基于机器学习模型的系统日志分析

陈佳美，徐根宏，和蔡正勋
(通讯作者: 陈佳梅)

国立中山大学信息管理系 804高雄市鼓山区连海路70号
(电子邮件: cchen@mail.nsysu.edu.tw)
(2020年2月7日收到；2020年6月8日修订并接受)

摘要

网络攻击成为政府、企业和人民最关心的威胁之一。有效的事件调查对于确定攻击的根本原因至关重要，这需要分析审计日志的专业知识。系统日志是了解系统状态的重要审计线索，对于分析安全漏洞中的异常情况非常有用。然而，由于日志的多样性和海量性，日志分析需要专业的领域知识，以及大量的人力和计算资源。为了使事件调查更容易进行，本研究提出了一种基于机器学习的系统日志分析方法，可以自动识别可疑的事件活动。实验结果表明，所提出的基于神经网络的方法可以有效地识别恶意软件，其精度为95.5%，并优于SVM。

关键词异常检测；大数据分析；机器学习

1 简介

电子商务的爆炸性扩张为企业提供了前所未有的机会，以扩大他们的市场。 政府、企业和人们严重依赖无缝的泛在计算服务，将有价值的机密数据放在互联网和云端上。然而，这些便利的服务也伴随着网络攻击的相应增加，并造成了严重的损害和经济损失。这些年来，网络犯罪在全球范围内不断增加。不仅金融公司遭受网络攻击的严重损失，而且高科技公司、政府和学术机构也经历了严重的数据泄露。

攻击者试图利用不同层次的漏洞，如最常见的应用技术或逻辑攻击[12]，并渗透到目标系统。为了检测可疑的行为，系统会记录重要的执行的活动。在操作系统、进程、网络或应用程序的执行过程中记录事件的过程被称为日志，它产生的日志文件由与系统、网络或应用程序中发生的事件相关的有用信息组成[11]，在它被破坏的情况下对分析异常情况非常有用。事件调查面临着巨大的数据收集和数据分析，这消耗了系统管理员或事件调查员大量的时间来从大量的系统日志中发现可疑的行为。我们需要一种有效的系统日志分析方法来识别可疑的事件。

有两种常见的攻击检测方法：误用检测和异常检测。误用检测是一种基于规则的方法，包含入侵模式的特征，在识别已知攻击方面很有效，但对新攻击或已知攻击的变体通常表现不佳。异常检测方法对正常或异常行为进行剖析，并将各自剖析中的偏差或相似性应用于异常检测，它可能采用统计、机器学习或数据挖掘技术来训练检测模型。

大多数研究分析了网络流量或来自防御系统的警报，但分析系统日志的问题尚未在文献中得到充分探讨。在现实世界的案例中，攻击者规避了防御机制并将恶意软件植入目标系统，而防御系统却未能发现它们。

为了减少攻击造成的损失，有效地识别攻击是非常关键的时间。审计跟踪的信息量越大，去检测模型可以更有效地建立识别攻击。系统日志提供了关于在系统上进行的活动的信息数据，对于检测可疑事件很有用。然而，分析审计跟踪是劳动密集型的，大多数组织缺乏安全专业人员以及资源来及时和有效地执行这项任务。我们需要一种自动和高效的系统日志分析方法。

超过78%的系统是基于Windows的[19]，而且在

此外，Windows已经成为攻击者最喜欢的黑客平台[20]。Sysmon（系统监视器）提供的事件日志是全面的，对识别基于Window系统的可疑活动很有用。因此，本研究的重点是分析系统日志和识别基于Windows系统的异常事件。

神经网络（NNs）是目前最流行的机器学习算法之一。随着时间的推移，已经决定性地证明了NNs在准确性和速度上优于其他算法[13]。循环神经网络（RNNs）是NNs的一个变种，可以有效地处理时间序列数据，如系统日志。为了使系统日志分析和异常检测能够为人员不足的组织所使用，本研究提出了一种基于RNN的系统日志分析方法，以自动识别可疑的行为。

本文的其余部分结构如下。第2节简要回顾了关于攻击检测和日志分析的相关研究，以及对Windows系统日志的背景研究；第3节阐述了所提出的检测方法；第4节介绍了性能评估，然后是结论和未来工作。

2 相关工作

Raftopoulos和Dimitropoulos[16]断言，来自入侵检测系统的警报经常产生大量的假阳性。 他们提出了一种减少警报的方法，该方法采用基于熵的信息理论标准来寻找重复出现的警报。Zargar等人[23]提出了一个用于分布式计算环境的入侵检测框架，其中服务提供商合作应对攻击。Lo[9]提出了一个框架，通过与其他入侵检测系统交换警报信息来检测攻击。需要一个全面的信任管理方案来支持服务提供者之间的信任关系。

Liu等人[18]提出了一个警报关联模型，用于构建攻击场景，需要给定的攻击图和签名规则来关联安全事件。Siraj等人[1]提出了一个攻击预测的框架，它包括以下几个部分：警报规范化、还原、优先级、攻击场景构建和预测。为了获得有效的检测结果，Amini等人[2]提出了一种结合多种分类器的检测方法：神经网络工作、模糊聚类和堆叠组合方法。实验结果表明，所提出的多分类器方法比单一分类器表现更好。

