基于云计算技术的网络通信数据安全传输策略研究

梁琛
国网冀北电力有限公司宽城县供电分公司

摘　要：现如今，网络平台上的数据传输面临诸多安全挑战，包括但不限于数据窃听、篡改及身份伪装等问题，这些都严重危害用户隐私和数据安全。因此，研究新型的网络通信数据安全传输策略具有重要意义。本研究首先对云计算技术进行简要概述，随后结合云计算技术，提出了一种新的网络通信数据安全传输策略，最后通过实验验证了该策略的有效性。本研究旨在增强网络环境中通信数据的安全性，从而提高用户对网络服务的信任度和满意度。

关键词：云计算；网络通信；数据安全
【DOI】10.12252/j.issn.2096-6261.2023.08.103

Abstract: Nowadays, data transmission on network platforms faces many security challenges, including but not limited to data eavesdropping, tampering, and identity disguising, all of which seriously endanger user privacy and data security.Therefore, studying new network communication data security transmission strategies is of great significance.This study first provides a brief overview of cloud computing technology, and then combines it to propose a new network communication data security transmission strategy.Finally, the effectiveness of this strategy is verified through experiments.The aim of this study is to enhance the security of communication data in network environments, thereby increasing user trust and satisfaction with network services.

Keywords: Cloud computing; Network communication; Data security

引言

在当前的网络环境下，数据传输面临诸多安全挑战，如数据泄漏、未授权访问和篡改等问题，这些都对用户隐私和数据完整性构成了严重威胁。鉴于这些安全难题，开发一种既高效又可靠的网络通信数据安全传输方案变得至关重要。随着云计算技术的兴起，它为解决这些挑战提供了新的可能性。因此，本研究提出了一种新的基于云计算的网络通信数据安全传输策略，旨在增强数据传输过程的可靠性，并为网络环境中的数据安全传输提供重要支持。

一、云计算技术概述

云计算技术是一种基于互联网的计算方式，它允许用户和企业通过网络访问共享的资源库，包括服务器、存储、应用程序和服务。这种技术的核心在于提供可扩展、灵活和高效的资源利用方式，无须用户管理复杂的后台硬件和软件。云计算支持按需付费模式，使得用户可以根据实际需求调整资源使用量，从而优化成本。它支撑了各种应用场景，从数据存储和备份，到复杂的数据分析和人工智能任务，极大地推动了数字化转型和创新。随着技术的不断进步和安全性的增强，云计算已成为现代企业IT架构不可或缺的一部分。而目前随着网络安全形式的日趋严峻，传统的网络通信数据传输方法面临着多种内外部攻击的威胁，而云计算技术的出现提供了一种新的解决方案，使得数据传输更加安全和可靠。通过云计算技术，数据传输可以利用高级加密技术和多重安全协议来保护信息不被未授权访问或窃取。

二、策略设计

1.制定安全传输协议

传统的网络通信数据传输方法面临着多种内外部攻击的威胁，为此，本研究提出了一种基于云计算的安全传输策略。该策略通过制定一套针对网络通信节点信息的安全传输协议，有效地防御了未知的信息截取攻击。具体地，传输协议通过TESLA协议实现了节点间的共享时钟，建立了协议验证机制。发送方能够依据信号的传递延迟来验证数据包的真实性，其中初始数据包 m 的标识设为 id ，其传输格式可按照下述公式展示：

$$m = id, T_{\text{int}}, K_0, T_0, N, I_0, d \geq Sign(m), cert \quad (1)$$

其中， $Sign(m)$ 和 d 分别代表对消息的签名和密钥

传递的时间延迟，而$cert$表示由认证中心颁发的证书，而$T_{\text{int}}, K_0, T_0, N, I_0$都是关键的传输验证参数。一旦开始数据传输，相连节点将即刻进行ID验证，并生成安全传输节点的具体位置信息。基于所得到的具体信息，节点和信标将进行重新配置和分组，进一步优化了数据传输的安全性，该步骤的具体形式如下：

