国 际 电 信 联 盟

# ITU-T X.1157

(09/2015)

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务 – 安全协议

# 欺诈检测的技术能力以及可满足高可信度要求的服务应答

ITU-T X.1157 建议书

国际电信联盟

ITU-T X 系列建议书

**数据网、开放系统通信和安全性**

| | |
|---|---|
| 公用数据网 | X.1–X.199 |
| 开放系统互连 | X.200–X.299 |
| 网间互通 | X.300–X.399 |
| 报文处理系统 | X.400–X.499 |
| 号码簿 | X.500–X.599 |
| OSI组网和系统概貌 | X.600–X.699 |
| OSI管理 | X.700–X.799 |
| 安全 | X.800–X.849 |
| OSI应用 | X.850–X.899 |
| 开放分布式处理 | X.900–X.999 |
| 信息和网络安全 | |
| 一般安全问题 | X.1000–X.1029 |
| 网络安全 | X.1030–X.1049 |
| 安全管理 | X.1050–X.1069 |
| 生物测定 | X.1080–X.1099 |
| 安全应用和服务 | |
| 组播安全 | X.1100–X.1109 |
| 家庭网络安全 | X.1110–X.1119 |
| 移动安全 | X.1120–X.1139 |
| 网页安全 | X.1140–X.1149 |
| **安全协议** | **X.1150–X.1159** |
| 对等网络安全 | X.1160–X.1169 |
| 网络身份安全 | X.1170–X.1179 |
| PITV安全 | X.1180–X.1199 |
| 网络空间安全 | |
| 计算网络安全 | X.1200–X.1229 |
| 反垃圾信息 | X.1230–X.1249 |
| 身份管理 | X.1250–X.1279 |
| 安全应用和服务 | |
| 应急通信 | X.1300–X.1309 |
| 泛在传感器网络安全 | X.1310–X.1339 |
| PKI相关建议书 | X.1340–X.1349 |
| 网络安全信息交换 | |
| 网络安全综述 | X.1500–X.1519 |
| 脆弱性/状态信息交换 | X.1520–X.1539 |
| 事件/事故/探索法信息交换 | X.1540–X.1549 |
| 政策的交换 | X.1550–X.1559 |
| 探索法和信息要求 | X.1560–X.1569 |
| 标示和发现 | X.1570–X.1579 |
| 确保交换 | X.1580–X.1589 |
| 云计算安全 | |
| 云计算安全综述 | X.1600–X.1601 |
| 云计算安全设计 | X.1602–X.1639 |
| 云计算安全最佳实践和指导原则 | X.1640–X.1659 |
| 云计算安全实现 | X.1660–X.1679 |
| 其他云计算安全 | X.1680–X.1699 |

欲了解更详细信息，请查阅ITU-T建议书目录。

**ITU-T X.1157 建议书**

# 欺诈检测的技术能力以及可满足高可信度要求的服务应答


## 摘要

ITU-I X.1157建议书为安全敏感的信息通讯技术（ICT）应用服务提供支持欺诈检测和响应所需的能力。欺诈检测和响应服务支持覆盖用户，账户，产品，流程和渠道的欺诈检测、分析和管理。它监控和分析在应用层面（而非系统，数据库和网络层面）的客户活动和行为，并利用提供给用户的任何渠道来观察账户内部和整体发生的情况。它还可以分析相关用户，账户和其他实体之间的行为，查找异常，贪污或滥用活动。这是垂直机构开展电子金融、企业远程接入等客户资金管理中最常见的应用，而它们也通常用于检测内部欺诈和其他类型未经授权的活动。



## 沿革

| 版本 | 建议书 | 批准日期 | 研究组 | 识别码* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1157 | 2015-09-17 | 17 | 11.1002/1000/12353 |

## 关键词

欺诈检测系统，欺诈管理。


* 访问建议书，请在您的Web浏览器地址栏中输入网址http://handle.itu.int/，其次建议书的识别码，例如http://handle.itu.int/11.1002/1000/11830-en。