在攻击检测方面，已经有大量的研究做出了贡献。已经探索了包括数据挖掘、有限状态机等在内的各种方法，以提出识别异常情况的有效方法。

Serketzis等人[17]提出了一个日志管理系统，该系统收集来自网络设备的审计日志。严格的设备、操作系统和应用程序。用户可以通过搜索功能来发现可疑的事件。Dwyer和Truta[6]提出了一种基于统计学的方法，利用标准差来识别Windows事件日志数据中的异常情况。计算任何服务器或用户在一天中任何时间的特定类型的事件的平均数和标准差；如果一个事件超出了标准差，则确定为异常事件。结果显示，拟议的解决方案将需要审查的日志数量降低到一个可行的数量。

Windows事件日志是Windows操作系统存储的系统、安全和应用程序通知的详细记录，对于识别系统故障和攻击非常有用。它可以大致分为两个层次的日志：操作系统和应用程序。两者都可以利用事件日志来记录重要事件。Windows系统日志记录软件安装、安全管理、初始启动时的系统设置操作以及问题或错误；另一个层次是服务日志，记录与应用程序相关的事件。为了识别系统中的可疑事件，本研究的重点是分析Windows系统日志。

系统监控器（Sysmon）是一个Windows系统服务，用于监控并将系统活动记录到Windows事件日志中，这些事件日志提供关于程序创建、网络连接和文件创建时间变化的详细信息。Sysmon不提供事件分析，但官方文件声称，通过收集和分析事件日志，可以发现异常的活动。

最近，各种机器学习算法在深度学习的基础上被开发出来，在分类和聚类方面表现出显著的能力。其中，有监督的机器学习算法已被应用于异常检测。分类任务包括根据从标记的训练数据中学习到的信息将数据分成不同的类别，其中训练数据集中的每个实例都包含一个 "目标值"（即类标签）和一些 "属性"（*即*特征或观察变量）。监督学习算法的目标是产生一个模型（基于训练数据），该模型可以对测试数据的目标值进行分类或预测，只需给出测试数据的属性。

监督学习机器模型，SVM（支持向量机），被广泛用于分类中。给定一个实例-标签对（xi; yi）的训练集，SVM模型就是要找到一个具有最大余量的线性超平面来分离数据。有四种基本的核函数被用于建立超平面模型。线性、多项式、径向基函数（RBF）和sigmoid。一般来说，RBF核是一个合理的选择。这个核将样本非线性地映射到一个高维空间，所以它可以处理类标签和属性之间的非线性关系的情况。线性核函数是RBF的一个特例，而sigmoid核在某些参数上表现得像RBF。

Zidi等人[24]采用SVM分类模型来研究。

识别无线传感器网络中的故障，并声称故障检测必须是精确的，以避免负面警报，并迅速限制损失。与其他算法相比，他们的研究表明，SVM是高效的。Wang等人[22]提出了一个基于SVM的高效入侵检测框架，并得出了类似的结论，即SVM在准确性、检测率、误报率和训练速度方面比现有的方法取得了更好的性能。 Anton等人[3]将SVM应用于工业环境的网络异常检测，实验结果显示SVM表现良好。

神经网络是最流行的机器学习算法之一。卷积神经网络（CNN）在模式识别和图像分类方面表现良好，但不适合有时间序列的数据。神经网络模型已经被应用于异常检测。Radford等人[15]表明，RNN可以代表网络上的通信序列并发现异常的网络流量。Prasse等人[14]分析了HTTPS网络流量，采用自然语言模型从域名中提取特征，并提出了一种基于LSTM的检测方法，其中LSTM（长短期记忆）是一种处理时间序列数据的RNN模型。他们的实验结果表明，LSTM分类模型的性能优于随机森林模型。 Kim和Ho[8]采用CNN来提取空间特征和LSTM的时间特征，并提出了一个用于检测网络流量异常的神经网络。

3 系统设计

根据文献回顾，攻击者可能会利用他们的攻击来规避检测机制。Sysmon日志提供了关于在系统上执行的行动的详细信息，包括网络连接、运行的进程、注册表文件和文件系统。通过分析审计日志的信息细节可以提高检测性能。RNN模型适用于分析像这样的审计日志的时间序列数据。本研究提出了一种基于RNN的日志分析方法，对可疑事件进行自动分类，其系统模型如图1所示。这项研究通过在受控环境中模拟攻击来收集恶意软件的行为，并从校园网络中收集正常的用户行为。这两部分标注的数据都是经过人工验证的。

我们的初步研究发现，大多数攻击包含以下四种类型的行为：进程、文件访问、注册表和网络访问，而且都可以被系统日志捕获。日志记录是有信息量的，但大多数是良性的。因此，预处理模块从日志文件中提取安全相关的事件记录，以减少以下步骤的处理时间，其中提取的安全相关的事件记录代表一个特定进程的行为。拟议的RNN模型从收集到的良性用户和恶意软件的标记数据中学习对不当行为进行分类。下面将详细解释所提出的方法。

