Software Engineering and Applications 软件工程与应用, 2025, 14(2), 280-290
Published Online April 2025 in Hans. https://www.hanspub.org/journal/sea
https://doi.org/10.12677/sea.2025.142026

Hans汉斯

基于风险评估的信息系统安全保密架构设计与实现

单伯瑜[1,2]，宋丽华[1]，崔又文[1,2]，高天昊[1]

[1]北方工业大学信息学院，北京
[2]文脉联坊(北京)科技有限责任公司，北京

收稿日期：2025年2月28日；录用日期：2025年4月9日；发布日期：2025年4月18日

摘　要

近年来，随着办公业务信息系统的广泛应用，系统中存储的涉密信息量日益增多。因此，对信息系统实施全方位、全流程、全要素的安全检测与分析显得尤为重要。通过提前识别潜在的安全隐患和风险窗口，可以有效预测可能遭遇的网络攻击路径和手段。基于此，本研究深入分析并识别网络攻击的关键环节，针对系统薄弱点进行安全措施的优化与改进，提出了一种多层次安全保密融合架构，从而实现对潜在威胁的全面防控。实验结果表明，该架构显著提升了系统的安全性能和应对复杂网络攻击的能力，通过加强安全与保密设计，进一步提升网络信息系统的整体防御能力。

关键词

风险评估，信息系统，涉密信息，安全隐患，安全措施，保密设计

Design and Implementation of Information System Security and Confidentiality Architecture Based on Risk Assessment

Boyu Shan[1,2], Lihua Song[1], Youwen Cui[1,2], Tianhao Gao[1]

[1]School of Information Science and Technology, North China University of Technology, Beijing
[2]Wenmai Lianfang (Beijing) Technology Co., Ltd., Beijing

Received: Feb. 28th, 2025; accepted: Apr. 9th, 2025; published: Apr. 18th, 2025

Abstract

In recent years, with the wide application of office business information system, the amount of

文章引用: 单伯瑜, 宋丽华, 崔又文, 高天昊. 基于风险评估的信息系统安全保密架构设计与实现[J]. 软件工程与应用, 2025, 14(2): 280-290. DOI: 10.12677/sea.2025.142026

classified information stored in the system is increasing. Therefore, it is particularly important to implement all-round, all-process, all-element security detection and analysis of the information system. By identifying potential security threats and risk windows in advance, the path and means of possible cyber attacks can be effectively predicted. Based on this, this study analyzes and identifies the key aspects of network attacks, optimizes and improves the security measures for the weak points of the system, and proposes a multi-level security and confidentiality fusion architecture to achieve comprehensive prevention and control of potential threats. Experimental results show that the architecture significantly improves the security performance of the system and the ability to cope with complex network attacks, and further enhances the overall defense capability of the network information system by strengthening the security and confidentiality design.

Keywords

Risk Assessment, Information System, Classified Information, Security Threats, Security Measures, Confidentiality Design

1. 引言

随着国内外计算机技术的迅猛发展，信息技术与相关产业呈现出前所未有的繁荣，各类信息的传播速度显著提升，资源在特定条件下实现了实时共享。信息化和计算机网络技术在政治、军事、金融、商业等领域的应用日益广泛，其作用愈发重要。尽管计算机技术的进步极大地推动了信息技术的发展，进而促进了社会生产力的提升，但与此同时，它也给信息系统网络的安全性带来了前所未有的挑战。

随着计算机病毒、黑客攻击、恶意软件的侵扰、计算机犯罪以及隐私泄露事件的频发，信息系统的安全面临严峻威胁。如果不能构建一个完善而可靠的信息系统网络安全保障体系，计算机网络中存储的敏感信息和数据的安全性将难以得到有效保障。因此，必须从多个角度深入分析信息系统可能存在的安全隐患，进而为制定科学、系统的网络安全防护措施提供理论基础。这不仅是确保信息系统安全与稳定运行的必要前提，也是维护社会经济秩序和个人隐私的重要举措[1]。

2. 问题分析

在当前办公业务信息系统中，用户数量庞大，并且随着新技术的不断应用及智能终端设备的多样化接入，信息系统的网络结构日益复杂，形态愈加多样化。在此背景下，单纯依赖传统的物理隔离手段，已无法充分保障信息系统中涉密数据的安全性。因此，信息系统的安全保密工作亟需从网络安全、计算环境安全、数据安全、应用安全以及安全管理等五个维度进行综合需求分析，以构建完善的网络防御体系，提升系统的抗攻击能力。