## 前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）在电信，信息和通讯技术领域是国际电信联盟的常设机构。国际电信联盟电信标准化部门负责研究技术，操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

世界电信标准化大会（WTSA），每四年举行一次，确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第一号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

## 注

本建议书为简明扼要起见而使用的的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性和适应性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

## 知识产权

国际电联提醒注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适应性不表示意见。

至本建议书截止之日起，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新消息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

# 目录


页码

1 范围 ..... 1

2 参考文献 ..... 1

3 定义 ..... 1

3.1 别处术语定义 ..... 1

3.2 本建议书术语定义 ..... 2

4 缩写词和首字母缩略语 ..... 2

5 惯例 ..... 3

6 欺诈检测和应答概况 ..... 3

6.1 问题陈述 ..... 3

6.2 欺诈管理的作用 ..... 4

6.3 欺诈管理的主要能力 ..... 4

7 欺诈管理和应答系统的体系结构 ..... 5

7.1 操作和组成部件 ..... 5

7.2 体系结构方面的考虑 ..... 6

8 欺诈检测和响应技术能力 ..... 7

8.1 监控能力 ..... 7

8.2 检测能力 ..... 10

8.3 应答能力 ..... 15

附录I – 敏感ICT应用服务 ..... 18

I.1 电子金融服务 ..... 18

I.2 电子医疗服务 ..... 19

I.3 企业远程接入服务 ..... 19

参考资料 ..... 22

# ITU-T X.1157 建议书

## 欺诈检测的技术能力以及可满足高可信度要求的服务应答

## 1 范围

本建议书在高保证要求服务中欺诈管理技术能力上提供了指导原则。本建议书旨在提供一个能够检测欺诈活动的系统。本建议书适用于通过欺诈检测和应答系统的部署使用安全敏感信息和通讯技术（ICT）应用程序的商业和企业部门。它也适用于一个机构内部和外部网络欺诈管理，通过远程访问和商业服务。此建议书包括以下几点：

– 欺诈检测和应答服务的能力；

– 欺诈检测和应答系统的操作和组成部件；

– 事件防御和应答服务的注意事项。

## 2 参考文献

无。

## 3 定义

### 3.1 别处术语定义

此建议书用到以下别处术语定义：

**3.1.1 保证水平 assurance level** [b-ITU-T X.1252]：表明对实体和所介绍的身份信息之间关联性的置信程度的量化表示。

**3.1.2 （实体）认证 (entity) authentication** [b-ITU-T X.1252]：对实体和所介绍身份之间关联性实现充足信任的过程

注 — 在身份管理（IdM）语境中，使用术语认证是指实体认证。

**3.1.3 认证保证 authentication assurance** [b-ITU-T X.1252]：是声称或预期为沟通伙伴的实体，在认证过程中实现的信任度。

注 — 信任是基于在沟通实体和显示的身份之间绑定的信任程度

**3.1.4 终端用户 end user** [b-ITU-T X.1141]：为了应用程序目的使用资源的自然人

**3.1.5 身份 identity** [b-ITU-T X.1252]：以一个或多个信息元素表示实体，使实体足以在语境内得到区分。至于身份管理（IdM）的目的，术语身份可以被理解为语境下的身份（属性的子集）即，属性的多样性受限于实体存在和互动的边界条件（语境）的框架。

注 – 各实体通过一个综合身份表示，它包括所有描述这类实体（属性）的可能信息元素。然而，这种综合身份是一个理论问题，不包括任何描述和实用情况，可能的属性数量是无限的。

**3.1.6 身份保证 identity assurance** [b-ITU-T X.1252]：用来确定获得证书的实体身份的身份认证过程中的信任程度以及对有关使用该证书的实体就是证书被颁发或分配的实体的信任程度。

**3.1.7 身份证明identity proofing** [b-ITU-T X.1252]：充分验证和核实信息来确认实体的声称身份的过程。

**3.1.8 身份认证 identity verification** [b-ITU-T X.1252]：通过以往经认证的信息比较所提供的身份声明确认声称身份的过程。

**3.1.9 服务提供者service provider** [b-ITU-T X.1141]：由系统实体赋予的角色，系统实体向委托人或其他实体提供服务。

## 3.2 此建议书的术语定义

此建议书用到以下术语：

**3.2.1 欺诈检测系统**：支持监控，检测和欺诈管理的应用软件或者通过用户（例如，客户），账户，渠道，产品或其他实体（例如，电话亭）的滥用。

注 – 若部署欺诈检测系统，企业应用程序可以与能够评估交易欺诈风险的欺诈检测工具结合，通过用户导航和应用程序访问，任何类型的活动，例如地址的更换，付款或敏感信息的检索。

