文章编号:1671-4598(2024)05-0253-07 DOI:10.16526/j.cnki.11-4762/tp.2024.05.036 中图分类号:TP393 文献标识码:A

基于方差特征选择与3DES加密算法的医院信息数据安全防御系统设计

蒲 亮，姚树智，敖继威
（联勤保障部队第九六四医院，长春 130062）

摘要：常规的医院信息数据安全防护主要采用信息属性特征融合分类的方法进行安全防护，忽略了信息存储逻辑节点拓扑结构造成的安全影响，导致安全防护攻击成功概率较高；因此，引入方差特征选择与3DES加密算法，研究医院信息数据安全防御系统；提出采用机器学习中的改进方差特征法对医院信息系统进行优化设计；在硬件设计部分，对医院信息数据安全防御系统终端、控制终端与人机接口和接口数据传输模块进行设计；在医院信息数据安全防御方案设计中，采用方差特征选择方法对医院信息进行过滤和归一化处理完成数据更新；采用3DES加密算法，建立信息的模糊判断矩阵，完成医院信息数据安全防御系统设计；经过实验测试设计的系统可有效降低各种攻击的成功概率，平均攻击成功率仅为2.33%，并且数据完整度达到了99.999%，安全性较高，有效保障医院信息安全，避免医院信息的泄露或故障。

关键词：医院信息；安全防御；方差特征选择；3DES加密算法；模糊判断

Design of Hospital Information Data Security Defense System Based on Variance Feature Selection and 3DES Encryption Algorithm

PU Liang, YAO Shuzhi, AO Jiwei
(The 964th Hospital, PLA, Changchun 130062, China)

Abstract: Conventional hospital information data security protection mainly adopts the method of information attribute and feature fusion classification for security protection, ignoring the security impact caused by the logical node topology of information storage, and resulting in the high probability of successful security protection attacks. Therefore, the variance feature selection and triple data encryption standard (3DES) encryption algorithm were introduced to study the hospital information data security defense system. an improved variance feature method based on machine learning was proposed to optimize the design of hospital information system. In the hardware design, the hospital information data security defense system terminal, control terminal, man-machine interface, and interface data transmission module were conducted to design. The variance feature selection method was used to filter and normalize hospital information to complete the data update in the hospital information data security defense scheme. The 3DES encryption algorithm was adopted to build the fuzzy judgment matrix of information, implementing the design of the hospital information data security defense system. The experimental results show that the designed system can effectively reduce the success probability of various attacks, the average success rate of attacks only reaches by 2.33%, with the data integrity of 99.999% and high security, it effectively ensures hospital information security and avoids the leakage or trouble of hospital information.

Keywords: hospital information; security defense; variance feature selection; 3DES encryption algorithm; fuzzy judgment

0 引言

随着互联网技术的发展，在生活中各个领域随处可见互联网技术的存在[1-2]。在互联网技术的应用中，产生的计算机网络信息在互联网共享性、包容性以及开放性的特点下，在网络环境中进行传播[3]。医院在管理工作中也逐渐引入了互联网技术[4]。医院可以利用互联网技术建立电子病历管理系统，使医生和医护人员可以在任何地点通过互联网访问和更新患者的病历信息。还可以通过互联网技术将医学影像信息上传至云端服务器，实现远程存储、分享和访问。与此同时，医院可以通过互联网技术建立在线挂号和预约系统，患者可以通过互联网平台方便地进行医生的预约和挂号。这样可以节省患者的等候时间，提高就诊效率。互联网技术为医院管理带来方便您的同时，也带来了一定的的信息安全问题。由于医院存储着大量的患者个人健康信息，包括病历、疾病诊断、药物配方等敏感信息。这些信息如果落入未经授权的人员手中，可能导致患者隐私泄露、身份盗窃等问题。一旦医院计算机网络系统被入

收稿日期:2023-09-28； **修回日期**:2023-11-03。
作者简介:蒲 亮(1984-),男,大学本科,助理工程师。
通讯作者:敖继威(1984-),男,硕士。
引用格式:蒲 亮 姚树智 敖继威.基于方差特征选择与3DES加密算法的医院信息数据安全防御系统设计[J].计算机测量与控制,2024,32(5):253-259.

