检测，因此本文先将负载解码再进行标准化处理。

SQL 注入攻击语句中通常包含：① 特殊字符，如单引号、双引号、分号、括号、注释符等；② SQL 语法结构，如关键字 SELECT、UPDATE、UNION、WAITFOR 以及函数 SUM、CONCAT、CAST 等，这两类字符是区别 SQL 注入类型的典型特征，因此本文在进行标准化处理时保留这些重要特征，只对注入攻击语句中无关

紧要的字符信息进行标准化。标准化处理步骤如下:① 替换表名、表别名、列名、运算符等为统一的标准化词汇占位符;② 替换整数、浮点数、十进制数、八进制数等数值类型为 INT、FLOAT、HEX、OCT 等字符;③ 替换字符串类型为 STRING 字符;④ 去除无效字符,如空格、制表符、换行符。

本文首先对 SQL 注入攻击负载进行解码,将负载中的编码转换为正常的形式,若负载中不包含编码,则解码后的负载保持不变;然后对解码后的负载进行标准化处理。SQL 注入攻击负载标准化示意图如图 2 所示,负载语句中包含编码部分。在解码阶段,成功提取出语句中的编码部分并对其进行解码操作;在标准化阶段,对解码后的语句进行进一步的标准化处理。这一步骤将表达式、表名、列名以及列值都标准化为指定字符。

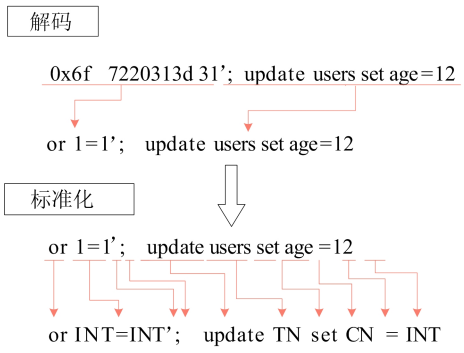


图 2 SQL 注入攻击负载标准化示意图

3.1.2 文本向量化

本文采用训练词向量模型 Word2Vec[18] 对 SQL 负载进行向量化。训练词向量模型 Word2Vec[18] 通过考虑单词在上下文中的出现模式来学习单词的向量表示,这种词向量化方法能够更好地捕捉到单词之间的语义和语法关系。具体步骤如下:① 使用 SQLInjData 数据集作为语料库训练 Word2Vec 模型;② 将训练好的模型权重作为神经网络 Embedding 层的初始化参数,不再对 Embedding 层的权重参数进行梯度更新;③ 得出SQL 负载的向量化表示。

3.1.3 特征融合

特征融合是一种将不同类型的特征或者处理后的特征进行组合的方法,旨在提高深度学习模型的性能和泛化能力。为了减少输入负载的信息冗余,本文首先对 SQLInjData 中的原始数据进行标准化处理,使模型更容易学习 SQL 注入攻击负载的特征和模式,从而提高模型的鲁棒性。但是 SQL 负载的标准化操作会丢失 SQL 负载的原始信息,因此本文参考残差网络的思想,将原始输入的特征和标准化之后的特征进行相加,作为分类模型的输入。该方式使得模型同时处理 2 种类型的数据,以获得更有信息量的特征表示。假设原始数据为 x,标准化后的数据为 $n(x)$,融合后的输入 F 计算公式为:

$$F = x + n(x) \tag{1}$$

3.2 特征提取模块

特征提取模块使用全卷积结构从输入中提取高维度的特征,卷积结构能够并行处理 SQL 负载中单词的时序信息,并通过设置不同的卷积核提取不同维度的特征信息。本文使用宽度逐渐增加的卷积核(3~5)兼顾相邻单词的相关信息和相距较远的单词信息,因此能够从每个 SQL 负载中提取到丰富的上下文信息。

3.3 鉴别器

本文使用深度卷积神经网络从 SQL 负载中提取高维度特征,为了能够充分利用这些特征信息,使用线性结构设计 SQL 负载鉴别器,线性结构中的每个单元都能直接参与所提取特征的计算。根据本文介绍的分类规则,SQL 注入攻击负载有 5 种类型,加上正常用户正常输入这一类,鉴别器的最后一层设置 6 个单元,每个单元输出对应类型的概率,取其中最高的概率就是该条 SQL 负载的类型。