3.1 与安全有关的事件

为了识别一个流程的错误行为，应该捕捉和分析流程的行为。在本研究中，进程行为被划定为系统日志所捕获的事件序列。根据我们的初步研究，从Sysmon事件日志中选择了上述四种与安全相关的事件，以确定系统的关键活动和状态变化。由于事件属性提供了事件的详细信息，因此选择了关键的事件属性来改进对所执行的行动的描述。总之，通过描述所执行的事件序列中的过程行为与相关的事件属性，所提出的异常检测方法绘制了系统的状态变化并发现了异常行为。下面将解释所提出的方法中选择的安全相关的事件和属性。

过程事件

一个二进制图像文件需要加载到内存中，以便能够运行这个程序，而一些恶意软件将其可执行文件注入另一个合法进程或杀死一个进程。这种行为可以被进程事件所捕获。根据上述注入异常情况和关于恶意软件不当行为的文献回顾，选定的关键进程事件/行为包括创建一个进程、终止一个进程、加载图像、创建一个远程线程和访问一个进程，其中表1概述了选定的进程事件和属性。

文件访问事件

恶意软件出于各种目的访问文件系统。下装器或投放器可能会下载额外的恶意软件或有效载荷，以执行进一步的攻击；勒索软件访问并加密文件和文档；一些恶意软件窃取并发送机密信息。文件访问事件记录了文件系统的访问行为。选定的关键文件访问事件包括改变文件创建时间、访问文件、创建文件和创建文件哈希，其中表2总结了选定的文件访问事件和属性。

登记处活动

注册表[10]是一个分层的数据库，包含了关于Windows操作系统、应用程序和服务的操作数据。这些数据是以树状格式结构的。树中的每个节点被称为一个键。每个键可以包含子键和称为值的数据条目。 有时，一个键的存在就是一个应用程序需要的所有数据；其他时候，一个应用程序打开一个键并使用值

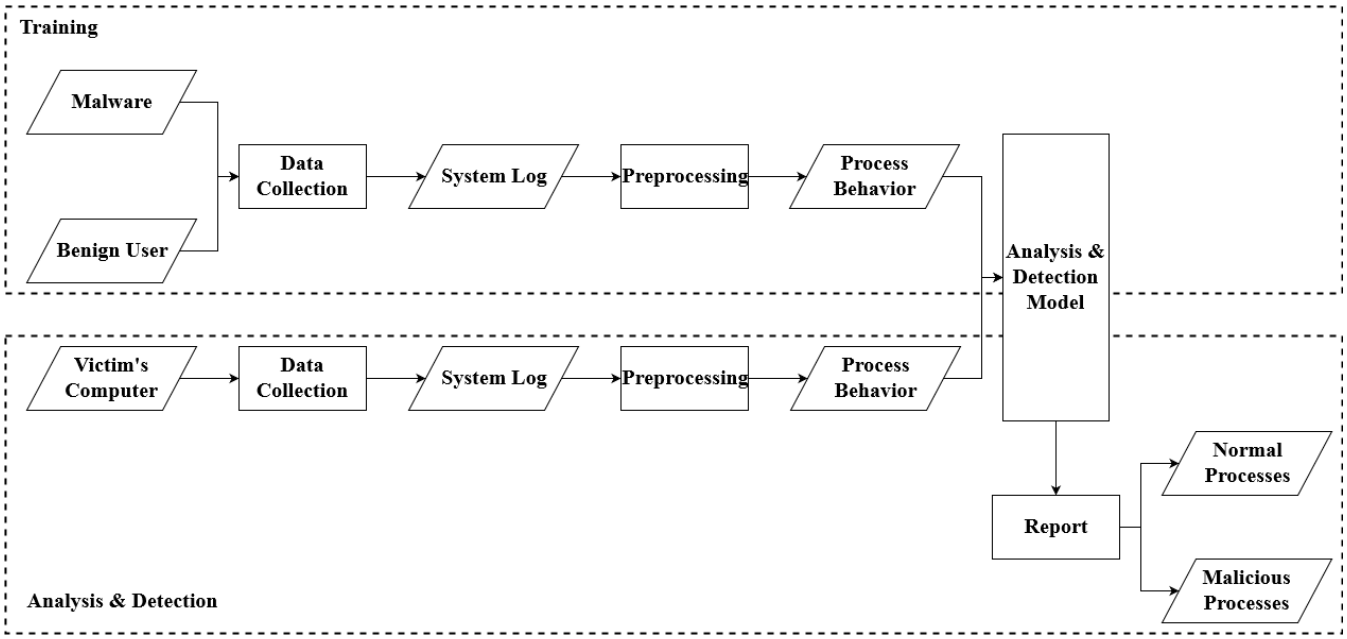

图1：建议的日志分析和异常检测方法

与该键相关联。注册表文件包含重要信息，包括安装的应用程序、最近访问的文件和路径、网络设置和账户信息。恶意软件[7]可能会修改注册表键，以实现在系统上的持久性，如利用Run、RunOnce、BootExecute、Winlogon和Startup键。选定的关键注册表事件包括设置注册表键值、重命名注册表键和值、创建和删除注册表对象，其中表3总结了选定的注册表事件和属性。