侵或遭到恶意攻击可能导致服务中断、信息丢失，严重的可能会导致设备故障、信息篡改甚至控制医疗设备造成伤害。因此，医院信息安全的重要性在于保护患者隐私、维护医疗服务的正常运行、预防恶意软件传播和保障医疗设备安全，这都直接关系到患者的健康和医院的声誉。在这样的情况下，对医院信息安全进行优化成为相关领域不可忽视的问题之一。对此，很多研究人员提出了网络信息安全技术[5]。

文献［6］采用正则表达对网络信息进行表达，将具备统一表达格式的网络信息进行统一转换。在转换信息中进行随机抽取，进行半自动化获取。分析原始信息与转换信息的属性特征关系，建立两者之间对应的信息关联关系，构建出关联信息的并行关系框架。根据框架参数，计算关联信息之间的属性特征相似度，采用 BP 神经网络对信息进行深度分析，计算信息的最佳权值。在框架中执行 BP 神经网络，并将信息进行融合分类处理，实现网络信息安全的建设。该方法在应用过程中存在数据完整度较低的问题，导致信息安全性不高。文献［7］对信息进行定义，以一定数量将信息进行集成，编写信息对应额密钥，通过密钥将部分信息进行重点加密。建立信息密钥的融合矩阵，将其代入到椭圆曲线方程中，进行密钥矩阵的矢量加密，得到信息的最终密钥。采用 DFT-S-OFDM 技术建立信息的加密传输模型，在该模型在计算内节点的数量以及空间位置信息，在内节点处实现信息的变换调频。对信息进行子载波映射处理，并传输至信息接收端中，实现网络信息安全的信息交互过程。该方法在受到攻击时，其平均攻击成功率较高，信息未得到较好的保障。文献［8］针对网络信息中隐私映射强度较低的问题，分析网络信息的流字节变化特点，对信息字节进行逐节加密，对应信息流映射，以此来进行信息隐私强度的提高。基于假设检验技术的支持，进行网络信息安全建模，优化信息流字节的加密进行。在该模型的信息层对信息进行转存，同时编写信息的第二层密钥。将第二层密钥与初始密钥进行替换。在模型映射的环境中，对信息进行二次加密传输，实现网络信息安全的信息传输过程。该方法由于未考虑前期的信息预处理，导致信息数据完整度较低，存在一定的局限性。

考虑到上述文献所提出的网络信息安全技术无法满足医院信息安全工作的现实需求，因此，本文设计一种基于方差特征选择与 3DES 加密算法的医院信息数据安全防御系统，通过硬件与软件的设计，将方差特征选择与 3DES 加密算法结合，实现对医院信息安全访问控制，提高医院信息的安全性，为医院和患者提供更好的保护和服务。

1 基于方差特征选择与 3DES 加密算法的医院信息数据安全防御系统总体结构设计

为了提高医医院信息数据安全防御系统的安全性能，设计一种新的基于方差特征选择与 3DES 加密算法的医院信息数据安全防御系统结构，医院信息数据安全防御系统总体结构如图 1 所示。

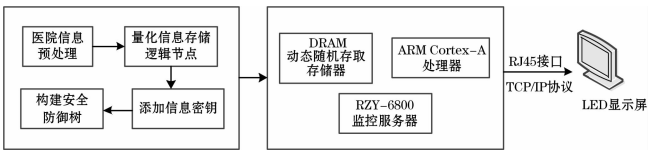

图 1 医院信息数据安全防御系统总体结构图

根据图 1 的医院信息数据安全防御系统总体结构可知，该系统中的第一个模块是“医院信息预处理－量化信息存储逻辑节点－添加信息密钥－构建安全防御树”，而第二个模块则包括“DRAM 动态随机存取存储器、ARM Cortex-A 处理器、RZU-6800 监控服务器”。第一个模块的作用是对医院信息进行预处理并存储量化信息，同时使系统具备安全防护的功能，在该部分引入方差特征选择与 3DES 加密算法，使用这两个算法识别和处理医院信息中的异常值或噪声，并且加密医院信息数据，实现数据预处理和加密，保障医院信息数据安全。具体来说，它负责对进入系统的医院信息进行处理和加密，然后以安全的方式存储在逻辑节点和构建安全防御树中。该模块的工作原理可能包括将医院信息转换为数字数据、应用加密算法对数据进行保护，并将这些加密的数据存储到相应的存储设备中。构建安全防御树可能是指通过使用密钥和其他安全机制创建一个可靠的数据保护架构。第二个模块涉及 3 个组件：DRAM 动态随机存取存储器、ARM Cortex-A 处理器和 RZU-6800 监控服务器。DRAM 存储器是一种常见的计算机内存，用于存储和读取数据。ARM Cortex-A 处理器是一种广泛应用于移动设备和嵌入式系统的处理器，它负责执行系统的核心计算任务。RZU-6800 监控服务器可能是用于管理和监控整个系统的服务器。基于方差特征选择与 3DES 加密算法的医院信息数据安全防御方案设计是最上层的设计，它需要通过控制终端与人机接口设计和接口数据传输模块设计来实现访问控制功能，该部分采用的是 RJ45 接口和 TCP/IP 协议。控制终端与人机接口设计是用户界面和输入来源，它们通过接口数据传输模块连接在一起。接口数据传输模块设计是连接控制终端与人机接口的桥梁，它负责数据的传输和转换。而医院信息数据安全防御系统终端设计是实现上述 3 个设计的底层硬件设施，它通过嵌入式系统实现硬件的控制和数据的处理。