4 实验与结果

4.1 实验设置

本文 FMC-SID 方法中的模型主要由输入层、卷积层、全连接层 3 个部分组成。在模型训练过程中为了防止模型过拟合,对全连接层的输出执行 dropout 操作,其参数设置为 0.2,批次大小为 64,学习率设置为 0.001,使用 CrossEntropyLoss 交叉熵损失函数计算损失。最后使用 Adam[19] 优化器更新模型的参数。

此外,本文使用 TfidfVectorizer 直接将文本数据转化为数值型的向量表示,作为随机森林、决策树、逻辑回归算法等传统机器学习算法的输入[12],评估这些算法在 SQL 注入攻击负载多分类任务上的性能作为对比实验。因为 TfidfVectorizer 得出的文本向量长度较长,所以本文采用 TruncatedeSVD[12] 对数据进行降维处理。

4.2 评价指标

为了评估模型在各个类别 SQL 负载上的性

能，本文采用 F_1 值[20]、召回率 R[21]、精确率 P[21] 等指标进行评价，计算公式分别为：

$$R_i = \frac{T_i}{T_i + N_i} \tag{2}$$

$$P_i = \frac{T_i}{T_i + F_i} \tag{3}$$

$$F_{1i} = \frac{2P_iR_i}{P_i + R_i} \tag{4}$$

其中：i 为第 i 个类别；T_i、F_i、N_i 分别第 i 个类别的真阳性数、假阳性数、假阴性数。

为了评估模型在整体上的性能，本文采用准确率 A 作为主要评估指标，使用宏平均 m 下的精确率、召回率、F_{1m} 值进行更加全面的评估。

$$R_m = \frac{\sum_{i=1}^{k} R_i}{k} \tag{5}$$

$$P_m = \frac{\sum_{i=1}^{k} P_i}{k} \tag{6}$$

$$F_{1m} = \frac{2P_mR_m}{P_m + R_m} \tag{7}$$

其中：R_i、P_i 分别为式(2)、式(3)的计算结果；k 为总类别数，本文 k 为 6。采用混淆矩阵[12] 可视化模型分类结果，混淆矩阵大小为 $n \times n$ 的矩阵，n 为总类别数，本文 n 为 6。

4.3　实验结果分析

4.3.1　对比实验

将本文的 FMC-SID 方法与机器学习算法在整体性能上进行对比，结果见表 2 所列。从表 2 可以看出，FMC-SID 方法的 A 为 99.99%，宏平均 F_{1m} 为 99.98%。

相较于机器学习算法，FMC-SID 方法在这 2 个指标上都有明显的提升，表明本文方法在 SQL 注入多分类检测任务上具有较高的分类能力和综合性能。

表 2　FMC-SID 方法与机器学习算法性能对比　%

算法	A	F_{1m}
FMC-SID	99.99	99.98
随机森林	99.68	98.40
决策树	98.84	95.99
逻辑回归	95.47	90.76

SQL 注入攻击负载多分类识别结果见表 3 所列。从表 3 可以看出，F_1、P、R 数值较高，在某些类别上几乎能够达到 100.00%，表明模型能够对各个类别 SQL 负载都进行准确的分类，而没有出现在某些少样本类别上性能下降的情况。

表 3　SQL 注入攻击负载多分类识别结果　%

类别	F_1	R	P
f	100.00	100.00	100.00
e	100.00	100.00	100.00
t	99.87	99.74	100.00
b	99.96	99.85	99.92
u	100.00	100.00	99.98
s	100.00	100.00	100.00