2.1. 网络安全保密需求

(1) 系统包含大量的终端、服务器、网络设备，网络架构复杂，仅依靠应用系统难以实现可靠的访问控制，因此需要对网络系统进行安全区域划分。

(2) 系统面向各单位日常办公提供服务，有大量的终端接入到系统中，为防止来自于内部的网络入侵和渗透攻击，阻止远程恶意破坏和越权访问等安全威胁，需要在终端办公区和核心交换区两个安全区域间实施网络边界防护措施。

(3) 系统依托虚拟专网与其他各单位互联，且部分终端部署于外部站点之内，为防止攻击者通过监听链路获取涉密信息，需要在跨站点链路上配备数据加密手段。

(4) 为防止非授权计算机接入网络，需要提供网络准入控制手段，实现对接入计算机的身份认证。

(5) 系统后台服务基于云平台架构，包括办公系统容器云平台以及集中管控系统的桌面云虚拟机，需要对云平台内部网络实施隔离，确保云平台的业务网、数据网、存储网之间逻辑隔离，并需要实现对虚拟服务器的网络访问进行有效的控制。

2.2. 计算环境安全保密需求

(1) 终端包括部署在各办公室的终端以及运行在服务器上的虚拟机或容器，各类计算机存在系统漏洞、病毒入侵、木马植入、蠕虫传播、非法入侵、数据外泄等安全威胁，需要采用可信防护、主机管控、漏洞扫描、补丁升级、恶意代码查杀等手段，加强操作系统对病毒及恶意代码的自我免疫能力，有效防止外部黑客攻击和内部人员违规操作、恶意破坏，实现计算环境的安全保密。

(2) 云计算平台需要进行不同容器之间的逻辑隔离，对容器之间进行访问控制。

(3) 各单位计算机终端分散部署，存在非授权用户非法访问计算机终端和系统的风险，需要实现对系统的授权访问控制。

2.3. 数据安全保密需求

数据安全访问：一是业务系统用户不能直接访问数据库；二是不能使用移动存储介质直接从服务器上复制数据；三是需要对数据库操作进行审计，及时发现潜在的威胁；四是对集中存储数据进行加密，防止数据被窃取[2]。

2.4. 应用安全保密需求

(1) 为了有效鉴别用户身份，集中管控、集中文印、办公云服务等应用需要使用单位公钥密码数字证书认证设备，对用户实施身份认证，基于认证结果对用户进行细粒度访问控制，确保系统用户身份的真实性，防止用户身份假冒、非法登录和越权访问；

(2) 为电子印章信息、手写签批信息提供数据签名验签手段，确保电子印章申请及使用过程的不可伪造性和不可否认性；

(3) 应用系统应对用户操作及办公流转过程进行安全审计，确保操作留痕，有迹可循；

(4) 针对 Web 应用访问，通过信息服务防护设备，提供应用层安全攻击的防护措施，避免泄露非授权数据信息及执行非法操作。

2.5. 安全保密管理需求

为了保证系统的正常运转和管理的高效及时，需要提供安全管理手段，确保用户能够对安全系统实施管理和维护。主要分为两个方面：一是对整个系统的密码设备以及密码设备所涉及的密码算法、密码参数、密钥等密码要素实施统一管理；二是需要对整个系统的安全设备所涉及的安全策略、安全规则等安全要素实施监控和管理，统一收集分析呈现安全设备的告警和日志等信息，并对安全事件进行分析和审计，通过对收集的各类信息进行关联分析、安全评估和行为回溯等，从而实现全方面的安全检测与管理[3]。

3. 安全保密系统设计

3.1. 安全保密设计思路

安全保密系统的设计应遵循办公和业务系统安全保密技术体制，按照“统一体制、互连互通、合理

防护、利于管控”的原则，提供专用的安全保密保障。安全保密系统从物理安全、网络安全保密、计算环境安全保密、数据安全保密、应用安全保密以及安全保密管理等多个维度进行设计。

在进行安全保密系统设计时应从以下几个方面出发：

(1) 建设全方位的安全保密防护

针对办公业务信息系统的整体建设内容，设计涵盖网络安全保密、计算环境安全保密、数据安全保密、应用安全保密等多个维度的安全保密体系，建设安全的网络环境、计算环境、数据共享环境和应用运行环境，确保能够达到安全防护要求。