2 医院信息数据安全防御系统硬件结构设计

2.1 医院信息数据安全防御系统终端设计

医院信息数据安全防御系统终端设计包括处理器、存储器、监控服务器等硬件设备，该部分实现第一个模块的逻辑功能，即设计的医院信息预处理、量化信息存储逻辑节点、基于 3DES 加密算法添加信息密钥、计算机网络信息安全防御树的医院信息数据安全防御方案算法。选择合适的处理器和存储器，以便于处理用户请求和存储访问权限数据。同时，监控服务器也是控制终端设计中不可或缺的一部分，它可以实时监控系统的运行状态和用户操作情况，以便于及时发现和处理异常情况。

本文设计系统选用 ARM Cortex-A 型号处理器，ARM Cortex-A 采用最新的 RISC 架构设计；支持 Thumb-2 指令集，提供了高效的代码密度；具有低功耗和高性能的特点；支持虚拟化技术，提供了更好的安全性。该处理器包嵌入了后文设计的基于 3DES 加密算法添加信息密钥、医院信息预处理等算法。

本文设计系统选用 RZY-6800 型号的监控服务器，该服务器采用了 32 位的、高性能的 ARM 处理器和 Linux 系统，并使用了 B/S 体系结构，为用户提供了方便的嵌入式 Web 服务。该服务器不需要网络，可高度集成短信通讯模组及 TTS 语音合成服务，可通过电话语音、短信、邮件、现场广播、声光进行报警。被监控主体直接接入监控主机，无需外接采控模块和协议转换模块，由监控主机集中为各种传感器提供工作电源，停电状态下能够使用内置后备电源独立为主机和传感器提供电，保证监控系统持续稳定运行。

本文设计系统选用 DRAM（Dynamic Random Access Memory）动态随机存取存储器，在系统中起到了存储和提供临时数据访问的作用。DRAM 可以实现更高的存储密度，因为它使用了较少的电路元件来存储相同数量的数据。这意味着在相同尺寸的芯片上可以存储更多的数据，从而提供更大的存储容量。选用 WINBOND 品牌的 DRAM 动态随机存取存储器，型号为 W9825G6KH-6；封装为 TSOP54，数据总线宽度为 16 bit，存储容量为 256 Mbit，最大时钟频率为 166 MHz，电源电压最大 3.6 V，最小 3 V，电源电流最大值 60 mA，最大工作温度 70 ℃。

2.2　控制终端与人机接口设计

接口采用标准 RJ45 接口并附带供电，控制终端与人机接口之间的接口采用标准 RJ45 接口，这是一种常见的网络接口标准，具有较高的传输速度和稳定性。附带供电是指在接口附近提供电源，以实现对设备的供电。这种设计可以方便用户连接设备，同时减少了对电源布线的需求，提高了系统的灵活性和便捷性。人机接口是实现用户与系统交互的界面，需要设计得友好、易用。为此，显示设备选择 LED 显示屏作为显示设备，以实现用户界面的展示。LED 显示屏拥有水平 140°～160°超宽视角，任何位置都是 C 位视角，可以更好的满足医院环境的需要。

2.3　接口数据传输模块设计

在医院的访问控制系统中，接口数据传输模块是负责将控制终端与人机接口设备之间的数据进行传输的核心部分。这一模块的设计需要考虑以下几个方面的要素。

1）传输协议：数据传输模块需要支持多种通用的传输协议，选用 TCP/IP 协议进行等数据传输，TCP/IP 协议具有可靠的传输控制机制，能够保证数据的正确传输，如果数据在传输过程中出现错误，TCP/IP 协议会自动进行重传，确保数据的完整性。

2）数据传输速度：为了满足实时性的需求，数据传输模块需要具备较高的数据传输速度。

3）数据加密：为了确保数据的安全性，数据传输模块应具备对数据进行加密和解密的能力。

4）稳定性：由于该系统应用于医院环境，因此数据传输模块需要具备高度的稳定性和可靠性，以避免因数据传输问题导致的系统故障。

5）兼容性：数据传输模块应能够与控制终端和人机接口设备无缝对接，以确保系统的整体协调性。

基于上述内容，选择 TCP/IP 芯片，配合适当的外围电路和程序代码，实现所需的数据传输功能。

3　医院信息数据安全防御方案设计

3.1　基于方差特征选择方法的医院信息预处理

在医院信息的存储终端中，将信息进行汇集。根据汇集到的信息建立信息空间，在该空间中对信息进行预处理。首先进行信息排查，将重复信息、错误信息进行过滤，对缺失信息进行自主补充，完整医院信息预处理。本研究采用方差特征选择方法对预处理医院信息。