由预测结果构成的混淆矩阵[12] 如图 3 所示。

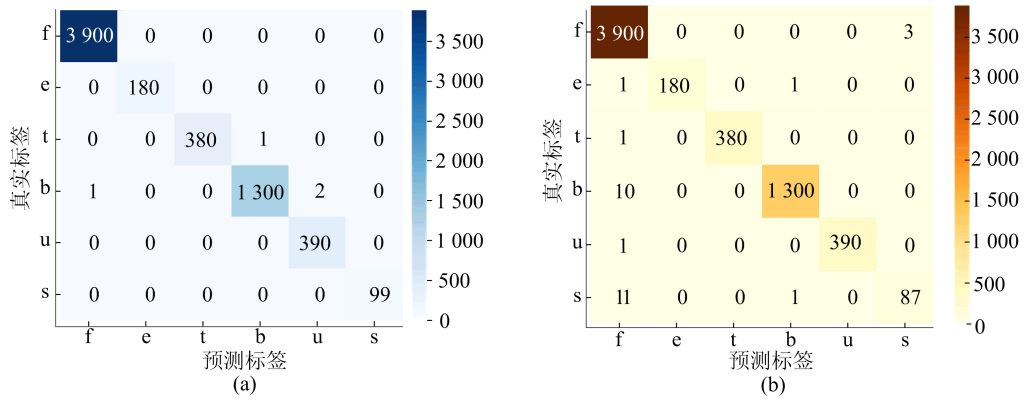


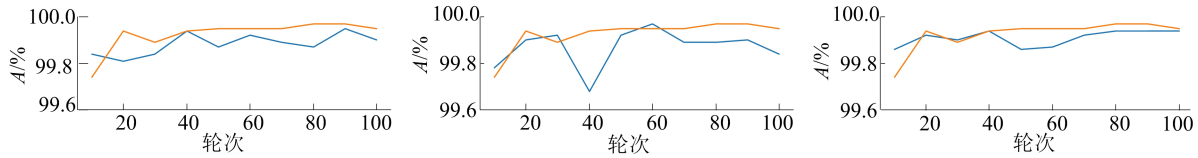
图 3　与机器学习算法的预测结果对比

从图 3a 可以看出，FMC-SID 方法能够近乎完全准确地识别所有 SQL 负载类别；从图 3b 可以看出，传统机器学习算法对 99 个堆叠注入样本中的 12 个出现误判，分类性能明显较弱。

4.3.2　消融实验

为验证 FMC-SID 采用预训练模型(Word2Vec)进行 SQL 负载词向量化的有效性，本文针对词向量化方法设计一组消融实验，并与

随机初始化嵌入(Embed)方法进行对比。引入特征融合机制,同时利用 SQL 负载的标准化与个性化特征使模型在不丢失原始信息的前提下学习高层表征,以驱动分类性能提升。通过消融实验验证其有效性,实验结果如图 4 所示。图 4 中,黄色、蓝色折线分别为使用 Word2Vec 词向量化方法、Embed 词向量化方法时 FMC-SID 的多分类准确率。从图 4a 可以看出,训练 20 个轮次后,Word2Vec 方法的准确率始终优于 Embed 方法的准确率,且波动更小,训练过程更稳定。从图 4b可以看出,去除特征融合后模型性能波动显著,训练至 60 个轮次后准确率明显下降,说明仅依靠标准化输入会丢失 SQL 负载的原始特征,从而降低模型性能。从图 4c 可以看出,Word2Vec 词向量化方法与特征融合叠加能够有效提升模型性能。



(a) 词向量化方法 (b) 特征融合机制 (c) 词的量化方法与特征融合机制叠加

图 4 词向量方法、特征融合机制及其叠加的消融结果

5 结 论

为了解决 SQL 注入攻击检测的多分类问题,本文提出一种基于标准化特征融合的 SQL 注入检测多分类方法 FCM-SID,在能够检测是否为 SQL 注入攻击的同时给出具体的攻击类型,为信息系统安全人员提供更多的参考信息,以针对各种 SQL 注入类型的攻击采取不同的应对策略。在今后的工作中,将致力于检测其他重要的应用程序的攻击类型,如命令注入、轻量级目录访问协议注入以及跨站脚本攻击注入等。

[参 考 文 献]

[1] HELMIAWAN M A, FIRMANSYAH E, FADIL I, et al. Analysis of web security using open web application security project 10[C]//2020 8th International Conference on Cyber and IT Service Management (CITSM). [S. l.]: IEEE, 2020. DOI: 10.1109/CITSM50537.2020.9268856.

