基于 CNN 和多注意力机制的 XSS 检测模型

关　慧[1,2],曹同洲[1]
(1. 沈阳化工大学 计算机科学与技术学院,辽宁 沈阳 110142;
2. 辽宁省化工过程工业智能化技术重点实验室,辽宁 沈阳 110142)

摘　要:为了解决普通深度学习模型存在的难以区分信息重要性差异,以及单一注意力机制存在的关注维度单一的问题,文中提出了一种基于卷积神经网络和多注意力机制的模型对 XSS 攻击进行检测。首先,将经过 word2vec 转换后的数据输入到卷积神经网络提取局部特征;然后,使用自注意力模块学习数据的长距离依赖关系,并加强模型对序列维度上重要特征的关注;接着,经过通道注意力模块从通道维度对不同的通道特征图加权;之后,将经注意力模块处理过的特征输入到池化层进行下采样处理,并使用 Dropout 层提高模型的泛化能力;最后,利用提取到的特征对样本进行分类。使用测试数据集对文中提出的模型进行实验,结果显示,该模型对 XSS 攻击的检测效果良好,准确率与 F1 值相比其他深度学习模型有一定程度提升。

关键词:卷积神经网络;多注意力机制;XSS 攻击;word2vec;自注意力;通道注意力
中图分类号:TP391　　**文献标识码**:A　　**文章编号**:1673-629X(2023)04-0175-07
doi:10.3969/j.issn.1673-629X.2023.04.026

XSS Detection Model Based on CNN and Multi-attention Mechanism

GUAN Hui[1,2],CAO Tong-zhou[1]
(1. School of Computer Science and Technology,Shenyang University of Chemical Technology,
Shenyang 110142,China;
2. Liaoning Province Key Laboratory of Industrial Intelligence Technology on Chemical Process,
Shenyang 110142,China)

Abstract:In order to solve the problems that ordinary deep learning models are difficult to distinguish the difference of the importance of information,and the attention dimension of single attention mechanism is single,a model based on convolutional neural network and multi-attention mechanism is proposed to detect XSS attacks. Firstly,the data converted by word2vec are input into convolutional neural network to extract local features. Then,the self attention module is used to learn the long-distance dependencies of the data and strengthen the model's attention on the important features in the sequence dimension. Next,through the channel attention module,different channel feature maps are weighted from the channel dimension. After that,the features processed by the attention modules are input into the pooling layer for down-sampling,and the Dropout layer is used to improve the generalization ability of the model. Finally,the extracted features are used to classify the samples. The test data set is used to test the proposed model,the results show that the model has a good detection effect on XSS attacks,the accuracy and F1 values are improved to a certain extent compared with other deep learning models.

Key words:convolutional neural network;multi-attention mechanism;XSS attacks;word2vec;self attention;channel attention

0　引　言

当前,随着互联网的快速发展,基于 Web 的应用也变得越来越普及。然而,互联网在带给人们便利的同时,也给不法分子提供了违法犯罪的机会,这严重危害到互联网用户的切身利益,给整个社会带来了极大的安全隐患。当下,跨站脚本(cross-site scripting,XSS)随着互联网的发展变得越来越普遍,攻击者可以通过 XSS 攻击进行网络钓鱼、会话劫持、盗取受害者的 cookie 等非法活动。根据国家信息安全漏洞库(CNNVD)统计,2020 年 4 月新增安全漏洞共 2 155

收稿日期:2022-06-06　　**修回日期**:2022-10-09
基金项目:辽宁省 2021 年度教育科学研究经费项目(LJKZ0434)
作者简介:关　慧(1976-),女(满),博士,副教授,CCF 会员(76281M),通讯作者,研究方向为软件演化、软件安全性以及语义处理等;曹同洲(1995-),男,硕士研究生,研究方向为深度学习、网络安全以及数据分析等。

个,从漏洞类型看,跨站脚本漏洞占比达 10.53%,仅次于缓冲区错误[1],因此,当下对于 XSS 攻击的检测与防范尤为重要。XSS 检测方法主要有静态分析方法、动态分析方法、机器学习方法等,由于深度学习具有自动提取特征、识别准确率高等优点,近些年人们开始把目光转向深度学习,并利用深度学习技术对 XSS 攻击进行检测。基于上述情况,该文研究并构建针对 XSS 攻击的深度学习模型。