网络活动

大多数恶意软件出于各种目的进行网络连接。例如，僵尸网络连接到命令和控制服务器，用于报告受害者信息和接收攻击指令；矿工恶意软件连接到采矿池；一些恶意软件试图利用和感染更多的机器。因此，网络连接对于识别不当行为至关重要。表4总结了所选择的网络事件和属性。

3.2 日志分析和异常检测方法

Sysmon系统日志记录了系统中所有运行中的进程所执行的事件，但失去了进程事件的时间顺序。然而，时间顺序对于理解进程的行为至关重要。本研究利用进程ID来连接一个进程的所有事件记录按时间顺序排列，观察到的过程事件在图2中概述。

传统的神经网络模型在时间序列数据集上表现不佳；根据文献回顾，LSTM适合处理时间序列数据。本研究采用了一种改进的RNN以及LSTM的变体：GRN（门控循环单元）[4]，因为它消除了标准RNN所面临的梯度消失问题，并产生了与LSTM同样出色的结果。拟议的GRU分类模型包括输入

表1：选定的过程事件和属性

活动	属性
事件ID 1:流程创建	活动ID
	图片
	用户
	父图像
事件ID5：进程终止 有名的	活动ID
事件ID 7：加载图像	活动ID
	负载的图像
	签名
事件编号8。 创建远程线程	活动ID
	目标图像
事件ID 10: ProcessAccess	活动ID
	目标图像
	授予访问权

表2：选定的文件访问事件和属性

活动	属性
事件ID 2：一个进程改变了一个文件的创建时间	活动ID
	目标文件名
	创建时间 (CreationUtcTime)
	上一页创造时间
事件ID 9：RawAccessRead	活动ID
事件ID 11: FileCreate	活动ID
	目标文件名
事件编号15。 文件创建流-哈希	活动ID
	目标文件名

表3：选定的登记处事件及其属性

活动	属性
事件ID 12: RegistryEvent (对象创建和删除)	活动ID
	事件类型
事件ID 13: RegistryEvent (数值集)	活动ID
事件ID 14: RegistryEvent (键和值重命名)	活动ID
	事件类型

表4：选定的网络事件和属性

活动	属性
事件ID 3：网络连接	活动ID
	议定书
	已启动
	源端口
	目的地港口

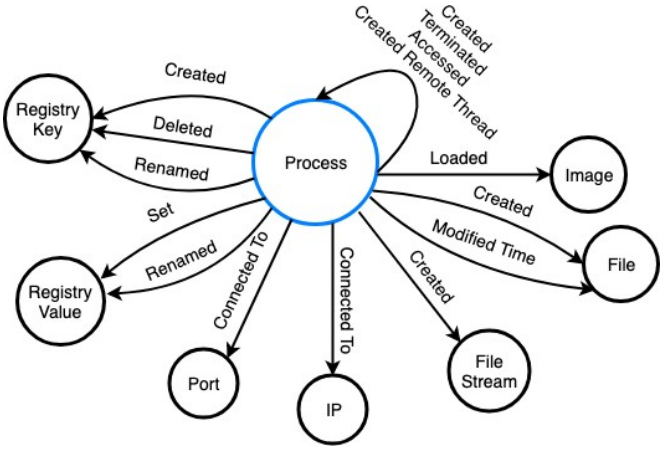

图2：一个过程的事件

图3中概述了拟议的模型结构，包括：第x层、嵌入层E、GRU层G和输出层y。

非数字输入数据需要进行编码，以便输入拟议的GRU分类模型的输入层。建议的特征属于以下数值类型之一：数值型、分类型和字符串数据。大多数建议的特征是数字数据，如事件ID；一些属于分类数据；属性如文件名或环境变量属于字符串数据。数字数据是简单明了的，不需要任何编码。分类数据是由数字编码的，每个类别由不同的数字来表示。一热编码通常用于编码字符串数据，但在处理稀疏数据时效率很低。本研究采用标签编码来减少维度嵌入并减少处理时间。

输入层的输入是由上述过程所执行的事件序列组成的。让$Nevents$为要捕捉的事件的最大数量，以代表一个过程的行为，N_{attr} 为相关事件属性的最大数量。所有的时间序列都需要有相同的长度。换句话说，一个过程的行为在输入层被表示为一个$Nevents$ N_{attr} 的矩阵，如果需要的话，零被填充以符合所需的维度。GRU分类模型在嵌入层上应用矢量变换。GRU层由$Nevents_{神经元}$组成，与进程中的事件数量相匹配，并从训练数据中学习良性和恶意进程之间的事件和属性关系。

4 绩效评估

为了评估所提出的方法是否能够识别恶意行为和未知恶意软件，本研究模拟了被各种类型的恶意软件破坏的机器。每个注入的攻击都在一个受控的环境中执行了5分钟。

环境，并在执行过程中收集系统日志。

从国家高性能计算中心主办的恶意软件知识库中检索了来自36个不同恶意软件家族的10051个恶意软件样本，其中8889个已经被VirusTotal分析过，其余的在评估进行时还没有被上传或分析过，在本研究中被视为未知恶意软件。 从上述实验中共收集了10048条事件记录。