方差特征选择方法是一种用于进行信息过滤的特征选择方法。它通过计算特征的方差，来判断不同特征之间的变化程度，进而确定哪些特征对信息集的分类或回归任务具有重要性。如果某个特征在整个信息集中的取值变化较小，其方差接近于零，那么这个特征对区分不同类别或解释目标变量的能力较弱。因此，可以通过设定一个阈值，将方差低于阈值的特征排除或减少其权重，以达到降维和去除噪声的目的。医院信息特征方差的计算过程如公式（1）所示[9]。

$$V_i^2 = \frac{\sum_{i=1}^{n}(x_i - M)^2}{n} \tag{1}$$

公式中，i 表示医院信息，V 表示信息特征方差，x_i 表示信息特征样本取值，M 表示均值，n 表示信息数量。

选取好的阈值则能够得到好的医院信息特征选择效果；反之则无法达到理想的选取效果。则阈值设定为：

$$\delta = V_s^2 / V \tag{2}$$

公式中，δ 表示阈值，V_s 表示噪声的方差。

将计算结果小于设定阈值的信息进行过滤。并对过滤后的信息进行深度处理。基于医院信息的特征差距较大，在数值范围上所占用的空间较大，本研究将信息特征的灰度值区间设定在［0，255］的范围内，对信息进行归一化处理，该处采用最大化最小化处理方法，最大－最小归一化保留了原始数据中的相对大小关系，即使将数据进行缩放和转换，数据之间的大小关系仍然保持不变，因此，归一化处理如公式（3）所示。

$$x_i' = \frac{255 \times (x_i - \min(x))}{\max(x) - \min(x)} \tag{3}$$

公式中，x_i'表示归一化后的信息特征值，x 表示信息特征值。

利用归一化处理后的信息进行判别博弈，过程如图 2 所示[10]。

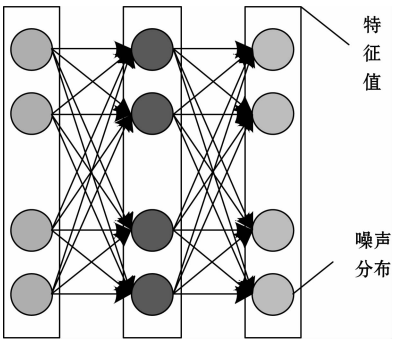

图 2 信息判别博弈

如图 2 所示，在信息空间中对归一化信息进行更新，得到新的网络参数。对判别博弈的参数进行设定，本研究将判别参数设定为 0.5。检验信息的噪声分布，判定信息的均衡状态。

通过上述步骤，完成医院信息的预处理过程。

3.2 量化信息存储逻辑节点

医院信息在存储及运行的过程中有着相对重要的逻辑节点，在计算机网络中进行单向或双向的逻辑连接[11]。在网络存储逻辑节点中，信息将被加权，对应着信息自身的安全属性。基于这一特点，对信息存储的逻辑节点进行量化处理。

对含有逻辑节点的计算机网络进行复杂静态表达。本研究采用线性耦合常微分方程进行这一步骤[12]，如公式（4）所示。

$$\overrightarrow{x_i} = f(x_i) + c\sum_{i=1}^{n} lx_i \tag{4}$$

公式中，$\overrightarrow{x_i}$ 表示节点状态，f 表示节点方程，c 表示耦合强度，l 表示拉普拉斯矩阵。

基于量化处理的目的，对公式（4）进行结果修正，避免信息拓扑结构对量化结果的影响、以适应目标为基础，进行修改计算，如公式（5）所示。

$$\overrightarrow{F_{x_i}} = v\sum_{i=1}^{n} S_i l^{\tau} \tag{5}$$

公式中，F 表示修改度量，v 表示逻辑节点的拓扑节点数量，S_i 表示逻辑节点加权价值，τ 表示修改耦合强度。

在本研究中，将修改后的耦合强度设定为 1。

对修改后的逻辑节点拓扑价值进行量化计算，如公式（6）所示。

$$\zeta = \sum_{i=1}^{n} \alpha^{\mathrm{d}} + F \otimes \beta^{\mathrm{d}} \tag{6}$$

公式中，ζ 表示逻辑节点拓扑价值量化值，α 和 β 均表示影响因子，d 表示两个逻辑节点之间的逻辑距离。在本研究中，将 α 和 β 两个影响因子的取值区间均设定为 $[0, 1]$。