1 相关工作

Mohammadi 等[2]提出了一种基于单元测试的方法自动检测 XSS 漏洞;曹黎波等[3]先提交合法向量以确定输出点的所在页面与具体位置,然后对输出点分类并使用不同类型的攻击向量,有效提高了检测效率;李洁等[4]在构造 DOM 模型与修改 Firefox Spider Monkey 脚本引擎的基础上,设计了一种动态的、基于 bytecode 的污点分析的检测算法以对 DOM-Based XSS 进行检测;Wang R 等[5]提出了一个检测 DOM-XSS 的框架 TT-XSS;谷家腾等[6]设计了一种基于动态分析的 XSS 漏洞检测模型,通过试探载荷测试及载荷单元的组合测试与单独测试判断是否存在 XSS 漏洞。

当下,随着机器学习的发展,网络安全领域开始引入机器学习来进行恶意攻击的检测与防范。Rathore 等[7]根据 SNSs 网页的特性与前人的经验,共提取了 25 个 XSS 特征,并使用 ADTree 等分类器进行 XSS 攻击检测;赵澄等[8]提出了一种基于 SVM 的 XSS 攻击检测方案;王培超等[9]利用贝叶斯网络对 XSS 攻击进行检测,并搜集恶意 IP 信息和恶意域名改善模型的准确性。

深度学习能够自动提取特征,这有效解决了人工提取特征存在的特征选取具有主观性、不全面等问题,因此,近些年深度学习开始被应用在 XSS 攻击检测等领域中,并逐渐成为这些领域的主流方法。Li Zhen 等[10]将深度学习引入到漏洞检测领域;Fang Y 等[11]使用 word2vec 模型将样本转换为由词向量构成的序列,然后利用长短时记忆网络(LSTM)自动提取特征并进行分类;Wu F 等[12]将 CNN、LSTM、CNN+LSTM 模型运用到漏洞检测领域;方忠庆[13]构建了 CNN+LSTM 模型对 XSS 攻击进行检测;程琪芩等[14]使用 BiLSTM 模型提取样本的特征;林雍博等[15]构建残差网络与 GRU 结合的模型检测 XSS 攻击。以上方法都取得了良好的效果,但是都没有解决普通深度学习模型难以区分数据中重要信息与非重要信息的问题。

自从 Bahdanau 等[16]提出注意力机制,它便引起学界的关注,并开始被广泛运用在各个领域。注意力机制能够帮助模型区分出重要特征与非重要特征,从而提升模型的整体性能。汪嘉伟等[17]利用卷积神经网络提取局部特征,并引入自注意力机制捕捉序列的长距离依赖特征;赵宇轩等[18]将注意力机制引入到深度学习模型,完成垃圾邮件的检测任务;陈莉媛等[19]在短文本情感分析的任务中引入自注意力机制,利用其捕获关键信息的特点提升模型性能;桂文明等[20]在歌声检测任务中应用点积自注意力模块使模型能够区分特征间的重要性差异;刘学平等[21]将通道注意力模块 SENet 结构嵌入到 YOLOV3 结构,以提升目标识别的查准率;康雁等[22]在文本情感分类任务中融合了 SENet 模块,提高了模型对深层次文本特征的抽取与分类能力;邱宁佳等[23]在文本主题识别任务中引入通道注意力模块 SENet,强化重要的通道信息以提升模型性能。

以上方法大多数是单独使用自注意力机制或通道注意力机制,虽然实验证明这些注意力机制的加入能够提升模型性能,但单独使用其中一种还是会存在关注维度单一的问题。自注意力模块以序列中各位置的词向量作为单位,根据相应位置上的单位与其他单位之间的相关性,确定该位置的最终结果,显然,它没有从通道的维度考虑各通道特征图的重要程度;而通道注意力模块则是从通道维度计算各特征图的注意力权重,并通过加权的方式确定各通道特征图的最终结果,但它并没有从序列的维度探究各词向量间的相关性。因此,该文根据上述分析提出了卷积神经网络与多注意力机制相结合的模型,并以此对 XSS 攻击进行检测。