(2) 提高安全保密系统的整体性能和可靠性

诸如防火墙、网络密码机、信息服务可信防护设备、UTM 安全网关等安全设备需要串接在通信链路中，安全保密设备的处理能力和可靠性极大地影响和制约着链路的性能和稳定性。因此，安全保密设备的部署需要考虑到高可靠性的支持，诸如利用双机热备、配置同步、关键部件冗余、链路聚合等设置，提高安全设备的可靠性。

(3) 建设集中的运维管理体制针对整系统安全设备种类和数量众多的问题，部署网络安全管理与态势分析系统和安全审计软件，通过与各类安全设备进行接口对接，实现对全网安全设备的统一管理、参数配置、状态监控和行为审计，便于运维人员进行日常管理。

3.2. 安全保密体系架构

为满足机关办公业务信息系统建设安全保密要求，针对网络、计算环境、应用、数据等不同类型的安全保密对象，设计由安全保密装备、安全保密服务、安全保密应用对象和安全保密管理组成的安全保密体系架构。机关办公业务信息系统安全保密建设体系如图 1 所示。

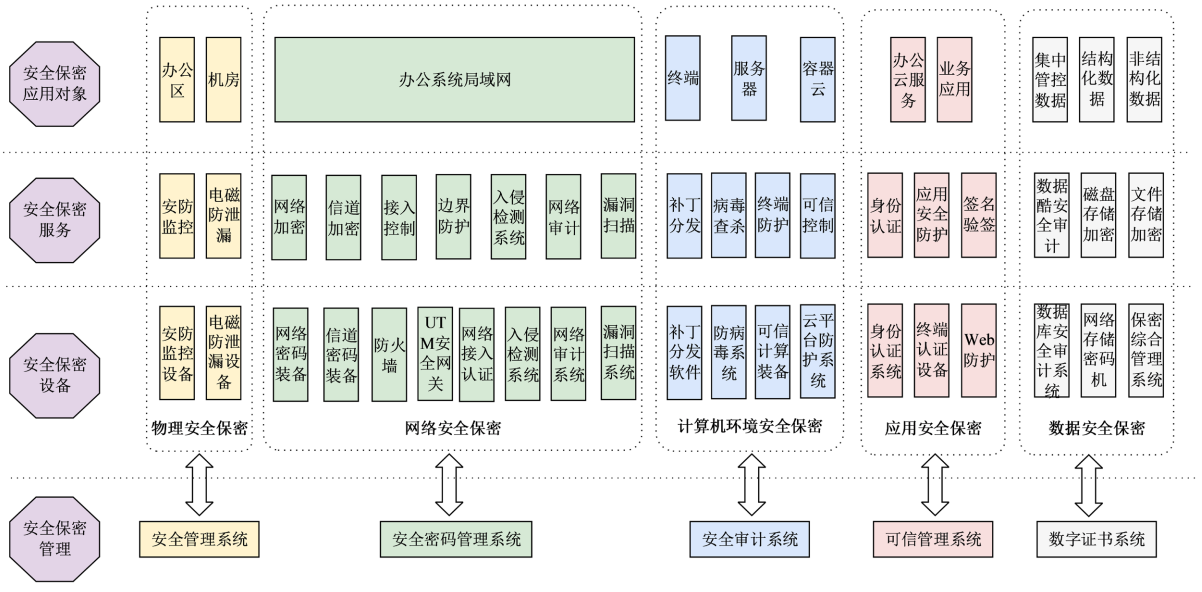

Figure 1. Security architecture diagram
图 1. 安全保密架构图

(1) 物理安全保密

各单位依托现有机房基础设施，为办公系统提供基础环境和物理设备的安全保护。设备机房应安装安防监控系统、配套消防设施、铺设防静电地板，满足基础环境要求；设置门禁、独立设备柜，防止非授