我们从一个校园网络中收集了常见的良性程序执行的正常行为，包括Windows系统进程和常见的用户进程，如文档编辑软件、网络浏览和其他良性应用程序。从良性程序中共获得47175条事件记录。

4.1 对所建模型的性能评估

拟议的基于ML的检测系统旨在对系统日志进行分析并对异常情况进行有效分类。本研究采用准确性作为性能衡量标准，因为正确分类良性行为和恶意行为是同等重要的。准确率表示如下，它是由表5中总结的混淆矩阵计算出来的。

表5：选定的网络事件及其属性

	良性（已检测）的	恶意的（已检测）。
良性	真正的底片 (TN)	假阳性（FP）
恶意的	假阴性(FN)	真正的积极因素 (TP)

表6列出了所提出的GRU模型的参数设置，其中$Nevents$设置为100，N_{attr} 设置为100，Nattr设置为8；提取100个事件来代表一个过程的行为，一个事件最多有8个事件属性。 对不同比例的10倍交叉验证的实验（训练。

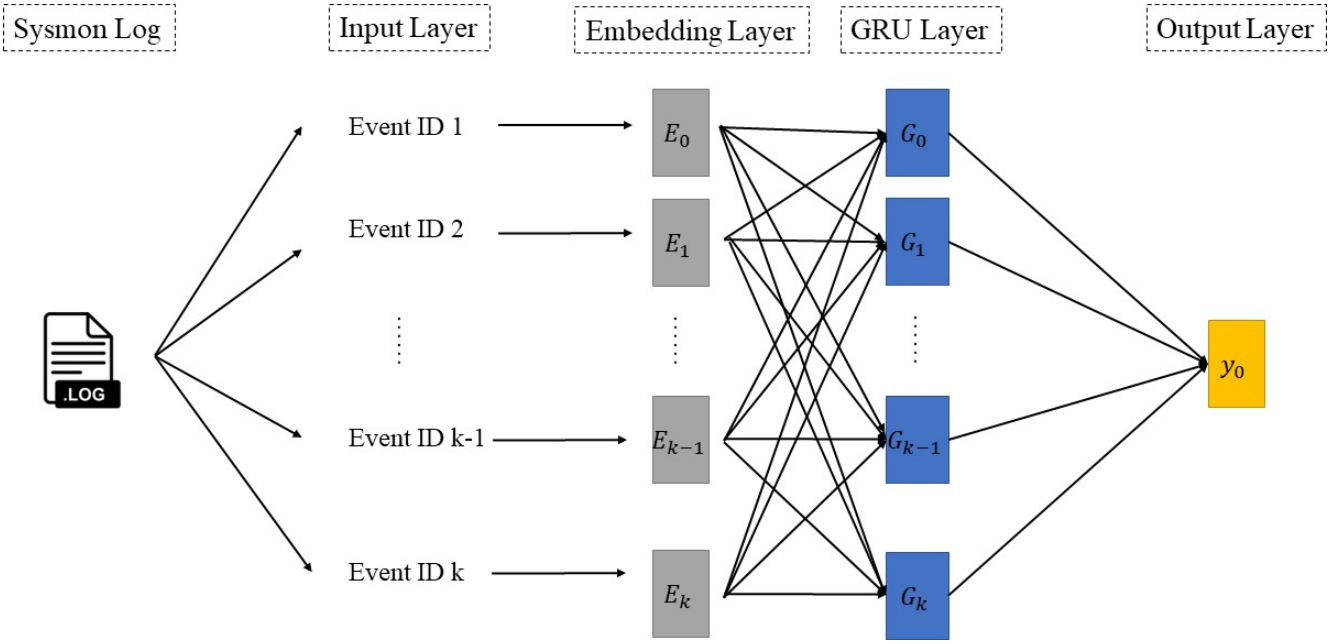

图3：拟议的GRU模型

表6：GRU模型的系统参数

层数	参数	参数设置
输入层	输入尺寸	(无, ∞)
	输出尺寸	(无,800)
嵌入层	输入尺寸	(无,800)
	输出尺寸	(无,800,21)
	掩码为零	真
GRU层	输入尺寸	(无,800,21)
	输出尺寸	(无,100)
	辍学	0.2
输出层	输入尺寸	(无,100)
	输出尺寸	(无,1)
	激活	乙字形
其他参数设置	纪元数：60 批 量大小：400 损失函数：二元交叉熵 优化器： Adam 评价：准确性	