2 相关理论知识

2.1 跨站脚本攻击

跨站脚本攻击主要分为 3 类[24]:反射型 XSS(reflected XSS)、存储型 XSS(stored XSS)及基于 DOM 的 XSS(DOM-based XSS)。反射型 XSS 是现在最普遍的一种 XSS,攻击者将恶意代码放在 URL 中,并诱使受害者点击,一旦受害者点击了该 URL,恶意脚本便会被服务器发送给受害者,在其被解析和执行后,攻击者便实现了对受害者的 XSS 攻击;存储型 XSS 是一种持久性的 XSS,与反射型 XSS 不同,存储型 XSS 是将恶意脚本存储在服务器端的数据库中,一旦有用户访问相应网站,攻击代码便会从服务器端数据库响应给受害者,该类型的 XSS 漏洞通常存在于留言板等能够进行交互的地方,并常被用于编写危害性更大的 XSS 蠕虫[25];基于 DOM 的 XSS 的请求不会被发送到服务器,而是在用户浏览器本地执行,因此,其威胁相较反射型 XSS 更大,防御难度也更高[4]。

2.2　自注意力

近些年,自注意力机制[26]被广泛运用在文本处理等领域。在处理文本类型数据时,人们希望模型在关注全局信息的同时,能更加关注序列中的重点信息,自注意力机制则可辅助模型达到这一目的。其总体框架如图 1 所示。自注意力机制的核心思想是通过计算单个词向量与序列中其他词向量的相似度来判定其在序列中的重要程度,它在训练时只关注自身信息,并且可以无视词向量之间的距离,在序列中的任意两个词向量之间建立联系,因此,自注意力机制具有提取长距离依赖特征的功能[19]。基于上述分析,该文在深度学习模型中加入自注意力模块以提高模型对长距离依赖特征的学习能力以及对序列中重点信息的关注能力。

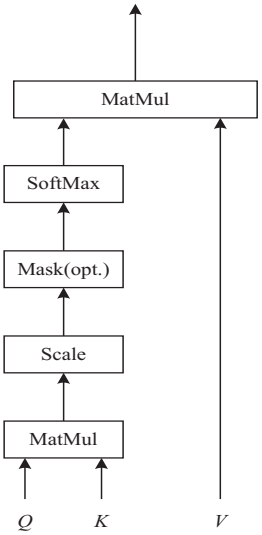

图 1　自注意力框架

2.3　通道注意力

通道注意力机制能够为各通道特征计算权值,常被用于辅助深度学习模型以提升其性能。Jie H 等[27]提出通道注意力模块 SENet(squeeze-and-ex-citation networks),这是一种最初应用在计算机视觉领域的轻量级模块,近些年在文本分类领域也开始被人们应用。SENet 的原理是通过加权的方式强化与分类相关性更强的通道特征图以提升模型的分类性能[28],其结构如图 2 所示。

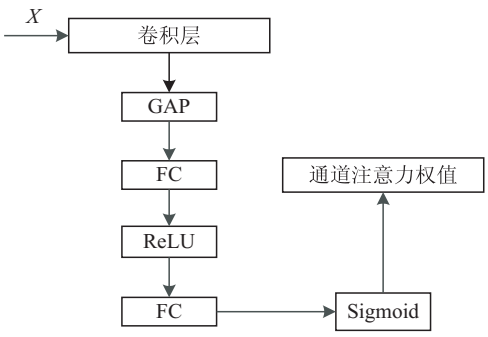

图 2　SENet 结构

SENet 模块首先通过全局平均池化层(GAP)获取各特征图的信息,然后依次经过全连接层(FC)、ReLU 激活函数、全连接层(FC),最后经由 Sigmoid 激活函数得到通道权值。

Woo S 等[29]提出了轻量级注意力模块 CBAM,该模块中通道注意力子模块的结构如图 3 所示,该子模块与 SENet 模块的不同之处在于它在获取通道信息时分别使用了全局平均池化层和全局最大池化层(GMP),全局平均池化与全局最大池化相配合能够生成更为合理的通道注意力权值。CBAM 模块的提出者对其中的通道注意力子模块进行了实验,并证明了同时使用全局平均池化和全局最大池化比单独使用一种全局池化的效果更好。因此,该文参考了 CBAM 中通道注意力子模块的结构构建适用于文本类型数据的通道注意力模块。

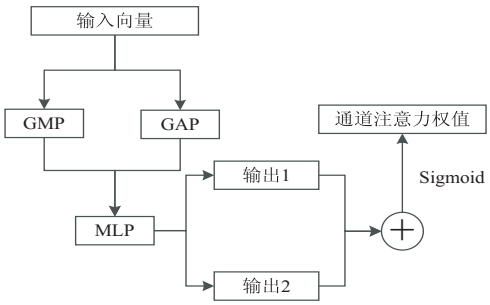

图 3　CBAM 通道注意力子模块结构

3　文中方法

3.1　深度学习模型设计思路

基于上一节的分析,该文提出了一种卷积神经网络与多注意力机制相结合的模型,它由两个卷积层、一个自注意力模块、通道注意力模块、最大池化层、Dropout 层、全局平均池化层和 softmax 分类器构成。该模型结构如图 4 所示。