**3.2.2 欺诈管理**：一系列的活动，包括早期预警系统，迹象和不同类型的欺诈，用户的个人档案和他们的活动，事件响应等，以减轻使用欺诈检测系统的安全风险。

注 – 开发欺诈管理系统必备的一些问题包括：巨大的数据量，不会造成业务不便的快速精确的欺诈检测要求；摆脱现有技术不间断的进行新欺诈的开发；和错误警报的风险。

**3.2.3 安全敏感信息和通讯技术（ICT）应用程序**：A要求非常高的安全保证级别的应用程序，为保护个人，私密信息，组织，和/或企业的信息资产。

注 – 当安全敏感信息ICT应用程序被攻击者妥协和控制，敏感信息的曝光，即，个人或财务信息，会对客户，组织，电信基础设施和服务造成巨大的不良影响，其中可能包括电子金融，电子医疗和企业远程访问应用程序。

# 4 缩写词和首字母缩略语

本建议书用到以下缩写词和字母缩略语：

API 应用编程接口

ATM 自动柜员机

DLP 数据外泄防护

DNS 域名系统

DSL 数字用户线路

GSM 全球移动通讯系统

HTTP 超文本传送协议

ICT 信息和通讯技术

ID 身份

IP 互联网协议

IPS 入侵防御系统

ISP 互联网服务提供商

IT 信息技术

MITM 中间人

NAC 网络访问控制

OS 操作系统

PC 个人计算机

PIN 个人识别码

SMS 短消息服务

SP 服务提供者

SQL 结构化查询语言

SSL 安全套接层

TAN 验证码

WiMAX 全球微波接入互操作性

## 5 惯例

“需要”一词指的是必须严格遵守的要求，要声明与本建议书一致就不得偏离这种要求。

“建议”这个词表示一种建议，但不是必须的要求。因此，因此在声明一致性时本建议书不用提及这种要求。

“禁止”一词指的是必须严格遵守的要求，要声明与本建议书一致就不得偏离这种要求。

“可选”字样表明一个可选的要求是被允许的，不意味着任何被建议的意思。该术语并不意味着供应商必须实施这一选项，是否启用这一特性可由网络运营商/服务提供商任选；而是指供应商可以视情选择提供这一特性，同时仍然声明与本建议书一致。

## 6 欺诈检测和应答概况

### 6.1 问题陈述

在通讯基础应用程序服务中，在许多类型的企业和垂直行业中（例如，电子运输，电子医院和其他类型的电子行业），恶意软件的攻击一直负责有针对性的攻击。这些攻击正成为一个主要关注的问题，并且通过针对性的钓鱼邮件和恶意软件感染对象越来越多地来实施，例如没有经验的用户点击的广告。这些方法曾被用来感染许多组织。

许多商业和企业部门的组织面临着数据丢失，不恰当的账户访问，和来自内部和外部资源交易活动的重大风险。针对性的恶意软件经常能够绕道现有保护技术，造成数据泄露直到很长时间以后才被检测到，并且引起重大数据泄露发生。恶意活动的迹象常常隐藏在普通的

场景中，并且由于监控能力的缺失和无法识别异常应用程序活动或正常活动类型中的数据访问导致不被检测到。例如，银行客户直到他们在其信用报告中看到一个未经确认的账户时，或者直至债务征收员因支付问题而联系他们时，才意识到问题的发生。