权人员随意进入，保护机房内部的设备安全。应具备空调监控、门禁系统、设备故障告警、消防系统、防电磁辐射相关的措施和设备。

(2) 网络安全保密

网络安全保密建设中主要包括安全准入控制、网络访问控制、网络结构安全三方面。

对于局域网延伸接入的站点，在网络出口部署网络密码机，防止 IP 被监视、追踪，实现网络流量加密功能；部署信道密码机，防止信道监听窃密，实现信道加密功能。

在本级边界部署防火墙设备，构建 ACL 策略，控制流量的通过或阻挡，以实现网络访问控制功能；部署入侵检测设备，监听进出交换机流量、记录攻击源 IP 地址和端口，对边界数据流量进行检测预警；在其他单位站点出口处部署 UTM 安全网关设备，实现对进出网络流量的报文进行访问控制、入侵防御和病毒检测；部署局域网接入鉴权设备，结合支持 802.1X 协议的交换机，完成主机局域网准入控制，实现对用户终端计算机的入网认证，防范非授权主机接入网络；部署漏洞扫描系统，实现对网络设备、计算环境等的漏洞扫描和发现。针对局域网接入的站点部署 UTM 安全网关，集成防火墙、入侵检测功能，实现对进出网络流量的报文进行访问控制、入侵防御和病毒检测，实施统一安全防护。

(3) 计算环境安全保密

在终端计算机和服务器安装网络防病毒客户端软件，配合后台管理端软件实现病毒查杀功能。

部署保密综合管理系统，为用户提供安全可靠的终端运行环境及主机状态信息监控功能。

部署可信计算防护设备，支持主机开机启动时的可信度量控制。主机可信管理系统保护客户端和服务端，服务端部署在安全服务器中，连接至安全接入交换机，客户端部署在计算终端上，实现对用户终端计算环境的可信安全管理。

(4) 应用安全保密

在用户终端部署身份认证设备，实现单位数字证书认证；在后台服务端，通过部署身份认证服务器、电子签名服务器提供动态口令验证、数字签名验签等服务，为上层应用提供统一认证服务，在后台服务网络出口部署信息服务可信防护设备等 WEB 防护装备，有效检测并阻断针对应用服务的各种攻击。

(5) 数据安全保密

通过数据库安全审计系统，能够分析和详细记录应用和各类工具对数据库的访问行为，对数据库资源违规访问进行告警。

针对信息服务中心和信息服务节点的各类办公应用数据存储需求，通过部署网络存储密码机，为系统中存储的结构化数据、非结构化数据提供存储加密服务。

通过保密综合管理系统，整合终端管控、标签管理、集中管控、集中文印等功能，实现涉密计算机管控、涉密文件全生命周期管理、电子文件集中加密存储，以及文件打印、复印、刻录等系统全方位的安全保密管控。

(6) 安全保密管理

通过安全管理系统、安全审计系统实现对全网安全设备的安全管理和安全审计。通过密码管理系统、可信计算综合管理系统和数字证书系统，实现对全网密码装备的设备管理、密码资源管理、可信管理和证书管理。

3.3. 安全保密设备组成

通过安全保密设备的合理配置，密码装备与安全防护设备相结合，形成最终的安全保密系统配置方案。其中密码装备(网络密码机、信道密码机、存储密码机等)应选用相关部门通用密码装备，遵循统一技术体制；身份认证系统应选用相关部门专用密码装备，遵循相关部门的统一身份认证体系；安全防护设