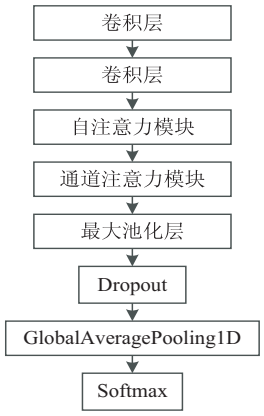

图 4　深度学习模型整体结构

模型的核心部分由卷积层、自注意力模块以及通道注意力模块构成。其中,卷积层能够对样本的局部特征进行提取,然而,卷积神经网络存在提取长距离依

赖特征的能力不足以及难以识别重要信息的缺陷,因此,在此基础上,加入了自注意力模块。自注意力模块能够在序列中的各个词向量之间建立联系,有效解决了卷积神经网络对长距离依赖特征提取能力不足的问题,并且能够使模型更加关注序列中的重要信息,自注意力机制的工作原理如图 5 所示。

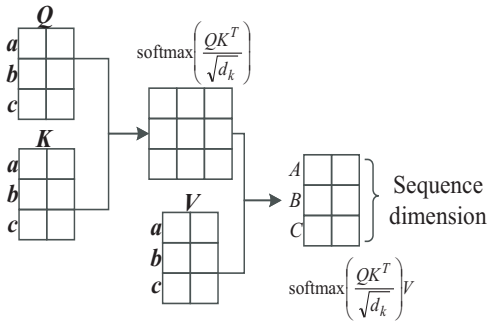

图 5 自注意力机制工作原理

图中的 $\boldsymbol{Q}$、$\boldsymbol{K}$、$\boldsymbol{V}$ 为输入向量矩阵通过线性变换映射而成的矩阵,词向量 $\boldsymbol{a}$、$\boldsymbol{b}$、$\boldsymbol{c}$ 沿着矩阵的序列维度(sequence dimension)分布。首先通过 $\boldsymbol{QK}^{\mathrm{T}}$ 得到序列中每个向量与其他向量之间的相似度矩阵,然后通过 $d_k^{1/2}$(d_k 是词向量的维度)对相似度矩阵进行缩放,并使用 softmax 函数对缩放后的相似度矩阵进行处理,得到注意力权重矩阵,最后使用该矩阵以加权求和的方式在序列维度上的各个位置生成新的特征向量 $\boldsymbol{A}$、$\boldsymbol{B}$、$\boldsymbol{C}$。其核心公式如下所示:

$$\mathrm{attention}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V}) = \mathrm{softmax}\left(\frac{\boldsymbol{QK}^{\mathrm{T}}}{\sqrt{d_k}}\right)\boldsymbol{V} \tag{1}$$

从自注意力机制的工作原理可以看出,自注意力机制能够通过注意力权重矩阵在序列维度上各个位置得到新的向量,但它并没有从通道维度分析各通道特征图之间存在的重要性差异。为了解决该问题,引入通道注意力模块。通道注意力的作用原理如图 6 所示。

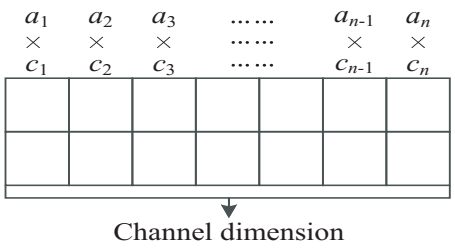

图 6 通道注意力作用原理

通道注意力模块接收由 n 个通道特征图构成的输入 $c = \{c_1, c_2, \cdots, c_n\}$,各个通道特征图沿着通道维度(channel dimension)依次分布,通道注意力模块可以根据输入 c 分析出这 n 个通道的注意力权重 $a_1, a_2, \cdots, a_n$,并利用它们为相应的通道特征图加权得到新的特征 $C = \{C_1, C_2, \cdots, C_n\}$,其加权公式如下所示:

$$C_i = \sum_{i=1}^{n} c_i \cdot a_i \tag{2}$$

在注意力模块完成对特征图的处理后,便将优化后的特征送入最大池化层进行下采样,与此同时加入 Dropout 层提高模型的泛化能力,最后经过全局平均池化层和 softmax 分类器对样本进行分类。