测试范围从2:8、5:5到2:8）进行了测试，检测结果见图4。所提出的模型即使在训练数据为20%的情况下也有很好的准确性，当它有更多的训练数据来学习异常行为时，其性能会有所提高。

$$准确率 = \frac{TP + TN}{tn + fn + fp + tp} \quad (1)$$

4.2 与SVM的性能比较

文献回顾表明，SVM在异常检测方面表现良好，被选为本研究的基线比较。SVM的核函数将数据映射到一个不同的空间，其中的线性混合平面可用于分离类别。RBF (径向基函数）是普遍使用的核函数，与其他核函数相比取得了更好的性能。在评估过程中对SVM的参数进行了优化，以建立一个具有最佳检测性能的SVM模型。获得的最佳SVM模型的参数是：核函数是高斯RBF，γ=0.00001，C=1000，其中超参数γ控制SVM模型中由于偏差和方差造成的误差之间的权衡，超参数C控制松弛变量惩罚（错误分类）和保证金宽度之间的权衡。每个实验都通过随机子抽样测试了5次。图5概述了性能比较的结果，证明了所提出的GRU模型优于SVM，并能有效地对恶意行为和良性行为进行分类。

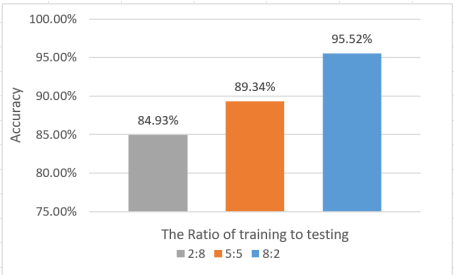

图4：交叉验证法的检测性能

4.3 与Hu-man分析报告的性能比较

为了验证所提出的系统是否能够识别有效的恶意事件，对生成的结果进行了比较

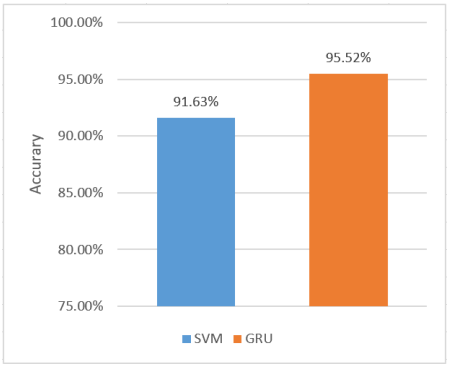

图5：性能比较

与一个安全专家进行的PhotoMiner的分析报告[21]。除了挖掘加密货币，恶意软件PhotoMiner（screen.scr）还通过密码猜测攻击来利用脆弱的FTP服务器。人工分析报告显示，该恶意软件调用cmd.exe将挖矿池的信息（pools.txt）存储到一个临时文件夹，并调用NsCpuMiner32.exe挖矿和xcopy.exe将其传播到受害者机器的磁盘设备。除了人类分析所观察到的上述行为，建议的系统可以提供额外的细节信息，如图6所示的可疑程序和文件的位置，其中恶意软件screen.scr创建了NsCpuMiner32.exe和一个html文件，并催生了一个子进程（cmd.exe），在临时文件夹中创建pools.txt。

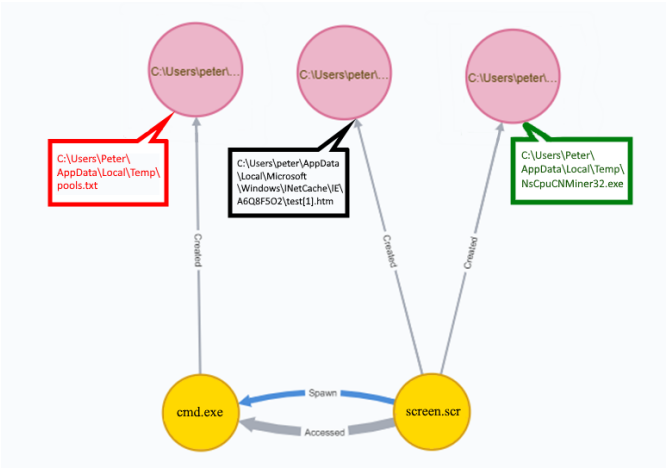

图6：文件系统的部分检测结果

拟议系统的检测结果表明，该恶意软件催生了许多进程，并提供了详细的父子进程关系。图7显示了在第一层深度中产生的子进程，其中红色方框表示恶意软件进程（screen.scr），其右边的米色圆圈表示其位置，大的绿色圆圈总结了其子进程，绿色方框中每个蜂蜜色的圆圈表示一个产生的子进程，蜂蜜圆圈上的数字是代表子进程的位置。可以看出，该恶意软件催生了许多xcopy.exe进程来传播恶意软件。更高深度级别的关系也可以产生。