备应通过安全测评认证中心测评认证。

所选的安全保密设备，应与国产化自主软硬件平台、应用系统等进行充分的集成联式适配，测试通过后方可建设实施。安全保密组成如图 2 所示。

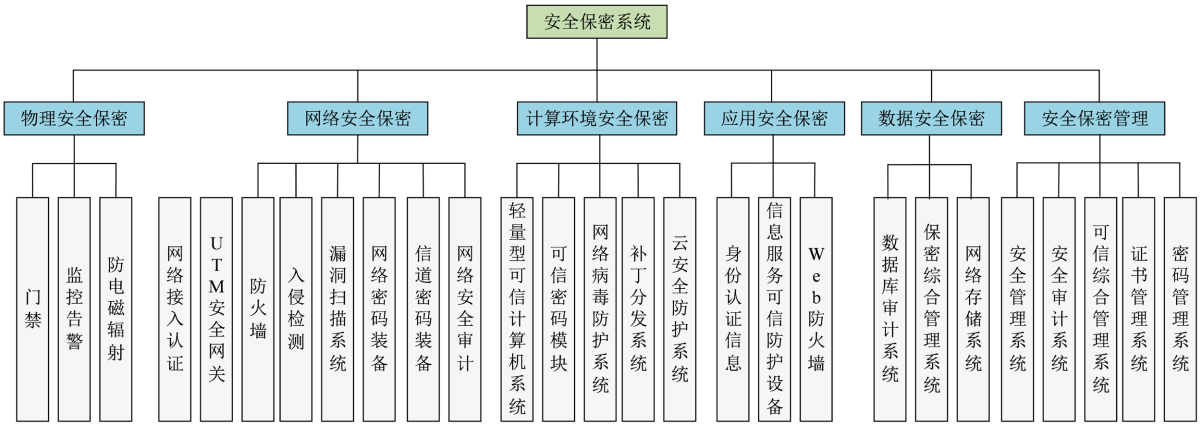

Figure 2. Components of the security system
图 2. 安全保密系统组成

3.4. 安全保密系统设计

3.4.1. 物理安全保密子系统

物理安全保密防护依托各单位数据机房基础设施，为办公信息系统提供基础环境和物理设备的安全保护。主要包括门禁系统、设备故障告警、消防系统、防电磁辐射等相关措施。

系统应配套监控设施对机房的人员进出、设备操作等进行监管；应配套模块化冷通道机柜来保证机房的温度和湿度，模块化冷通道机柜中的制冷系统用来调节机房的温度和湿度，确保机房符合 GB 2887-2011 中 4.6.1 所规定的温湿度等要求。

3.4.2. 网络安全保密子系统

网络安全保密子系统由防火墙、入侵检测设备、漏洞扫描系统、网络接入认证设备、网络密码机、信道加密机、网络安全审计组成[4]。

(1) 防火墙

防火墙就是设置在不同网络或网络信任域与非信任域之间的一系列功能部件的组合设备，一般部署在内网对外的网络接口上，是内部网络的唯一对外出口，提供网络边界防护功能，对进出的网络流量进行基于五元组的包过滤，能够对通用应用协议进行检查和控制，能够抵御常见网络攻击，负责内网和外网之间的访问控制。防火墙部署如图 3 所示。

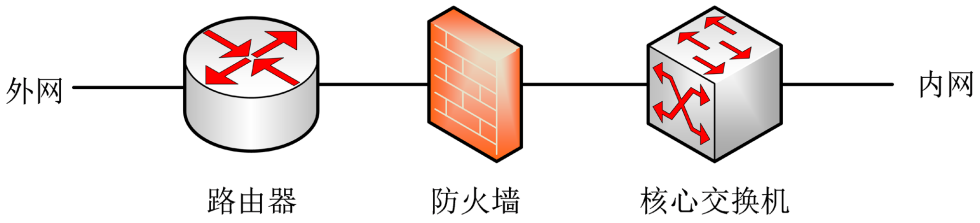

Figure 3. Firewall deployment diagram
图 3. 防火墙部署图

(2) 入侵检测设备

入侵检测，是检测计算机网络和系统发现违反安全策略事件的过程，它通过在计算机网络或计算机系统中的若干关键点收集信息并对收集到的信息进行分析，从而判断网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测一般过程是：信息收集、数据预处理、数据的检测分析、根据安全策略做出响应。入侵检测设备部署如图 4 所示。

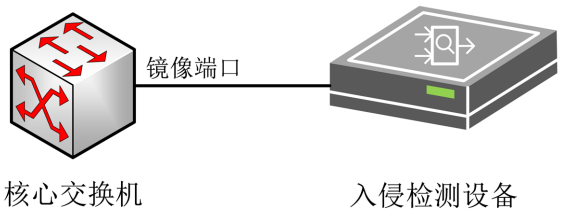

Figure 4. Intrusion detection equipment deployment diagram
图 4. 入侵检测设备部署图

(3) 漏洞扫描系统

漏洞扫描系统是网络安全防御中的一项重要技术，其原理是根据已知的安全漏洞知识库，对扫描的目标可能存在的安全隐患进行模拟攻击，及时发现主机存在的漏洞和安全隐患，从风险管理角度出发，科学分析网络信息系统的安全需求，提供专业、有效的安全分析和修复建议，将风险控制在可接受的程度，为最大限度地保障网络和信息安全提供科学依据。漏洞扫描设备部署如图 5 所示。