恶意软件对金融客户和公司员工的攻击对受害人的声誉和财务造成严重的损失。它们正在迅速成为攻击客户和公司账户，窃取敏感信息或资金的普遍工具。因此，除非业务流程和组织正常结构化，可以有效管理欺诈检测，才可以忽略重要的警告和提醒。最后，恶意软件的攻击可能被用来接管用户的账户，欺诈或窃取基于服务器的资产。

## 6.2 欺诈管理的作用

一个欺诈管理系统可被应用于三个典型欺诈实例中：

- 检测账户接管，通常发生在用户账户证书通过恶意软件被盗。恶意软件不仅通过入侵邮箱附带的文件，而且仅通过已入侵的网页被访问就能入侵企业计算机系统。
- 检测新账户欺诈，通常发生在用户账户证书被恶意软件盗取。
- 检测被盗（或其他的）账户，例如，假装一个正常用户用被盗信用卡购物。

一个欺诈管理系统通常用于一个或更多欺诈实例，例如账户接管，内部欺诈检测，实时支付卡欺诈检测和交易拦截，并且作为企业的特定欺诈或滥用管理系统。在每种情况中，它主要服务于企业的交易，来验证该人进行交易的合法性。

## 6.3 欺诈管理的主要功能

当谈到全面对抗身份欺诈，欺诈检测系统需要坚持三个能力来处理这个问题：监控，检测和事件应答。这些能力包括：首先，采取措施，为了从各种事件数据中发现可疑活动；当可疑活动发生时尽早检测欺诈； 如果可疑活动被检测出来采取措施解决欺诈。

**监控**：欺诈检测系统能在应用程序级，和系统，数据库或网络级中通过寻找客户活动和行为中的异常现象来监控欺诈，并且能用任何可用通道观察账户内和跨账户发生了什么，并提供给用户。它也能通过使用规则或统计模型监控和分析用户或账户行为和相关的交易并且识别异常行为。它也能（最优）利用用户和账户不断更新的配置文件和同位体组来比较交易和识别可疑行为。尤其，全面的内部欺诈监控需要可以直接修改文件和数据的特权信息技术（IT）用户的监控，而不是普通用户的应用程序。

**检测**：欺诈检测系统能够通过使用复杂的关系和由业务定义的规则筛选来挖掘，剖析和分析数据来预防欺诈。它可以用于内部人（即，员工）和外部人（即，客户和业务合作伙伴）的欺诈检测。对于欺诈检测能力，它能并且应该扼要描述各种实体，如用户，账户，家庭，个人计算机（PCs),手机和报停，从该实体交易中识别异常行为。欺诈检测使用基于人类判断和认知和/或预测数学模型的基本原则政策来获得一个给定事物欺诈的可能性。

**应答**：在检测可疑活动之后，欺诈管理系统应该用各种预防措施来回应可疑活动，例如账户冻结或信息共享。各种补充的监控和检测技术能够帮助企业更好地检测可疑用户的活动，识别不恰当资源访问和欺骗性的账户活动的类型，并且用实时警告，事件管理，账户冻结或交易妨碍来调查和回应事件。因此，组织需要决定哪种监控和分析技术的结合对他们的风险等级是最合适的，并确定他们安全技术的实现和支持能力。

# 7 欺诈管理和应答系统的体系结构

## 7.1 操作和组成部件

ICT应用程序可与欺诈检测组成部件集成，以支持从用户访问到任何类型活动管理交易欺诈风险的主要功能。对于黑客和用户，欺诈检测系统的操作应该是不透明的，因此黑客不能学到系统的规则，而且不会给合法用户带来不便。在对用户交易产生怀疑的情况下，实时地对其进行重新验证，利用欺诈检测系统对其合法性进行评估，或者暂停交易，直至欺诈检测系统有时间来对其合法性进行研究。

欺诈检测系统由几个组成部件构成，这些组成部件通过处理，储存和传递数据来检测异常活动。欺诈检测系统能力的操作是由组件间的数据处理体现的。图1详细地介绍了欺诈检测系统的操作和组成部件。理想情况下，欺诈检测系统在初始登录后将开始监控整个会话。因此，欺诈检测系统执行操作来管理欺诈，即，从监控能力到响应能力，如下：

