A CNN-LSTM Hybrid Model for Encrypted Website Fingerprinting

1st Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

2nd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

3rd Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

4th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

5th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

6th Given Name Surname
dept. name of organization (of Aff.)
name of organization (of Aff.)
City, Country
email address or ORCID

***Abstract*—**在网络安全与隐私保护领域，网站指纹识别技术至关重要，其核心目标是依据网络流量特征识别加密网络环境下用户访问的网站。然而，当前主流方法存在应用场景受限、适用性欠佳以及特征选取单一等问题。为此，本文提出一种创新的基于深度学习的加密网站指纹识别方法。首先，精心设计一种全新的原始数据包预处理方式，基于直接抓包所得的原始 **PCAP** 文件，构建包含时间戳、数据包长度和方向的层次化时空特征序列，该方法不依赖特定协议的特定单元，极大提升了通用性。接着，搭建卷积神经网络（**CNN**）与长短期记忆网络（**LSTM**）融合的深度学习模型，并引入注意力机制，深度挖掘数据中的时空特征。同时，深入探索不同激活函数、模型参数及优化算法，显著提高模型的识别准确率与泛化能力。实验结果表明，在洋葱匿名网络环境下，即使不依赖其数据单元，该方法的网站指纹识别准确率也表现卓越；在虚拟私人网络场景中，相较于主流机器学习方法，同样取得了更高的准确率，有力验证了方法的有效性和广泛适用性。在网络安全与隐私保护领域，网站指纹识别技术至关重要，其核心目标是依据网络流量特征识别加密网络环境下用户访问的网站。然而，当前主流方法存在应用场景受限、适用性欠佳以及特征选取单一等问题。为此，本文提出一种创新的基于深度学习的加密网站指纹识别方法。首先，精心设计一种全新的原始数据包预处理方式，基于直接抓包所得的原始 **PCAP** 文件，构建包含时间戳、数据包长度和方向的层次化时空特征序列，该方法不依赖特定协议的特定单元，极大提升了通用性。接着，搭建卷积神经网络（**CNN**）与长短期记忆网络（**LSTM**）融合的深度学习模型，并引入注意力机制，深度挖掘数据中的时空特征。同时，深入探索不同激活函数、模型参数及优化算法，显著提高模型的识别准确率与泛化能力。实验结果表明，在洋葱匿名网络环境下，即使不依赖其数据单元，该方法的网站指纹识别准确率也表现卓越；在虚拟私人网络场景中，相较于主流机器学习方法，同样取得了更高的准确率，有力验证了方法的有效性和广泛适用性。

***Index Terms*—**深度学习**;**加密流量**;**网站指纹识别**;**洋葱网络**;**虚拟私人网络

I. Introduction

With the rapid development of the Internet and its deep penetration into social life, network technology has become an indispensable part of people's daily work and life. In the early days of the Internet, users often browsed web pages, sent and received emails, or communicated without sufficient security measures, which inevitably brought significant security risks. To better protect personal privacy, numerous privacy - enhancing technologies (PETs) have emerged, aiming to strengthen the privacy protection ability in the network environment. According to the latest Google Transparency Report, 95% of Google's products and services have achieved encryption functions, and this proportion is still rising. Besides encrypting network traffic, researchers have developed various PETs, such as anonymous networks, encrypted proxies, and tunneling technologies, including the onion router (TOR) and virtual private network (VPN). These technologies have greatly improved the security of users' network usage.

However, the emergence of website fingerprinting technology poses a great challenge to this security. This technology can infer and identify users' browsing privacy by leveraging the website fingerprint features exposed during web browsing. Studying deep - learning - based encrypted website fingerprinting methods is of great significance. It helps to reveal the information in encrypted traffic that can still be used to violate privacy, thereby promoting the development of more advanced privacy - protection technologies and protocols. In recent years, with the development of various protocols, traffic is continuously encrypted during transmission, which requires researchers to deeply mine traffic features. Deep learning technology, capable of automatically extracting features through neural networks, not only reduces human resource input but also significantly improves the accuracy of the identification process. Thus, it has gained the favor of many scholars. Many studies have been conducted on applying deep learning to website fingerprinting, resulting in numerous achievements. However, there are still some limitations in existing methods, such as limited application scenarios and single - feature selection. This paper focuses on addressing these issues and proposes a novel deep - learning - based encrypted website fingerprinting method.

Fig. 1.

II. FIGURE

III. TABLE

TABLE I
CIFAR - 10

AlexNet	22	61M	83.6%	
VGG16	45	138M	89.4%	
ResNet-50	60	25.6M	91.7%	

IV.

TABLE II
不同卷积神经网络模型在 CIFAR - 10 数据集上的实验结果

模型名称	训练时间	参数量	测试准确率	边缘部署可行性
AlexNet	22 分钟	61M	83.6%	高
VGG16	45 分钟	138M	89.4%	中
ResNet-50	60 分钟	25.6M	91.7%	低

A. 准确率方面

从表 II 中的测试准确率数据可知，ResNet-50 表现最优，其准确率达到了 91.7%，明显高于 AlexNet 的 83.6% 和 VGG16 的 89.4%。这表明 ResNet-50 的网络结构能够更有效地从 CIFAR-10 图像数据集中学习特征，从而实现更精准的分类。

B. 边缘设备部署方面

由表 II 数据可得，AlexNet 最适合部署到资源受限的边缘设备上。它的参数量为 61M，训练时间仅 22 分钟，且边缘部署可行性评价为”高”。相对较小的参数量和较短的训练时间意味着它对边缘设备的计算资源和存储资源需求较低，能够在资源有限的情况下较为高效地运行。

C. 性能与部署可行性平衡方面

从表 II 中各项数据综合分析，VGG16 在性能与部署可行性之间取得了较好的平衡。虽然其测试准确率（89.4%）略低于 ResNet-50，但远高于 AlexNet，同时它的边缘部署可行性为”中”，相较于 ResNet-50 的”低”可行性，在保证一定准确率的前提下，更易于部署到实际环境中。

D.

CNNLSTM

$$\mathbf{H}_{cnn} = f_{cnn}(\mathbf{X}; \mathbf{W}_{cnn}) \tag{1}$$

$$\mathbf{H}_{lstm} = f_{lstm}(\mathbf{H}_{cnn}; \mathbf{W}_{lstm}) \tag{2}$$

$$\mathbf{A} = \text{Attention}(\mathbf{H}_{lstm}) \tag{3}$$

$$\hat{y} = \text{softmax}(\mathbf{W}_o \mathbf{A} + \mathbf{b}_o) \tag{4}$$

XWA