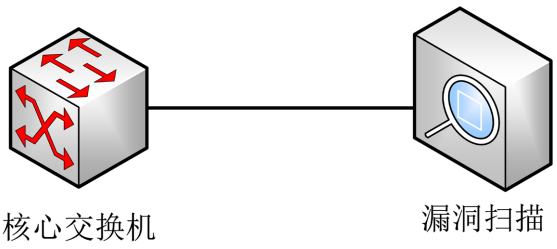

Figure 5. Intrusion detection appliance deployment diagram
图 5. 入侵检测设备部署图

(4) 网络安全审计系统

网络安全审计系统能够通过主被动结合的手段，实时不间断地采集用户网络中安全设备、网络设备等产生的日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，并出具丰富的报表报告，获悉全网的整体安全运行态势，实现全生命周期的日志管理。网络安全审计设备部署如图 6 所示。

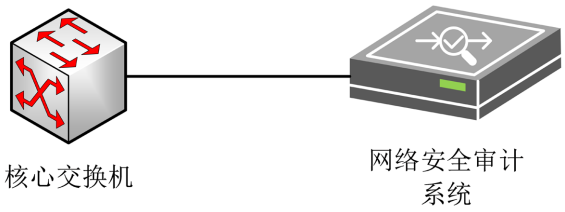

Figure 6. Network security audit system deployment diagram
图 6. 网络安全审计系统部署图

(5) 网络接入认证

网络接入认证设备主要部署于有安全接入风险的用户网络节点。网络接入认证设备负责对网络接入认证代理软件发送的主机入网请求进行响应，验证入网主用户身份和设备平台身份、特征信息和安全状态，基于认证和授权结果，结合支持 802.1X 交换机实施端口控制，解决局域网内部主机的准入控制问题，并能对入网主机在线状态和非法主机接入行为进行实时监控和综合统计。同时提供日志审计功能，支持对管理员操作、用户访问行为的日志记录，可按要求向安全审计系统上报信息。网络接入认证部署如图 7 所示。