3.2 数据预处理

在实验开始前,需要对数据集中的数据进行预处理。由于攻击者在构造 XSS 攻击向量时会通过恶意混淆的方式来躲避检测,因此,首先需要对数据集中的样本进行解码操作,以提高样本数据的可读性;其次,将样本中的数字用“0”替换,并将超链接用“http://u”替换;最后进行分词操作,从而将样本分割为由单词组成的序列。

3.3 词向量转换

完成预处理的工作后,就可以利用词向量模型 word2vec 将原数据转换为由词向量构成的语句序列,并将其作为深度学习模型的标准输入。

3.4 特征提取与分类

完成词向量转换的工作后,就可以利用构建的深度学习模型提取样本的特征并对样本进行分类。在深度学习模型中,卷积神经网络负责提取样本的局部特征,自注意力模块负责提高模型对长距离依赖特征的学习能力以及对重要序列特征的关注能力,通道注意力模块则负责加强模型对重要通道特征的关注度。提取完特征后,经由最大池化层以及 Drouout 层进行下采样及泛化处理,并通过全局平均池化层及分类器完成样本的分类工作。

3.5 算法设计

在训练模型之前需要对训练样本以及测试样本进行预处理及词向量转换等操作以得到适应深度学习模型的标准训练集 Train_set 以及标准测试集 Test_set。文中模型的算法设计如下所示:

输入:训练集 Train_set 与测试集 Test_set。

输出:经分类器预测得到的结果。

构建深度学习模型并初始化参数。

训练模块:

Fori in epochs:

将训练集 Train_set 的数据送入输入层得到 result1;

将 result1 送入卷积神经网络提取特征得到 result2;

将 result2 送入自注意力模块进行处理得到 result3;

将 result3 送入通道注意力模块,从通道维度对特征图加权得到 result4;

将 result4 送入最大池化层进行下采样,然后再利用 Dropout 层进行泛化得到 result5;

将 result5 送入全局平均池化层,然后输入到 soft-max 分类器中进行预测得到分类结果 result;

将分类结果与实际类别进行对比,并根据误差进行反向传

播以调整参数;

更新深度学习模型各层的参数;

end for;

测试模块:

将测试集 Test_set 中的数据送入训练好的模型中进行预测,并将预测结果与实际类别进行对比,判定模型的检测性能。

4　实验及分析

将攻击样本设置为正样本,将正常样本设置为负样本。为了验证文中所提模型的性能,使用准确率(accuracy)、精确率(precision)、召回率(recall)、和 F1 值作为模型的评价指标。其中,准确率表示被正确预测的样本数占总样本数的比例;精确率表示被正确预测的正样本数占所有被预测为正样本的样本数的比例;召回率表示被正确预测的正样本数占所有正样本的样本数的比例;F1 值是综合精确率和召回率的评价指标,它们的公式如下所示:

$$\text{accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

$$\text{precision} = \frac{TP}{TP + FP} \tag{4}$$

$$\text{recall} = \frac{TP}{TP + FN} \tag{5}$$

$$F1 = \frac{2 \times \text{precision} \times \text{recall}}{\text{precision} + \text{recall}} \tag{6}$$

其中,TN 是指被正确预测的负样本数量,FP 是被预测为正样本的负样本数量,FN 是被预测为负样本的正样本数量,TP 是被正确预测的正样本数量。

4.1　实验准备

实验的硬件环境为:处理器 Intel(R) Core(TM) i5-10300H、内存 8 GB;软件环境为:Win10(64 位)操作系统、Python3.5、TensorFlow1.8.0、Keras2.2.0。

实验使用从 Github 收集到的 24 687 个 XSS 攻击样本以及 24 818 个正常样本,两类样本的总数为 49 505。按照 7∶3 的比例将样本划分为训练集与测试集。样本的分布情况如表 1 所示。

表 1　样本分布情况

样本类别	训练集	测试集	总计样本
攻击样本	17 242	7 445	24 687
正常样本	17 411	7 407	24 818

由于深度学习模型要求所有输入数据的序列长度和词向量维度保持一致,因此,该文需要统一输入数据的形状。为了确定输入数据的序列长度,对分词后样本序列长度的分布情况进行了统计,结果显示,序列长度小于等于 100 的样本数量超过总样本数量的 99%,因此将所有输入样本的序列长度统一为 100,对于长度超过 100 的样本进行截断处理,并对长度小于 100 的样本使用零向量进行填补。为了确定 epoch 值,对模型的性能与 epoch 之间的关系进行了探究,模型在测试集的准确率曲线及 F1 值曲线如图 7 和图 8 所示。从图中可以看出,当训练轮数到达 3 的时候,模型的准确率与 F1 值都达到了高位水平,当继续增加训练轮数时可以发现,模型的性能并没有明显的提升,曲线趋向平稳,因此,将 epoch 设置为 3。