通过上述步骤，完成信息存储逻辑节点的量化处理过程。

3.3 基于 3DES 加密算法添加信息密钥

在计算机网络信息存储的逻辑节点处，采用信息加密技术为信息添加对应的密钥[13-17]。本研究采用 3DES（Triple Data Encryption Standard）加密算法完成这一步骤。3DES 是通过多次应用 DES 算法的加强型对称密钥加密算法，使用 3 个不同的密钥对信息进行加密和解密，首先使用密钥 1 对明文信息进行加密，然后用密钥 2 进行解密，最后再用密钥 3 进行加密。这样的加密过程称为 EDE（Encrypt-Decrypt-Encrypt）。解密过程则是相反的操作，即使用密钥 3 解密，然后用密钥 2 加密，最后用密钥 1 解密。这种加密算法的密钥空间更大，使得密钥猜测攻击的难度大大增加，同时弥补了 DES 算法中可能存在的密钥长度过小的问题，提高了信息的安全性。该方法中，信息密钥添加过程[18]如公式（7）所示。

$$y_i = D_k(i \oplus k_1) \oplus k_2 \oplus i \cdot k_3 \tag{7}$$

公式中，y_i 表示信息密钥，D_k 表示加密技术，k_1 、k_2 以及 k_3 分别表示 3 个不同的密钥。

上述步骤可以表示为如图 3 所示的示意图[19]。

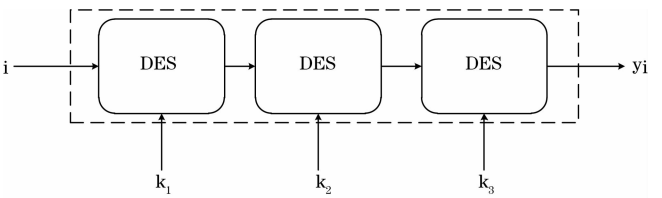

图 3 信息加密示意图

按照如图 3 所示的过程对医院信息进行三重加密。

根据需要，生成或选择合适的密钥。3DES 加密算法支持 3 个密钥长度：128 位、192 位和 256 位。根据加密强度的要求和系统支持的密钥长度，选择一个合适的密钥长度，并确定相应的添加重数。添加重数表示对明文信息进行加密操作的轮数。密钥长度为 128 位时，添加重数为 10；密钥长度为 192 位时，添加重数为 12；密钥长度为 256 位时，添加重数为 14。

按照添加重数和密钥顺序，依次对明文信息进行三次加密操作。具体操作如下：

1）使用第一个密钥加密明文信息。

2）使用第二个密钥解密上一步得到的加密信息。

3）使用第三个密钥再次对上一步得到的解密信息进行加密。

解密过程与加密过程相反。按照相同的添加重数和密钥顺序进行解密操作：

1）使用第三个密钥解密加密信息。

2）使用第二个密钥加密上一步得到的解密信息。

3）使用第一个密钥再次对上一步得到的加密信息进行解密，得到最终的明文信息。

3.4 构建计算机网络信息安全防御树

为经过信息加密处理的医院信息构建信息安全防御树，进一步提高计算机网络信息安全。

确定因素集，建立信息的模糊判断矩阵[20]，如公式（8）所示[21-22]。

$$\boldsymbol{A}=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{m} \end{bmatrix} \tag{8}$$

公式中，$\boldsymbol{A}$ 表示模糊判断矩阵，$\boldsymbol{a}$ 表示矩阵指标标度。

根据该矩阵，建立信息安全的攻击防御树，如图 4 所示。

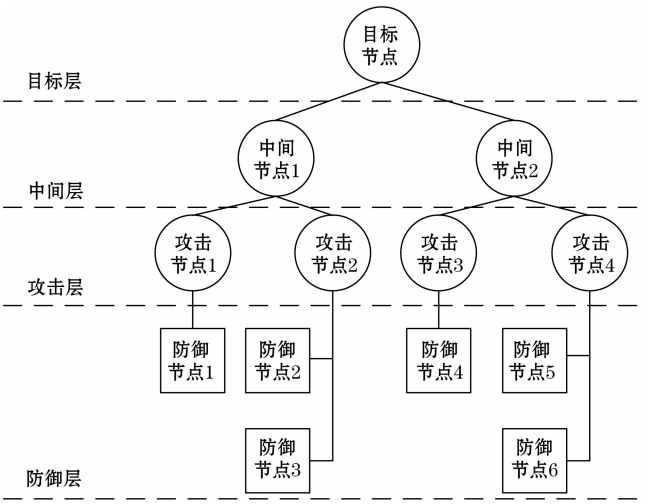

图 4　信息安全防御树示意图

通过建立如图 4 所示的信息安全防御树，对加密处理后的信息攻击防御训练。至此，完成信息加密技术在医院信息安全中的应用设计过程。

4　实验测试

4.1　实验准备

对本文设计的基于方差特征选择与 3DES 加密算法的医院信息数据安全防御系统的应用效果进行验证，采用模拟仿真的方法进行。从实验结果分析本文所提系统在医院信息安全中的有效性。

以某三甲级医院的计算机网络信息集作为本次实验的信息模拟样本。该信息集已经做过预处理，将含有患者、医院内部等隐私信息进行剔除，确保本次实验所模拟的信息不会造成该医院涉及人员隐私信息的泄露。该信息集中的信息按照医院运作系统的不同进行信息划分，如表 1 所示。