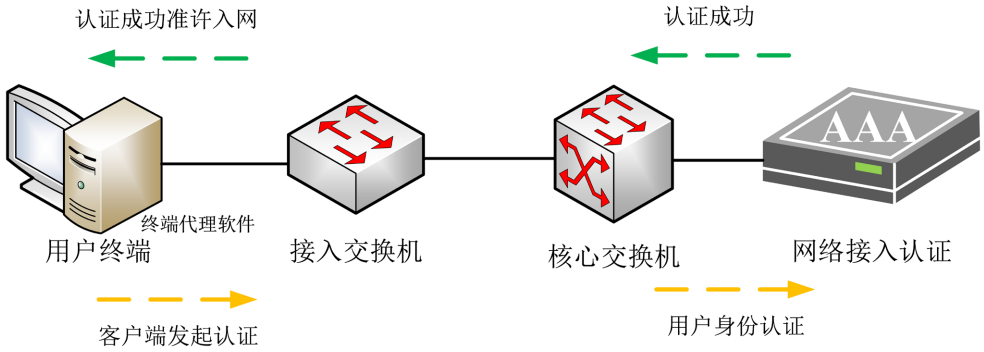

Figure 7. Network security audit system deployment diagram
图 7. 网络安全审计系统部署图

(6) 传输加密

局域网延伸单位网络出口处部署网络密码机和信道加密机，用于局域网延伸单位远程互联，为远程互联的数据提供网络加密和传输加密保护。传输加密设备部署如图 8 所示。

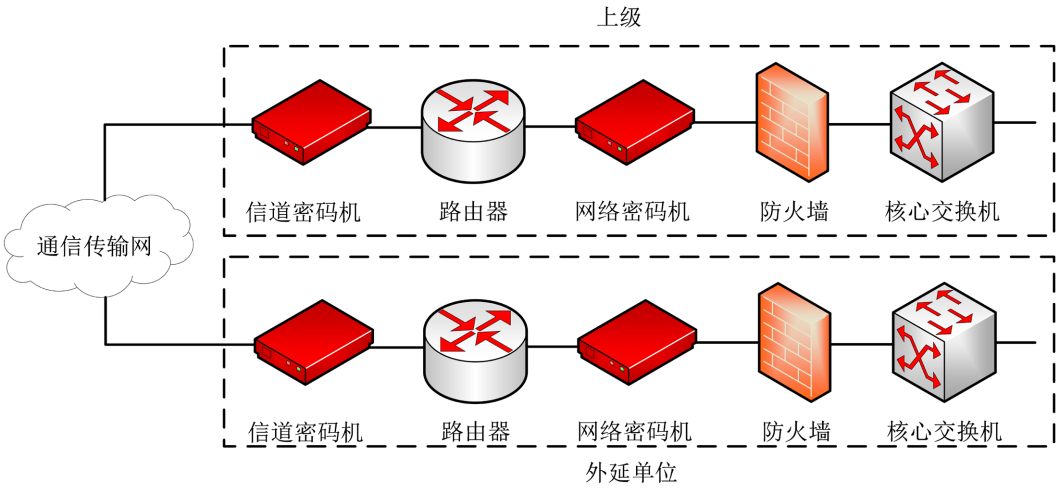

Figure 8. Transmission encryption device deployment diagram
图 8. 传输加密设备部署图

3.4.3. 计算环境安全保密子系统

计算环境安全保密子系统由网络防病毒防护系统、可信密码模块、轻量型可信计算系统、补丁分发系统、云安全防护系统组成[5]。

(1) 网络病毒防护系统

网络防病毒是计算机安全的一项基础技术，是目前应用最广泛的安全附加技术。病毒防护系统通过建立一个病毒特征数据库，监控系统是否匹配表明病毒感染的特征，能够实时检测和拦截攻击行为，并能对系统中存在的恶意程序进行有效的识别和查杀。所有好的防病毒系统都有清除受感染文件病毒的能力，或者通过隔离文件使其不再造成进一步破坏。

(2) 可信密码模块

为国产自主可控计算机配备可信密码模块，可信密码模块与计算终端在固件、操作系统方面进行集成适配，实现终端可信运行，为终端计算机提供可信计算防护，提供登录认证、可信白名单、文件访问控制等可信安全增强和主机管控功能。

(3) 轻量型可信计算系统

终端计算机部署轻量型军用可信计算系统，该系统为单机版，单机模式运行，对可执行程序进行可信验证，阻止非法程序启动。

(4) 补丁分发

网络防病毒系统包含补丁分发系统功能，可实现对全网服务器及计算机的集中管控、补丁策略制定、补丁自动分发。

(5) 云安全防护系统

云安全防护系统提供容器镜像漏洞扫描和容器的微隔离能力，防止不安全的容器镜像被加载运行和容器之间恶意代码传播、跳板攻击等网络攻击行为，保护整个容器云的安全运行。

3.4.4. 数据安全保密子系统

数据安全保密子系统由数据库审计系统、保密综合管理系统、网络存储密码机组成[6]。

(1) 数据库审计系统

分析不同应用访问关系型数据库和分布式大数据平台的方式、行为和主要特征，并进行深度学习，实时监测访问数据库所有行为、智能识别数据库高危操作；智能分析数据访问偏好和规律，展现用户数据访问规律图谱，发现数据资源价值，预警潜在风险；发现热点业务数据，呈现敏感数据关注分布；提供可视、合规的审计日志和事件回放功能，为数据资源访问安全事件提供快速响应和取证支撑。采用数据智能感知变化、数据智能分发、数据路由智能选择，快速构建高速任务交互矩阵，提供异构静态、增量数据的抽取、转换、同步整合与数据交换任务实时和按计划执行能力。

(2) 保密综合管理系统

保密综合管理系统主要用于解决未经允许随意安装计算机应用程序或非法接入行为导致网络感染病毒和网络泄密的情况。该系统可以为主机、服务器等终端设备提供身份识别和登录控制等安全功能，可以对终端、服务器的在线状况、违规接入、非法外联、外设拷贝和网络访问等行为进行安全监控和审计。

(3) 网络存储密码机

网络存储密码机分组做集群。第一组集群为办公业务数据提供 SAN 磁盘存储加密服务；第二组集群为终端用户集中管控数据提供 NAS 文件存储加密和访问控制服务；第三组集群用于集中管控存储密码机，为 FC 存储提供结构化数据、非结构化数据、历史归档数据加密存储能力。

3.4.5. 应用安全保密子系统

应用安全保密子系统由身份认证系统、信息服务可信防护、Web 防火墙设备组成。

(1) 身份认证系统集成设计

部署身份认证系统，主要包括用户身份识别设备(含接口密码模块)、用户身份令牌、用户身份标识管

理系统、认证服务代理软件、密码模块批量制证套件和身份认证服务器。

(2) 信息服务可信防护设备

信息服务防护设备主要提供用户访问应用系统的统一身份认证、集中授权、应用访问控制、抵御各类应用层攻击等功能，实现用户受控访问信息服务和受控获取网上资源。

(3) Web 防火墙

Web 防火墙对信息系统进出的流量进行过滤，通过镜像流量的方式对访问 Web 系统的流量进行检测，同时对 HTTP 的请求进行异常检测，拒绝不符合 HTTP 标准的请求，只允许 HTTP 协议的部分选项通过，从而减少攻击的影响范围，有效防止网页篡改、信息泄露、木马植入等恶意网络入侵行为，如有检测到异常并及时发出警告。