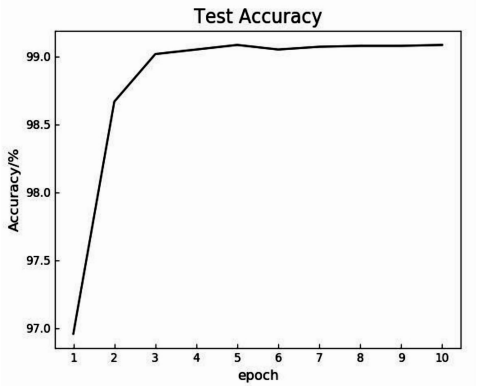

图 7　模型测试集准确率曲线

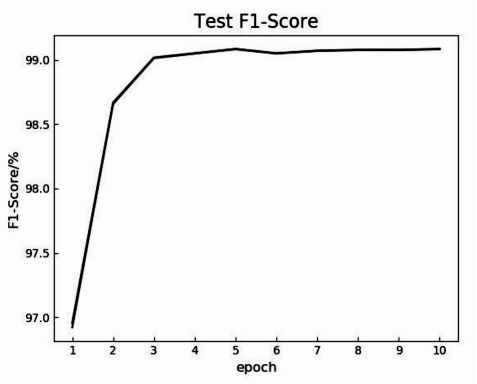

图 8　模型测试集 F1 值曲线

实验参数如表 2 所示。

表 2　实验参数

参数	设置
词向量模型	CBOW
词向量维度	128
序列长度	100
batch_size	500
分类器	softmax
epoch	3
卷积核尺寸	3
卷积核数量	64

4.2　实验数据与分析

在实验训练阶段与测试阶段所用的数据集均为经过预处理及词向量转换处理的标准数据集。首先使用标准训练集训练文中提出的模型,并在该模型训练完成后将其应用在标准测试集中。为了探究注意力机制对模型性能的影响,进行了消融实验,对文中提出的模

型进行了拆解。实验的结果如表 3 所示,其中基准模型为在文中模型基础上去掉所有注意力模块的模型,方法 1 为基准模型加通道注意力模块的模型,方法 2 为基准模型加自注意力模块的模型。从实验结果可以看出,加入通道注意力模块或者加入自注意力模块都能提高卷积神经网络的性能,而文中模型的准确率与 F1 值分别为 99.02% 与 99.01%,明显高于其他 3 个对照组。与基准模型相比,文中模型的准确率提升了 1.07 百分点,召回率提升了 2.09 百分点,F1 值提升了 1.09 百分点,其相对于基准模型的提升幅度大于单独使用一种注意力机制的方法 1 和方法 2。

表 3 消融实验结果 %

检测模型	准确率	精确率	召回率	F1 值
文中方法	99.02	99.75	98.28	99.01
基准模型	97.95	99.72	96.19	97.92
方法 1	98.71	99.47	97.94	98.70
方法 2	98.84	99.74	97.94	98.83

为了继续验证该模型的性能,还将其与深度学习中常用的 RNN 模型和 LSTM 模型进行了对比。此外,由于数据集及预处理等方面存在差异,根据文献[13]、文献[30]、文献[14]中所提供的信息构建了相应的 CNN+LSTM、LSTM-Attention、BiLSTM 模型进行实验,因为未明确文献[30]中 L-STM 的 units 参数,所以,在进行对照实验时将该参数设置为 128。对照实验依旧使用表 3 实验所用的标准数据集,其中,对照实验的 batch_size、epoch 均依照表 3 设置。模型主要性能指标的对比结果如表 4 所示。

表 4 文中模型与其他深度学习模型对比结果 %

检测方法	准确率	精确率	召回率	F1 值
文中方法	99.02	99.75	98.28	99.01
RNN	93.53	96.43	90.44	93.34
LSTM	98.22	99.14	97.30	98.21
CNN+LSTM	98.69	99.52	97.85	98.68
LSTM-Attention	98.65	98.97	98.33	98.65
BiLSTM	98.62	99.37	97.86	98.61