表 1　医院信息分类

类型	信息量
医院运营管理信息	44 632
检验网络系统信息	1 636
医学影像系统信息	46 649
远程医疗系统信息	78 965
对外办公系统信息	7 966
病案扫描系统信息	94 661
网上图书馆信息	64 573
医疗器械信息	49 865
医疗药品信息	11 053

如表 1 所示，本次实验共获得模拟信息样本 400 000 条。在每个类别的医院信息中进行随机筛选。本次实验采用 finebi 软件的随机筛选功能完成这一步骤。将不同类别的信息进行分别编号，在软件中输入初始信息。按照如表 2 所示参数进行设定。

表 2　信息随机筛选参数

参数项	参数设定
信息连接名称	Mysql 连接
驱动	com. mysal. jdbc. Driver
信息库名称	Database2
主机	Hostname
端口	3 306
用户名	Root
编码	默认

通过上述步骤，完成实验模拟信息的随机筛选。根据筛选所得的信息，使用信息模拟软件进行多样化信息模拟。本研究采用高通量的 wgsim 软件进行信息模拟。将该软件上传至 Linux 服务器，进行加压缩折处理，进而进行信息模拟的代码编译，如图 5 所示。

```
wgsin

(short read simulator lerogramwgsimversion:0.3.1-113
Contact :Heng Ti <1h3Gsanger.ac.uk>

Usage: wqsim[options] <in,reffa> <out .read1 fg> <out , read2 fg>

baso orror rate [0.020]outor distance between the two onds [5001
standard deviation [50]
number of read pairs [1000000]lenqth of the firat read 1701
lenqth of the second read [701
rate of mutations [0.00101
fraction of indels [0.15]
probability an indel is extended [o.30lseed for random generator [-1]
disgard if the fraction of ambiguous bases higher than FLOAT (0.05]
haplotype mode
```

图 5　信息模拟编译

通过上述过程，完成实验信息的模拟，得到本次实验信息共 10 546 210 条。

完成实验信息的准备后，搭建本次实验的整体环境。本次实验在联合仿真平台上进行。采用 OPNET 和 MATLAB 进行联合仿真，利用 OPNET 软件将实验信息中的计算机网络层边缘节点和物理对象节点进行识别与存储，实现实验信息在仿真平台上的模拟医院信息的日常运行。搭建出的实验外环境如图 6 所示。

如图 6 所示，本次实验所使用的主控计算机为 Windows 10 操作系统的台式电脑，其参数配置如表 3 所示。

为了对本研究所提方法进行评估，采用模拟攻击的方法在实验信息模拟运行的过程中进行攻击测试，检验医院信息的安全防护效果。设置 DOS、Pod、DDOS、Prel、Rootkit、Spy、Neptune、Worm、Ipsweep、Tunnel 共 10 种攻击类型，每次随机发起一种攻击，具体攻击类型及参数设

图 6 实验外环境

置如表 4 所示。

表 3 主控计算机参数配置

参数项	参数配置
CPU	Intel Xeon E5-2620v4
硬盘	4 T
内存	128 GB
网卡	1 000 Mbps 以太网卡
处理器	八核
主频	3.40 GHz
PostgreSQL	9.6

表 4 攻击类型及参数设置

攻击类型名称	攻击流量实际数量/Mbps	攻击持续时间/min
DOS	150	45
Pod	45	12
DDOS	150	1200
Prel	13	260
Rootkit	13	—
Spy	15	720
Neptune	200	450
Worm	8	120
Ipsweep	20	50
Tunnel	16	100

完成上述准备后，开展本次医院信息安全防护效果测试实验。

4.2 医院信息安全

随机选择某一类型的医院信息进行攻击测试，攻击时长设定为 24 h，单次攻击时长设定为 5 min。攻击间隔为 4～10 min 不等。判定攻击下，信息的损失值。得到该类型信息的安全防护结果如图 7 所示。

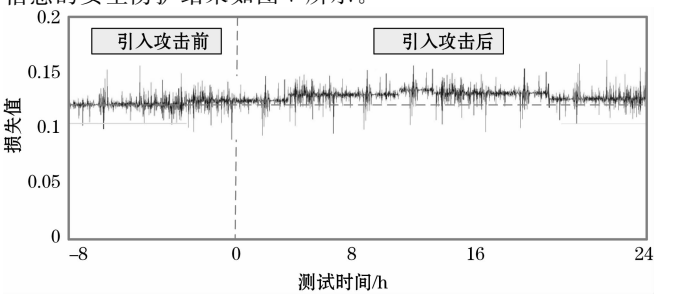

图 7 医院信息安全防护效果测试

由图 7 可知，在引入攻击信息之前，实验信息在模拟运行中的损失值平均约为 0.127，在引入攻击信息后，实验信息的损失值在一定程度上有所增高，平均损失值约为 0.139，与正常运行时的损失值相比，受到攻击后的信息损失值仅增高了 0.012，符合预期效果。从这一测试结果可以看出，该方法在医院信息安全检测中起到了较好的防护效果，有效展现了应用结果，表明了本文所提方法的可行性。