3.4.6. 安全管理保密子系统

安全保密管理子系统用于提供网络统一安全管理能力，实现安全管理功能，保障安全保密系统的正常运转和管理的高效及时。

安全保密管理子系统主要由安全管理与态势分析系统、安全审计系统、可信计算综合管理系统、公共普通密码管理软件系统、证书和密码管理系统组成。

(1) 安全管理系统

安全管理软件支持设备集中配置，终端集中管控；支持拓扑管理，能够半自动绘制生成网络拓扑图和安全管理级联关系；支持资产管理质量评估，运行监控质量评估，值班管理质量评估，运维质量综合评价，运维质量监察。支持安全策略预置，支持网络安全设备策略模板功能。

(2) 安全审计系统

安全审计系统通过数据的采集、分析、识别，实时动态监测通信内容、行为和流量，发现和捕获各种敏感信息、违规行为，实时报警响应，全面记录系统中的各种会话和事件，实现对信息的智能关联分析、评估，并可作为电子证据实现责任认定。

(3) 可信计算综合管理系统

可信计算综合管理系统通过安装公共普通密码管理软件来管理可信密码模块，对可信计算平台实施密码资源、数字证书以及安全策略的管理。在线或离线接收一体化对称密码管理系统分发的可信计算平台的设备注册信息和密钥，离线接收数字证书认证系统分发的证书和私钥；为可信计算平台及用户装配密钥，支持在线分发和更换密钥及证书。

(4) 证书管理系统

电子签名服务器、用户身份识别设备、接口密码模块、认证服务器、用户身份令牌、用户身份标识管理系统等采用相关部门数字证书，依托公钥密码基础设施，由数字证书认证系统为各类密码设备和用户颁发数字证书，并对数字证书进行更新、撤销和恢复等管理工作。

(5) 密码管理系统

网络密码机通过栅格化密码管理基础设施，采用分级保障模式，实施离线密钥保障。

4. 结束语

通过对办公信息系统的业务活动和信息流转的全面分析，本文结合信息系统安全保密建设的实际需求，从多个角度与维度出发，深入探讨了办公信息系统的安全保密设计与实现策略。旨在通过有效的预防措施，减少信息泄露风险，确保信息系统符合“受控互联、安全隔离、分群保护”的安全策略。本文提出的安全保密体系构建方案，能够实现符合相应防护等级的网络安全保障标准，从而保障信息系统的安全稳定运行，为信息系统计算机网络的长期健康发展提供有力支持[7]。

基金项目

大学生创新创业训练计划课题(2025)；北方工业大学教育教学改革项目。

参考文献

[1] 张焕国, 韩文报, 来学嘉, 等. 网络空间安全综述[J]. 中国科学:信息科学, 2016, 46(2): 125-164.

[2] 刘孟栋. 数据加密技术在计算机网络安全中的应用价值评价[J]. 现代工业经济和信息化, 2022, 12(9): 82-84.

[3] 付圣. 论计算机网络安全问题及其防范措施[J]. 软件, 2022, 43(6): 124-126.

[4] Lau, P., Wei, W., Wang, L., *et al*. (2020) A Cybersecurity Insurance Model for Power System Reliability Considering Optimal Defense Resource Allocation. *IEEE Transactions on Smart Grid*, **11**, 4403-4414.

[5] 徐琳娜. 大数据时代下计算机网络安全与防范措施分析[J]. 信息与电脑(理论版), 2024, 36(11): 180-182.

[6] Kaur, H., Jameel, R., Alam, A.M., *et al*. (2023) Securing and Managing Healthcare Data Generated by Intelligent Blockchain Systems on Cloud Networks through DNA Cryptography. *Journal of Enterprise Information Management*, **36**, 861-878.

[7] 杨志祥. 计算机信息安全技术在网络安全管理中的应用[J]. 电脑知识与技术, 2024, 20(30): 91-93+96.