从表 4 可以看出,RNN 模型、LSTM 模型、CNN+LSTM 模型、LSTM-Attention 模型、BiLSTM 模型的准确率分别为 93.53%、98.22%、98.69%、98.65%、98.62%,F1 值分别为 93.34%、98.21%、98.68%、98.65%、98.61%。相比 RNN 模型,文中方法在准确率与 F1 值方面均提升了超过 5 百分点,召回率提升了接近 8 百分点,除此之外,其他几个对照模型均取得了不错的检测效果,但是,相比之下文中提出的模型在准确率、精确率与 F1 值这些指标上都表现得更加优秀。因此,通过对照实验可以得出结论,文中提出的模型在 XSS 攻击检测方面有着良好的表现。

5 结束语

如今,随着 Web 应用的普及,XSS 攻击的威胁也变得越来越大,如何有效地检测 XSS 攻击成为当前一项重要的任务。针对这一情况,构建了基于卷积神经网络和多注意力机制的 XSS 攻击检测模型。在卷积神经网络的基础上,引入了自注意力模块及通道注意力模块,从序列与通道两个维度对特征进行优化处理。首先,对输入数据进行解码、替换、分词等预处理工作;然后,使用 word2vec 模型进行词向量的转换工作,并利用提出的模型进行特征提取等工作;最后,根据提取到的特征进行分类。为了验证文中所提模型的性能,进行了消融实验,并将该模型与其他深度学习模型进行了对比。下一步,可以继续收集样本构建数据集以观察该模型的效果,并继续尝试改进模型,以提高检测的性能,应对日益复杂的 XSS 攻击。

参考文献:

[1] 国家信息安全漏洞通报[J]. 中国信息安全,2020(5):91-93.

[2] MOHAMMADI M,CHU B,LIPFORD H R. Detecting cross-site scripting vulnerabilities through automated unit testing[C]//2017 IEEE international conference on software quality,reliability and security(QR-S). Prague:IEEE,2017:364-373.

[3] 曹黎波,曹天杰. 基于动态测试的 XSS 漏洞检测方法研究[J]. 计算机应用与软件,2015,32(8):272-275.

[4] 李 洁,俞 研,吴家顺. 基于动态污点分析的 DOM XSS 漏洞检测算法[J]. 计算机应用,2016,36(5):1246-1249.

[5] WANG R, XU G, ZENG X, et al. TT-XSS:a noveltaint tracking based dynamic detection framework forDOM Cross-Site Scripting[J]. Journal of Parallel and Distributed Computing,2018,118:100-106.

[6] 谷家腾,辛 阳. 基于动态分析的 XSS 漏洞检测模型[J]. 计算机工程,2018,44(10):34-41.

[7] RATHORE S,SHARMA P K,PARK J H. XSSClas-sifier:an efficient XSS attack detection approach based on machine learning classifier on SNSs[J]. Journal of Information Processing Systems,2017,13(4):1014-1028.

[8] 赵 澄,陈君新,姚明海. 基于 SVM 分类器的 XSS 攻击检测技术[J]. 计算机科学,2018,45(S2):356-360.

[9] 王培超,周 鋆,朱 承,等. 基于贝叶斯网络的 XSS 攻击检测方法[J]. 中国科学技术大学学报,2019,49(2):166-172.

[10] LI Z,ZOU D Q,XU S H,et al. VulDeePecker:a deep learning-based system for vulnerability detection[C]//Network and distributed systems security (NDSS) symposium. San Diego:Internet Society,2018:1-15.