4.3 结果评价指标

为了更加直观地体现出本研究所提方法的有效性，将本次模拟仿真实验的结果评价指标设置为攻击成功的概率。将获取该条信息的读取权限作为攻击成功的表现，总概率的计算方法如公式（9）所示：

$$p_s = \frac{n_1 + n_2 + \cdots + n_9}{\delta} \times 100\% \tag{9}$$

公式中，p_s 表示攻击成功概率，δ 表示攻击总条数，n_1 至 n_9 分别表示成功获取读取权限的信息数量。

攻击成功概率的计算结果直接反映了医院信息安全的防护效果。计算所得的攻击成功概率结果数值越低，则说明该方法对计算机网络信息安全的防护效果越好，信息的安全性越高，具备更高的实践应用价值。

同时，以医院访问数据完整度为评估指标，其计算公式为：

$$B = (1 - \frac{B'}{B_0}) * 100\% \tag{10}$$

公式中，B' 表示缺失数据的数量，B_0 表示总数据量。

公式（10）的评估指标数值越大，则说明系统的安全性越好，可以有效保障医院信息数据安全防御系统数据的完整性。

4.4 结果分析与讨论

为了体现本研究所提方法实验结果的有效性，分别应用文献［6］和文献［7］所提出的网络消息安全方法作为对比对象进行对比实验，文献方法的硬件配置与本文实验一致，其文献［6］方法的相似度计算参数设置为 0.874、输出层神经元对应权重为（0，0.428）、输出层节点阈值为 0.647，常数为 0.682，文献［7］方法的加密信息种类参数设置为 9、密匙数量对设置为 6、可传输距离的系数阈值设置为 0.741、示映射过程间隔为 1.245。将对比实验的信息安全攻击时间延长至 10 天。在为期 10 天的实验时间内，进行不规律的间断性攻击，在每天的上午 10 点进行过去 24 小时的攻击成功的信息量统计，进行攻击成功概率的计算。

为了保证本次对比实验的科学性，每天为不同方法导入的信息保持完全一致。在前 9 天的实验时间里，分别导入一个类型的医院信息，在实验进行的第 10 天，为不同方法导入全部的实验模拟信息。

经过实验，得到不同方法的实验结果如图 8 所示。

由图 8 可知，在为期 10 天的实验测试过程中，3 种方法均在第 10 天的攻击成功概率达到最高，说明本次实验结果可信。在 10 天的实验时间里，本文所提方法的平均攻击

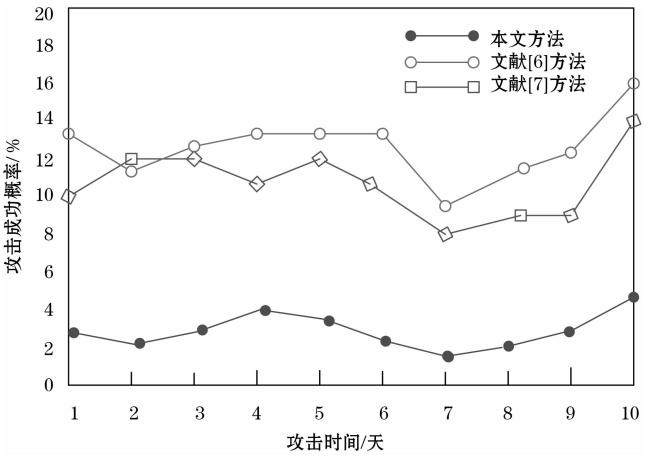

图 8　不同方法实验结果

成功概率为 2.33%，文献［6］和文献［7］所提方法的平均攻击成功概率分别为 12.64 和 9.26%，由此可见，本文方法中，医院信息被攻击成功的概率有着较大幅度的降低。

从对比实验结果可以看出，本文所提出的医院信息安全防护方法能够有效应对外界的攻击手段，攻击成功概率较低，大幅度提高了计算机网络信息的安全性。在医院信息安全防护的实践工作中，能够抵抗外界的攻击，有效保障了信息安全，避免医院信息的泄露或故障，为医院的日常运营工作提供基础支持，有着较高的实践应用价值。

为了进一步验证本文方法的安全性，以医院信息数据安全防御系统数据完整度为评估指标，分析不同方法的数据完整度，结果如表 5 所示。

表 5　不同方法的数据完整度

数据量/G	数据完整度/%		
	本文方法	文献[6]方法	文献[7]方法
0.5	99.997	99.987	99.988
1.0	99.998	99.983	99.977
1.5	99.997	99.979	99.990
2.0	99.998	99.985	99.986
2.5	99.998	99.980	99.984
3.0	99.999	99.984	99.988