[2] LIAO H J, LIN C H R, LIN Y C, et al. Intrusion detection system: a comprehensive review[J]. Journal of Network and Computer Applications, 2013, 36(1): 16-24.

[3] PRANDL S, LAZARESCU M, PHAM D S. A study of web application firewall solutions[C]//ICISS 2015: Proceedings of the 11th International Conference on Information Systems Security-Volume 9478. [S. l.]: Springer, 2015: 501-510.

[4] VOLKOVA M, CHMELAR P, SOBOTKA L. Machine learning blunts the needle of advanced SQL injections[J]. Mendel, 2019, 25(1): 23-30.

[5] LUPTAK P. Bypassing web application firewalls[C]//Proceedings of 6th International Scientific Conference on Security and Protection of Information. [S. l: s. n.], 2011: 79-88.

[6] APPIAH B, OPOKU MENSAH E, QIN Z. SQL injection attack detection using fingerprints and pattern matching technique[C]//2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS). [S. l.]: IEEE, 2017. DOI: 10.1109/ICSESS.2017.8342983.

[7] JOSHI A, GEETHA V. SQL Injection detection using machine learning[C]//2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). [S. l.]: IEEE, 2014. DOI: 10.1109/ICCICCT.2014.6993127.

[8] FALOR A, HIRANI M, VEDANT H, et al. A deep learning approach for detection of sql injection attacks using convolutional neural networks[J]. Proceedings of Data Analytics and Management, 2021. DOI: 10.1007/978-981-16-6285-0_24.

[9] MIKOLOV T, KARAFI M, BURGET L, et al. Recurrent neural network based language model[J]. ACM, 2011. DOI: 10.1145/3236024.3264597.

[10] HOCHREITER S, SCHMIDHUBER J. Long short-term memory[J]. Neural Computation, 1997, 9(8): 1735-1780.

[11] KAR D, PANIGRAHI S, SUNDARARAJAN S. SQLiGoT: detecting SQL injection attacks using graph of tokens and SVM[J]. Computers & Security, 2016, 60: 206-225.

[12] SWAMI A, JAIN R. Scikit-learn: machine learning in python[J]. Journal of Machine Learning Research, 2013, 12(10): 2825-2830.

[13] TANG P, QIU W, HUANG Z, et al. Detection of SQL injection based on artificial neural network[J]. Knowledge-Based Systems, 2020, 190: 105528.

[14] LI Q, WANG F, WANG J, et al. LSTM-based SQL injection detection method for intelligent transportation system [J]. IEEE Transactions on Vehicular Technology, 2019, 68(5): 4182-4191.

(下转第 193 页)

Geology,2021,236:103671.

[7] BERNE C,ELLISON C K,DUCRET A,et al. Bacterial adhesion at the single-cell level[J]. Nature Reviews Microbiology,2018,16:616-627.

[8] ROSSI E,PARONI M,LANDINI P. Biofilm and motility in response to environmental and host-related signals in Gram negative opportunistic pathogens[J]. Journal of Applied Microbiology,2018,125(6):1587-1602.

[9] ODER M,ARLIČ M,BOHINC K,et al. *Escherichia coli* biofilm formation and dispersion under hydrodynamic conditions on metal surfaces[J]. International Journal of Environmental Health Research,2018,28(1):55-63.

[10] JARA J,ALARCÓN F,MONNAPPA A K,et al. Self-adaptation of *Pseudomonas fluorescens* biofilms to hydrodynamic stress[J]. Frontiers in Microbiology,2020,11:588884.

[11] MANUEL C M,NUNES O C,MELO L F. Unsteady state flow and stagnation in distribution systems affect the biological stability of drinking water[J]. Biofouling, 2010, 26(2):129-139.

[12] PALMER J,FLINT S,BROOKS J. Bacterial cell attachment,the beginning of a biofilm[J]. Journal of Industrial Microbiology and Biotechnology,2007,34(9):577-588.