[11] FANG Y, LI Y, LIU L, et al. DeepXSS: cross site scripting detection based on deep learning[C]//Proceedings of the 2018 international conference on computing and artificial intelligence. New York: ACM, 2018: 47-51.
[12] WU F, WANG J G, LIU J Q, et al. Vulnerability detection with deep learning[C]//2017 3rd IEEEinternational conference on computer and communications (I-CCC). Chengdu: IEEE, 2017: 1298-1302.
[13] 方忠庆. 基于深度学习的跨站脚本攻击检测研究[D]. 长沙:湖南大学, 2018.
[14] 程琪芩, 万　良. BiLSTM 在跨站脚本检测中的应用研究[J]. 计算机科学与探索, 2020, 14(8): 1338-1347.
[15] 林雍博, 凌　捷. 基于残差网络和 GRU 的 XSS 攻击检测方法[J]. 计算机工程与应用, 2022, 58(10): 101-107.
[16] BAHDANAU D, CHO K, BENGIO Y. Neural machine translation by jointly learning to align and translate[J]. arXiv: 1409.0473, 2014.
[17] 汪嘉伟, 杨煦晨, 琚生根, 等. 基于卷积神经网络和自注意力机制的文本分类模型[J]. 四川大学学报: 自然科学版, 2020, 57(3): 469-475.
[18] 赵宇轩, 胡怀湘. 基于 BiGRU-Attention-CNN 模型的垃圾邮件检测方法[J]. 计算机与现代化, 2021(4): 122-126.
[19] 陈莉媛, 毋　涛. 融合主题模型与自注意力机制的短文本情感分析方法[J]. 国外电子测量技术, 2021, 40(11): 18-23.
[20] 桂文明, 曾　岳, 臧　娴. 基于点积自注意力卷积神经网络的歌声检测[J]. 信号处理, 2021, 37(10): 1899-1906.
[21] 刘学平, 李玓乾, 刘　励, 等. 嵌入 SENet 结构的改进 YOLO-V3 目标识别算法[J]. 计算机工程, 2019, 45(11): 243-248.
[22] 康　雁, 李　浩, 梁文韬, 等. 针对文本情感分类任务的 textSE-ResNeXt 集成模型[J]. 计算机工程与应用, 2020, 56(7): 205-209.
[23] 邱宁佳, 杨长庚, 王　鹏, 等. 改进卷积神经网络的文本主题识别算法研究[J]. 计算机工程与应用, 2022, 58(2): 161-168.
[24] NAGARJUN P M D, AHAMAD S S. Cross-site scripting research: a review[J]. International Journal of Advanced Computer Science and Applications, 2020, 11(4): 626-632.
[25] 孙　伟, 张凯寓, 薛临风, 等. XSS 漏洞研究综述[J]. 信息安全研究, 2016, 2(12): 1068-1079.
[26] VASWANI A, SHAZEER N, PARMAR N, et al. Attention is all you need[C]//Advances in neural information processing systems. Long Beach: NIPS, 2017: 5998-6008.
[27] HU J, SHEN L, SUN G. Squeeze-and-excitation networks[C]//Proceedings of 2018 IEEE/CVF conference on computer vision and pattern recognition. Salt Lake City: IEEE, 2018: 7132-7141.
[28] 肖　禹, 王景中, 王宝成. 基于深度学习的中文文本分类方法[J]. 计算机工程与设计, 2021, 42(4): 1014-1019.
[29] WOO S, PARK J, LEE J Y, et al. CBAM: convolutio-nal block attention module[C]//Proceedings of the European conference on computer vision (ECCV). Munich: Springer, 2018: 3-19.
[30] LI L, CHEN M, HE C W, et al. XSS detection technology based on LSTM-attention[C]//2020 5th international conference on control, robotics and cybernetics (CRC). Wuhan: IEEE, 2020: 175-180.

(上接第 174 页)

[J]. 计算机应用, 2021, 41(8): 2265-2272.
[14] QU Chiwen, HE Wei, PENG Xiangni, et al. Harris hawks optimization with information exchange[J]. Applied Mathematical Modelling, 2020, 84: 52-75.
[15] 张九龙, 王晓峰, 芦　磊, 等. 若干新型智能优化算法对比分析研究[J]. 计算机科学与探索, 2022, 16(1): 88-105.
[16] 童怀水, 吴小俊. 一种基于 PCNN 的多聚焦图像融合改进算法[J]. 计算机工程, 2012, 38(24): 220-224.
[17] 张佳星, 褚晓凯, 屈俊峰. 多模态多目标进化算法研究综述[J]. 现代计算机, 2021, 27(35): 12-19.
[18] 李美丽, 李言俊, 王红梅, 等. 基于自适应脉冲耦合神经网络图像融合新算法[J]. 光电子. 激光, 2010, 21(5): 779-782.
[19] WANG Nianyi, WANG Weilan. An image fusion method based on wavelet and dual-channel pulse coupled neural network[C]//Proceedings of 2015 IEEE international conference on progress in informatics and computing (PIC 2015 V1). Nanjing: IEEE, 2015: 301-305.
[20] 王　玉, 王明泉. 基于小波变换的红外与可见光图像融合技术研究[J]. 红外, 2013, 34(3): 12-14.
[21] CHOI. Development of building 3D spatial information extracting system using HSI color model[J]. Journal of Korean Society for Geospatial Information System, 2013, 21(4): 151-159.