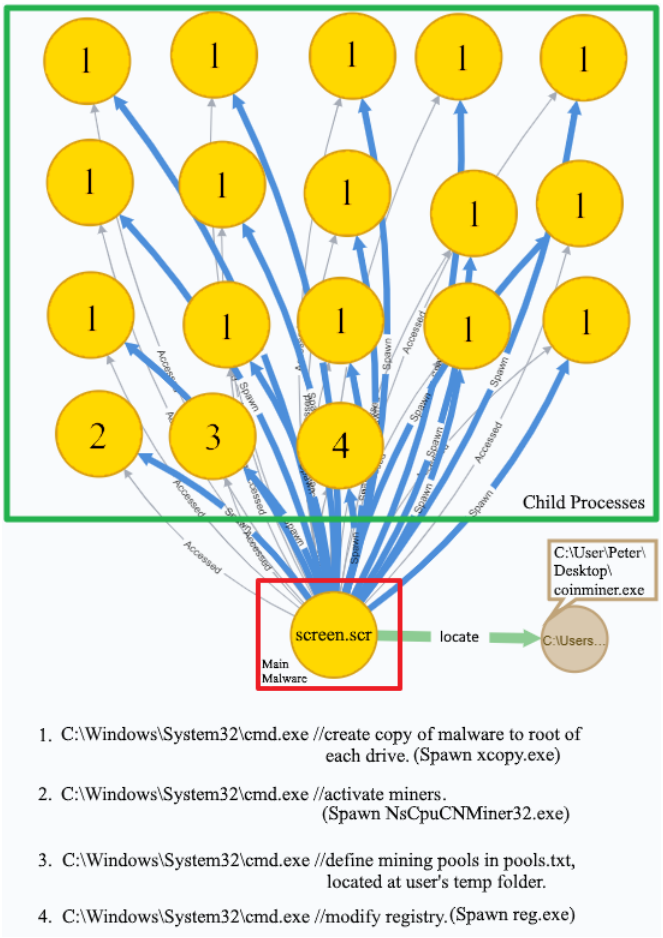

图7：关于过程关系的部分检测结果

对于注册表，人类分析报告指出，恶意软件调用cmd.exe执行reg.exe，在HKCU SOFTWARE Microsoft Windows \ CurrentVersion\Run下创建了一个新条目 \\\ ，以便 在系统重新启动时自动 。除了这一 发现，建议的系统标记了更多的注册表 异常：网络安全设置， 以及 HKU（用户）软件 \ Microsoft\Windows CurrentVersion Internet \\ SettingsZoneMap 下的 多个注册表 键值 ，包括 ProxyBypass、 IntranetName、UNCAsIntranet、AutoDetect， 被修改。由于大量的注册表键值，如果没有有效的工具，人类专家无法识别所有的区分键值，而拟议的系统是有用的，可以识别注册表变化。这个比较的结论是，拟议的系统可以有效地检测出可疑的事件。

表7：未知恶意软件的检测结果

检测到的 / Real	恶意的 (正面)	良性 (负面的)
恶毒的	97.15%	3.80%
良性	2.85%	96.20%
准确度	96.68%	

4.4 未知恶意软件检测的评估

1162个恶意软件样本没有在VirusTotal中进行分析和重新移植，被认为是未知的恶意软件。1072个样本能够在沙盒环境中成功运行，总共获得了1159条恶意日志记录。为了评估所提出的方法是否能对未知的恶意软件和良性进程进行正确分类，还混合了同样数量的良性行为。表7列出了检测结果，表明所提出的检测模型具有93.23%的精确度和3.8%的低误报率。这些结果证明，拟议的解决方案在检测未知恶意软件方面表现非常好。

5 总结

在发生安全攻击的情况下，查明原因和减少损害的影响是时间紧迫的事情。审计日志是发现攻击的可靠来源，应该得到很好的保护，以防止它们被破坏。许多组织将其重要的日志文件保存在云存储中；因此，数据隐私成为一个问题。高效的密码学解决方案，如基于椭圆曲线密码学的基于属性的加密数据共享方案[5]，适合用于满足云存储访问的安全要求。大多数组织缺乏安全专家和人力来分析大量的审计跟踪和发现可疑的事件。本研究提出了一种基于GRU的检测方法，分析系统日志和识别恶意软件的错误行为。

实验模拟了真实世界环境中的攻击和非恶意使用情况。实验结果表明，所提出的解决方案能够有效地对良性和恶意行为进行分类，能够很好地识别未知的恶意软件，并优于SVM检测。总之，性能评估表明，拟议的机器学习模型是实用和高效的。未来的研究可以通过包括额外的日志文件和专业知识来加强日志分析和异常检测，以提高检测性能。

参考文献

[1] H.H. T. Albasheer, M. M. Siraj and M. M. Din, "Towards predictive real-time multi-sensors intrusion 警惕的相关框架，" *Indian Journal of Science and Technology*, vol. 8, no. 12, 2015.

[2] M.Amini, J. Rezaeenoor, and E. Hadavandi, "Effective intrusion detection with a neural network ensemble using fuzzy clustering and stacking combination method," *Journal of Computing Security*, Vol. 1, no.4, pp. 293-305, 2014.

[3] S.D. D. Anton, S. Sinha, and H. D. Schotten, "Anomaly-based intrusion detection in industrial data with svm and random forests, " *Cryptography and Security*, 2019.(https://arxiv.org/abs/ 1907.10374)

[4] K.Cho, B. Van Merriënboer, C. Gulcehre, D. Bahdanau, F. Bougares, H. Schwenk, and Y. Bengio, "Learning phrase representations using rnn encoder-decoder for statistical machine translation, " *Computation and Language*, 2014.(https://arxiv.org/abs/1406.1078)

[5] M.A. Doostari, S. Rezaei and M. Bayat, "A lightweight and efficient data sharing scheme for cloud computing," *International Journal of Electronics and Information Engineering*, vol. 9, pp. 115-131, 2018.