根据表 5 数据可知，不同方法的数据完整度均较高，达到了 99.975%以上，但是详细分析可知，应用本文方法的医院信息数据安全防御系统的数据完整度在 3.0 G 数据量时，其达到了 99.999%，而此时的文献［6］方法和文献［7］方法的数据完整度仅为 99.984%和 99.988%，相比可知，本文方法的数据完整度比文献方法提高了 0.011%，说明本文方法具备更好的安全性能，可以有效保障医院信息数据安全防御系统的数据完整性。

5　结束语

在医院的日常运营工作中，信息安全成为各方面所共同关注的问题，提高信息安全，避免信息泄露对于医院的运营十分关键。对此，本研究设计基于方差特征选择与 3DES 加密算法的医院信息数据安全防御系统，并检验设计系统在医院信息安全控制中的应用。经过实验可知，该方法在信息运行存储过程中，被攻击成功的概率较低，有效对医院信息安全进行了防护，保障信息安全，助力医院运营，推动网络信息技术在医院领域的应用与发展。

参考文献：

［1］牛　耕. 基于模糊匹配的蜂窝形光纤传感网络信息安全检测方法［J］. 激光杂志，2022，43（6）：206－210.

［2］王厚奎. 数据加密机制下的船舶网络信息安全管理系统［J］. 舰船科学技术，2021，43（24）：154－156.

［3］陈辉定. 基于计算机网络技术的网络信息安全防护体系构建［J］. 现代雷达，2023，45（2）：101－103.

［4］龚剑敏，顾东兴，冯　骏. 互联网医院信息安全面临的挑战与对策［J］. 中国医院，2021，25（9）：81－83.

［5］段　然，杨聚加，周来新. 智慧医院医疗数据安全交换平台的设计与实现［J］. 重庆医学，2021，50（21）：3740－3745.

［6］杨昌尧，袁展伍，翁云峰. 舰船移动网络信息安全大数据集成模型［J］. 舰船科学技术，2021，43（20）：172－174.

［7］马艳娥，李瑞金. 基于 DFT－S－OFDM 的网络信息安全加密传输仿真［J］. 计算机仿真，2022，39（1）：358－361＋393.

［8］乔俊峰. 假设检验技术下舰船通信网络信息安全加密建模研究［J］. 舰船科学技术，2021，43（10）：121－123.

［9］王甜甜. 互联网新闻分类中特征选择和特征提取方法研究［D］. 中国科学技术大学，2016.

［10］魏明月，陈　敏，郁嘉波，等. 基于区块链的互联网医院云药房平台设计和实践［J］. 中国卫生资源，2021，24（3）：219－222.

［11］陈宏君，蒋建军. 基于光通信技术的物联网数据加密技术研究［J］. 激光杂志，2021，42（5）：116－119.

［12］易新蕾. 具有时变线性耦合结构的常微分方程系统的局部完全同步分析［D］. 上海：复旦大学，2014.

［13］张馨方，周江华. 基于轻量型 AES 加密算法的浮空器平台数据传输方案［J］. 计算机测量与控制，2023，31（6）：183－190.

［14］杨　亮. 基于区块链技术的机器人数据加密传输控制系统设计［J］. 计算机测量与控制，2021，29（6）：119－122.

［15］杨小东，廖泽帆，刘　磊，等. 基于区块链和属性基加密的电力数据共享方案［J］. 电力系统保护与控制，2023，51（13）：169－176.

［16］王鑫淼，孙婷婷，马晶军. RSA 算法在网络数据传输中的研究进展［J］. 计算机科学，2023，50（s1）：703－709.

［17］冯　涛，陈李秋，方君丽，等. 基于本地化差分隐私和属性基可搜索加密的区块链数据共享方案［J］. 通信学报，2023，44（5）：224－233.

［18］陈　炜. 安全网关中密钥交换与 3DES 加密算法实现研究［D］. 成都：电子科技大学，2010.

［19］琚　理，赵金币. 基于卷积神经网络的文档有效数据加密仿真［J］. 计算机仿真，2022，39（10）：440－444.

［20］高　翔，祝跃飞，刘胜利. 应用三角模糊矩阵博弈的网络安全评估研究［J］. 西安交通大学学报，2013，47（8）：49－53.

［21］哈冠雄，贾巧雯，陈　杭，等. 无第三方服务器的基于数据流行度的加密去重方案［J］. 通信学报，2022，43（8）：17－29.

［22］牛淑芬，宋　蜜，方丽芝，等. 智慧医疗中基于属性加密的云存储数据共享［J］. 电子与信息学报，2022，44（1）：107－117.