[13] STOODLEY P,DODDS I,BOYLE J D,et al. Influence of hydrodynamics and nutrients on biofilm structure[J]. Journal of Applied Microbiology,1998,85(Suppl1):19S-28S.

[14] PAN M,LI H Z,HAN X Y,et al. Effects of hydrodynamic conditions on the composition,spatiotemporal distribution of different extracellular polymeric substances and the architecture of biofilms[J]. Chemosphere,2022,307:135965.

[15] FLEMMING H C,WINGENDER J. The biofilm matrix [J]. Nature Reviews Microbiology,2010,8:623-633.

[16] SCOTT M,HWA T. Bacterial growth laws and their applications[J]. Current Opinion in Biotechnology,2011,22: 559-565.

[17] SEZONOV G,JOSELEAU-PETIT D,D'ARI R,et al. *Escherichia coli* physiology in Luria-Bertani broth[J]. Journal of Bacteriology,2007,189(23):8746-8749.

[18] SZTILKOVICS M,GERECSEI T,PETER B,et al. Single-cell adhesion force kinetics of cell populations from combined label-free optical biosensor and robotic fluidic force microscopy[J]. Scientific Reports,2020,10:61.

[19] TSAI Y P. Impact of flow velocity on the dynamic behaviour of biofilm bacteria[J]. Biofouling,2005,21(5/6):267-277.

[20] TEODÓSIO J S,SIMÕES M,MELO L F,et al. Flow cell hydrodynamics and their effects on *E. coli* biofilm formation under different nutrient conditions and turbulent flow [J]. Biofouling,2011,27(1):1-11.

[21] THOMEN P,ROBERT J,MONMEYRAN A,et al. Bacterial biofilm under flow:first a physical struggle to stay,then a matter of breathing[J]. PLoS ONE,2017,12(4):e0175197.

[22] XUE Z,SENDAMANGALAM V R,GRUDEN C L,et al. Multiple roles of extracellular polymeric substances on resistance of biofilm and detached clusters[J]. Environmental Science & Technology,2012,46(24):13212-13219.

[23] JIN C L,YU Z W,PENG S Y,et al. The characterization and comparison of exopolysaccharides from two benthic diatoms with different biofilm formation abilities[J]. Annals of the Brazilian Academy of Sciences, 2018, 90(2): 1503-1519.

[24] HOU J P,VEEREGOWDA D H,VAN DE BELT-GRITTER B,et al. Extracellular polymeric matrix production and relaxation under fluid shear and mechanical pressure in *Staphylococcus aureus* biofilms[J]. Applied and Environmental Microbiology,2018,84(1):e01516-17.

[25] HERMANSSON M. The DLVO theory in microbial adhesion[J]. Colloids and Surfaces B:Biointerfaces,1999,14: 105-119.

(责任编辑　张淑艳)

(上接第 172 页)

[15] KASIM Ö. An ensemble classification-based approach to detect attack level of SQL injections[J]. Journal of Information Security and Applications,2021,59:102852.

[16] MEJIA-CABRERA H I,PAICO-CONTRERAS D,VALDERA-CONTRERAS J H,et al. Automatic detection of injection attacks by machine learning in nosql databases [C]//Mexican Conference on Pattern Recognition. Cham: Springer International Publishing,2021:23-32.

[17] KUMAR P,PATERIYA R. A survey on SQL injection attacks,detection and prevention techniques[C]//Third International Conference on Computing Communication & Networking Technologies. [S. l.]:IEEE,2012:6396096.

[18] MIKOLOV T,CHEN K,CORRADO G,et al. Efficient estimation of word representations in vector space[EB/OL]. [2023-07-20]. https://blog.csdn.net/qq_37388085/article/details/102593614.

[19] KINGMA D P,BA J. Adam:a method for stochastic optimization[EB/OL]. [2023-07-20]. https://blog.csdn.net/weixin_47133012/article/details/124900178.

[20] CHICCO D,JURMAN G. The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation[J]. BMC Genomics,2020,21:1-13.

[21] BUCKLAND M,GEY F. The relationship between recall and precision[J]. Journal of the American Society for Information Science,1994,45(1):12-19.

(责任编辑　张　锴)