$$B_j = \left\{ id, id_x, id_y, I_i, e_j, P(B_{j+1}) \right\} \quad (2)$$

其中，e_j和I_t分别代表休眠状态下的分组变量和数据传输的时间间隔，id_x与id_y指代数据传输的位置坐标，B_j和$P(B_{j+1})$分别表示当前的信标分组包和下一信标分组的预期位置。该协议利用哈希函数精确计算认证过程的延迟，并通过监测信标能量的变化预测潜在的传输攻击点，以此确保数据传输的安全。随着时间间隔的延长，协议内部密钥始终保持加密状态，且通过不同的信标分组来增强安全性。为了进一步加强所设计协议的安全性，本文引入了信标位置验证机制，通过邻近节点的信标分组发送及接收者的验证来实现，协议的安全性条件可以通过下述公式表达：

$$\left[\frac{t_r - T_0}{T_{\text{int}}} \right] \le I_i + d \quad (3)$$

其中，T_{int}和t_r分别表示数据实际到达的时间与接收方的本地接收时间。若传输违背此条件，则暗示传输存在安全风险，需对数据重新进行分组，确保数据安全准确地传输。反之，若符合该安全条件，这意味着数据可以被安全地接收。这一过程将重复进行，直到数据传输符合协议规定的安全标准为止。

2.构建安全传输模型

为了最大化云计算中虚拟化资源调度的潜能，本研究构建了一个虚拟采样模型p，具体如下：

$$p = x(t + q\Delta t) - h(t + q\Delta t) + \omega \quad (4)$$

其中，x和t分别表示经过中心重构后的传输数据和数据重构的时间点，而q和Δt分别表示数据的最小维度与重构的初始时间。h表示云计算环境中用于确保数据传输安全的函数，而ω表示在数据重构过程中使用的加权系数。该模型通过有效提取并随机分配网络通信数据的传输特征，实现了数据特征的高效管理和优化。接着，这些特征被送入云计算的数据资源分析中心，进行深入的资源处理与调度。然后为了得到特征演化的动态和其峰值参数Y，可以依据下式进行计算：

$$Y = X(T + K)\sum_{i=1}^{n} h_i (N-1)^r \quad (5)$$

其中，T和K分别表示进行空间动作捕捉的时间与云计算环境中的特征向量，而h_i是用于安全匹配的参数，N表示采样时间延迟，而r代表采样次数。利用这些参数计算得到的峰值可以用来评估网络通信数据与云计算资源库之间的匹配度和拟合关系。基于这种评估，设计了安全传输模型C如下：

$$C = XYf^{-j2\pi fk} \quad (6)$$

其中，f是归一化频率，用于量化数据传输频率的标准化值，而j代表云计算中心的实时流量，捕捉数据中心处理能力和流量状况的即时指标，k是安全传输常数，反映了安全策略在数据传输过程中的固有属性。考虑到网络通信数据的固有可变性，本文提出的传输方法内置了相关联性规则，该规则与数据输出频率相结合，用于描述数据传输特征。这种特征描述的计算方法由描述式Q给出，它基于数据传输频率及其关联性规则，为网络通信数据传输提供了一种新的特征描述方式，具体如下：

$$Ra_n e^{-j2\pi f} \quad (7)$$

其中，a_n代表中心资源调度信息$e^{-j2\pi f}$，R指的是传输匹配函数，它是用于评估数据传输效率和安全性的关键参数。在这种特征描述的基础上，可以对数据传输的安全性进行进一步的优化。具体方法是对云计算中心的数据处理能力进行三维重构，通过这种三维重构，可以得到网络数据安全传输的迭代公式如下：

$$W = \theta_1(k) - R[\varphi(k)] \quad (8)$$

其中，$\theta_1(k)$和$\varphi(k)$表示经过迭代处理后的资源信息和应用于安全过滤的资源。这个迭代公式允许对网络通信数据进行安全迭代处理，通过综合频谱分析，进一步优化和调度资源传输。应用该迭代公式后，可以进行资源传输的优化调度，其结果可以通过下式表示：

$$A(t) = E + W\sqrt{a}B \quad (9)$$

其中，E表示输出频谱向量，这是通过综合频谱分析得到的结果，它反映了数据传输过程中的频率特性。W代表数据传输的初始化参数，包括了传输开始时所有必要的设置信息。而a是振荡幅值，指的是数据传输过