[6] J. Dwyer和T. M. Truta, "使用标准偏差在windows事件日志中寻找异常"，在*第九届IEEE协作计算国际会议上。网络、应用和工作共享*，第563-570页，2013年。

[7] Infosec Institute, *Common Malware Persistence Mechanisms*, Technicalreport, 2016.(https://resources.infosecinstitute.com/common-malware-persistence-mechanisms/#gref)

[8] T.Y. Kim 和 S. B. Cho, "Web traffic anomaly detection using C-LSTM neural networks," *Expert Systems with Applications*, vol. 106, pp. 66-76, 2018.

[9] C.C. Lo, C. C. Huang, and J. Ku, "A cooperative intrusion detection system framework for cloud computing networks," in *The 39th 国际并行处理会议 研讨会*，第280-284页，2010年。

[10] 微软，*注册表的结构*。Technicalreport,2018.(https://docs.microsoft.com/en-us/windows/win32/sysinfo/structure-the-registry)

[11] N.Mishra A. Tayal和S. Sharma，"网络威胁的主动监测和死后取证分析。A survey," *International Journal of Electronics and Information Engineering*, vol. 6, pp. 49-59, 2017.

[12] F.Nabi和M. M. Nabi，"A process of security assurance properties unification for application logic," *International Journal of Electronics and Information Engineering*, no. 6, pp. 40-48, 2017.

[13] V.Nigam, *Understanding Neural Networks.从神经元到RNN、CNN和深度学习*，技术报告，2018。(https://towardsdatascience.com/understanding-neural-networks-from-neuron-to-rnn-cnn-and-deep-learning-cd88e90e0a90)

[14] P. Prasse, L. Machlica, T. Pevný, J. Havelka, and T. Scheffer, "Malware detection by analysing network traffic with neural networks," in *IEEE Security and Privacy Workshops (SPW'17)*, pp. 205- 210, 2017.

[15] B.J. Radford, L. M. Apolonio, A. J. Trias, and J.A. Simpson, "Network traffic anomaly detection using recurrent neural networks," *Computers and Society*, 2018.(https://arxiv.org/abs/1803.10769)

[16] E.Raftopoulos和X.Dimitropoulos，"EDGe在野外的IDS警报相关性"，*IEEE Journal on Seleted Areas in Communi-cations*，第32卷，第10期， pp.1933-1946，2014。

[17] N.Serketzis, V. Katos, C. Ilioudis, D. Baltatzis, and G. Pangalos, "Towards a threat intellegence informed digital forensics readiness framework, " in *Twenty-Fifth European Conference on Information Systems (ECIS'17)*, 2017.(http://eprints.bournemouth.ac.uk/30391/)

[18] A.Singhal, C. Liu and D. Wijesekera, "A model towards using evidence from security events for network attack analysis," *International Workshop on Security in Information System*, pp.83-95, 2014.(https://doi.org/10.5220/0004980300830095)

[19] Statcounter, *Desktop Operating System Market Share Worldwide*, 技术报告，2020。(http://gs.statcounter.com/os-market-share/desktop/worldwide)

[20] Thycotic, *Black Hat 2018 Hacker Survey Report*, Technical report, 2018.(https://go.thycotic.com/l/101722/2018-09-12/5gf8wq/101722/74015/Report_2018_Black_Hat_Survey.pdf?_ga=2.52829416.1772536159.1560412381-274843393.1560412381)

[21] 台湾学术网络计算机应急小组，*矿工木马Photominer感染事件分析报告校园机器*, 技术报告，2017。(https://portal.cert.tanet.edu.tw/docs/pdf/201709290109555585771228906051.pdf)

[22] H.Wang, J. Gu, and S. S. Wang, "An effective intrusion detection framework based on svm with feature augmentation," *Knowledge-Based Systems*, vol. 136, pp. 130-139, 2017.

[23] S.T. Zargar, H. Takabi, and J. B. D. Joshi."DCDIDP。用于云计算环境的分布式、协作式和数据驱动的入侵检测和预防框架，"在*第七届协作计算国际会议上。网络、应用和工作共享（CollaborateCom'11）*，第332-341页，2011年。

[24] S.Zidi, T. Moulahi, and B. Alaya, "Fault detection in wireless sensor networks through SVM classifier," *IEEE Sensors Journal*, vol. 18, no. 1, pp.340- 347, 2017.

纪要

陈佳美自1996年起在中山大学组建管理部工作。2009-2011年，她曾担任网络部的科长和图书馆与信息服务办公室的副主任。1998年至2013年，她曾担任TWCERT/CC（台湾计算机应急小组/协调中心）的协调员，并于2009年成立了TACERT（台湾学术网络计算机应急小组）。她曾担任台湾信息安全中心分支机构TWISC@NCKU的副主席三年之久。她继续为网络安全协会工作。她目前的研究兴趣包括异常检测、恶意软件分析、网络安全和网络威胁情报。

Gen-Hong Syu是国立中山大学信息管理系的一名研究生。他对数字取证感兴趣。

蔡正勋于2017年在台湾高雄的国立中山大学获得硕士学位。 现为台湾国立中山大学博士生。他的研究兴趣涉及数字取证、网络分析和流程分析。