SM4加密算法在车联网上的应用

汇报人：

2024-01-21

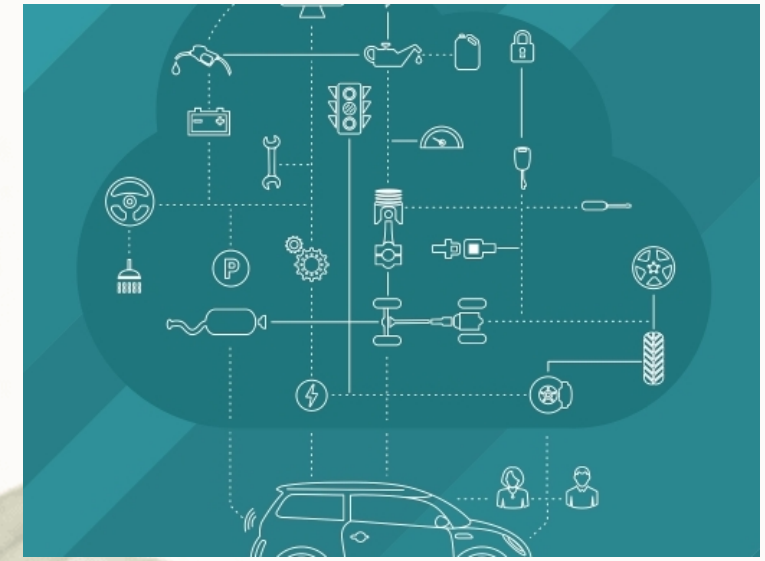
目录

CONTENTS

01

引言

背景与意义



车联网技术的快速发展

随着汽车智能化、网联化的加速推进，车联网技术已成为汽车产业创新发展的重要方向。

信息安全问题日益突出

车联网技术的广泛应用使得汽车信息安全问题日益突出，如何保障车联网信息安全已成为亟待解决的问题。

SM4加密算法的优势

SM4是一种分组密码，具有安全性高、性能优良、易于实现等特点，适用于车联网等安全要求较高的场景。

车联网安全现状与挑战

01

安全现状

当前，车联网安全领域存在诸多挑战，如车载系统漏洞、通信协议缺陷、恶意攻击等，严重威胁着车联网系统的安全性和稳定性。

02

挑战一

车载系统漏洞：车载系统漏洞是车联网安全领域面临的主要挑战之一。攻击者可以利用这些漏洞，对车载系统进行非法访问和控制，从而窃取敏感信息或破坏系统功能。

03

挑战二

通信协议缺陷：车联网系统中使用的通信协议存在诸多缺陷，如缺乏加密机制、认证机制不完善等，容易被攻击者利用进行中间人攻击或重放攻击等。

04

挑战三

恶意攻击：恶意攻击是车联网安全领域面临的另一大挑战。攻击者可以通过伪造身份、篡改数据等方式对车联网系统进行攻击，造成系统瘫痪、数据泄露等严重后果。

02

SM4加密算法概述

SM4算法原理及特点

原理

SM4是一种分组密码，采用对称密钥加密方式，分组长度为128位，密钥长度也为128位。加密过程包括轮密钥加、字节替换、行移位和列混淆四个步骤，共进行32轮迭代。

运算速度快

SM4算法采用非线性替换和线性变换相结合的方式，具有较高的安全性，能够抵抗现有的各种密码攻击。

安全性高

SM4算法针对硬件和软件实现进行了优化，具有较高的运算速度，适用于各种实时性要求较高的应用场景。

易于实现

SM4算法结构简洁，易于在各种平台上实现，包括通用计算机、专用芯片和嵌入式系统等。

与其他加密算法比较

与AES比较

安全性：SM4与AES均采用分组密码体制，具有相似的安全性。但在某些特定攻击下，SM4可能表现出更高的安全性。

性能：在相同的硬件和软件环境下，SM4的加密和解密速度通常略低于AES。但在一些特定应用场景中，如低功耗设备或嵌入式系统，SM4可能具有更好的性能表现。

与DES比较

安全性：DES密钥长度较短（56位），容易受到暴力攻击。相比之下，SM4的128位密钥长度提供了更高的安全性。

性能：DES的加密和解密速度较慢，尤其在处理大量数据时性能瓶颈更为明显。而SM4则具有较高的运算速度，更适合处理大规模数据。

03

车联网中SM4加密算法应用

车载终端安全通信

数据加密传输

使用SM4加密算法对车载终端与服务器之间的通信数据进行加密，确保数据传输过程中的机密性和完整性。

防止重放攻击

引入SM4加密算法的时间戳机制，防止恶意攻击者截获并重复发送旧的数据包，确保通信过程的新鲜性和安全性。

身份认证与访问控制

结合SM4加密算法，实现车载终端与服务器之间的双向身份认证，确保只有授权的设备可以接入网络并访问相应资源。

远程故障诊断与升级

安全远程诊断

利用SM4加密算法对远程诊断过程中的数据进行加密，确保诊断数据的机密性和完整性，防止被恶意攻击者篡改或窃取。

安全远程升级

在远程升级过程中，使用SM4加密算法对升级文件进行加密传输和存储，确保升级文件不被篡改或窃取，保障车辆系统的安全性和稳定性。

防止中间人攻击

通过SM4加密算法的双向认证机制，确保远程故障诊断和升级过程中通信双方的身份真实性，防止中间人攻击。

车内网络安全防护

1 车内网络数据加密

应用SM4加密算法对车内网络中的关键数据进行加密处理，如CAN总线数据、传感器数据等，确保车内网络数据的机密性和完整性。

2 防止恶意攻击和篡改

通过SM4加密算法的强安全性，防止恶意攻击者截获并篡改车内网络中的关键数据，保障车辆的正常运行和乘客的安全。

3 安全存储与备份

利用SM4加密算法对车内网络中的关键数据进行安全存储和备份，确保数据在存储和传输过程中的安全性，防止数据泄露和丢失。