程中信号强度的变化幅度。B代表关联系数，用于量化数据传输过程中各个参数间的相互依赖性和联系强度。

3.设计安全传输方案

保障网络通信数据安全的关键是建立一个全面而坚固的传输方案。本研究提出的方法致力于完全达到网络通信数据安全传输的标准，融合了当前最先进的数据安全传输技术。该策略以保障数据传输的自主安全为目标，实施了数据流的认证和加密，并为WIA-PA网络定制了专门的报文格式，有效提高了网络通信系统的安全性。除此之外，该策略还采用了HMAC-SM3认证机制并搭配SM4加密算法，为数据传输提供了两层安全保护，其中SM4加密算法结构如图1所示。通过这种结合，传输初始化过程中，相关通信节点能够接收到节点认证和密钥配置的指示，使用这些信息完成消息认证，并将请求报文安全地发送到网关。网关在接收到报文后，将执行必要的验证工作，确保数据的双向传输和响应的安全性。

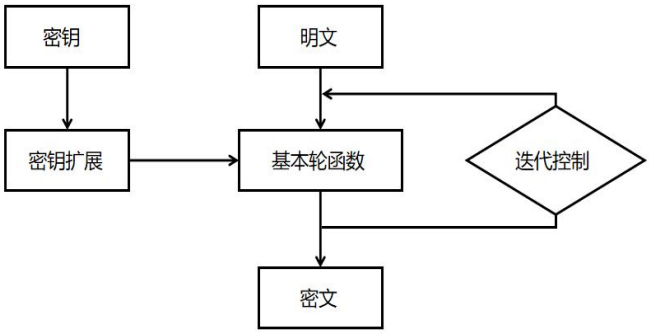

图1 SM4加密算法结构

此外，本文通过在数据传输初期应用CCM算法并结合随机数因素，增强了控制效力并有效抵御了潜在的不规则攻击，确保了传输过程的安全。该设计确保了传输数据的真实性和完整性，有效验证了通信双方身份，增强了数据交换的可信度。通过对处理参数的即时验证，极大地减少了外部攻击对数据传输安全的威胁。同时，定期更换传输密钥提升了防篡改和防盗取的能力，从而显著提高了网络通信数据传输的安全性与可信性。

三、实验

在本次实验中分别应用了本研究所提出的基于云计算的网络通信数据安全传输策略和传统的数据传输策略，对从126，465条网络通信数据中随机抽取的一定数量的数据进行了传输测试。本实验旨在比较和分析两种传输方法在实际应用中对数据安全性的影响。具体的实验结果记录在表1中。

表1 实验结果

传输数据条数	基于本文所提出的传输策略被窃取数据数/条	基于传统的数据传输策略被窃取数据数/条
59	0	4
136	0	7
248	0	14
365	2	16
496	2	18
598	2	24
638	2	41
781	2	71
1052	4	88

根据表1的结果显示，通过本研究设计的基于云计算技术的网络通信数据安全传输策略所传输的数据中，被非法窃取的数据条数明显少于采用传统网络通信数据传输策略的情况。这一结果明确表明，本文提出的安全传输策略在减少数据泄漏方面表现出更高的效率和可靠性，从而证实了该策略在网络通信数据传输安全性方面的优越性。

四、结论

本文结合云计算技术，成功设计了一种新的网络通信数据安全传输策略。通过与传统网络通信数据传输策略的对比实验，结果明确显示本文提出的策略在降低数据被非法窃取的风险方面具有显著优势，从而证明了该策略的传输效果和可靠性。本研究旨在提高数据传输的可靠性，为云平台中的数据安全传输作出实质性贡献。

参考文献

[1]郭丽.工业互联网数据传输安全问题及改进策略研究[J].现代工业经济和信息化，2022，12（07）：117-119.

[2]余志浩.CBTC系统数据传输安全分析[J].铁道通信信号，2021，57（06）：66-70.

[3]王朋成.电铁牵引变电所内部数据传输网络安全防护研究[J].电气化铁道，2020，31（S2）：66-68.

[4]李红叶.结合云计算技术分析网络安全攻防实验平台的设计和实现[J].辽宁科技学院学报.2018，（3）.

[5]苏华江.大数据和云计算技术在智慧城市建设中的应用[J].数字通信世界.2021，（9）.