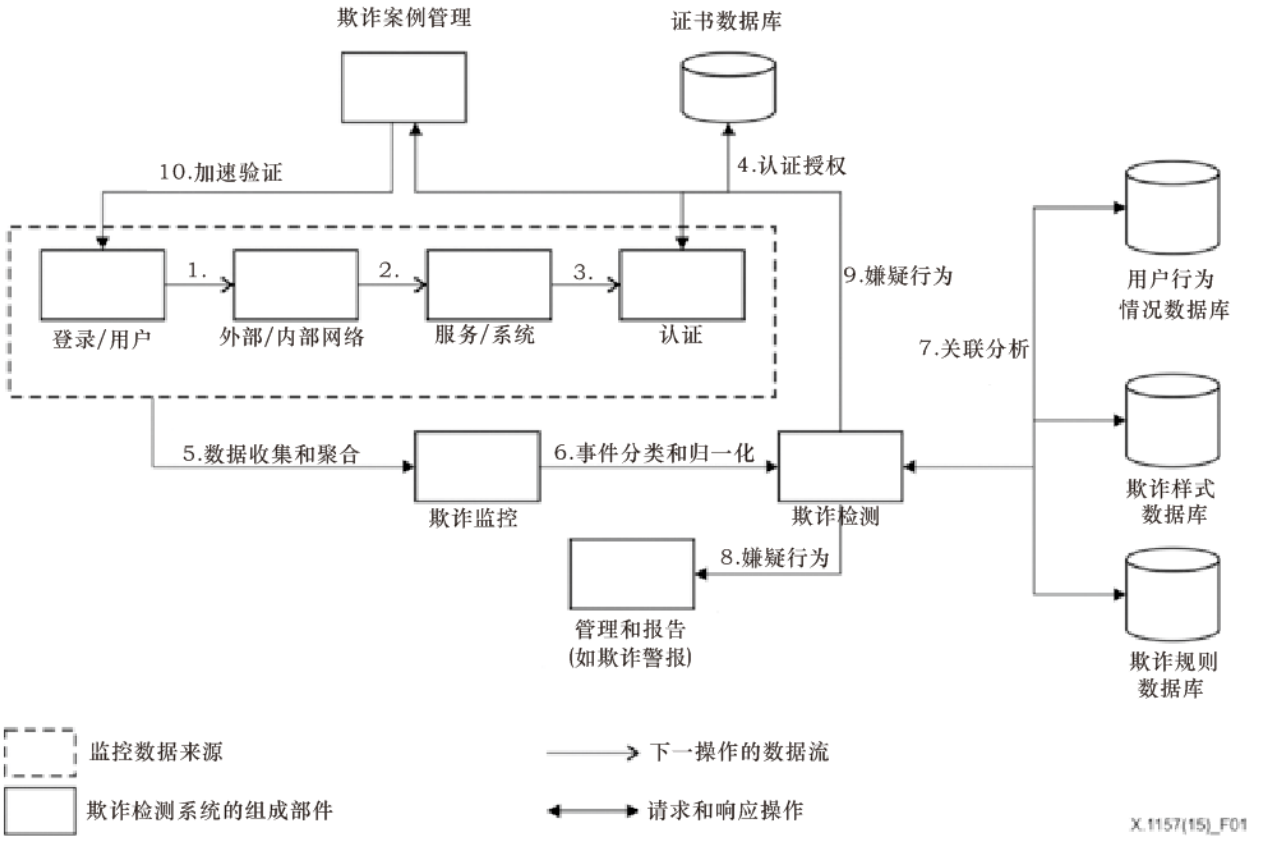


**图1 – 欺诈检测系统的操作和组成部件**

**登录、认证和验证授权操作（数据流1、2、3和4）**

正常情况下，当对登录期间收集的证书与驻留在用户证书数据库（用户名和密码），IP，和用户行为概况数据库等中的数据进行比较时，对初始登录进行分析并分配一个风险评分。验证授权受证书数据库中定义的验证规则指导，通常可由机构进行配置和扩展，以便允许引入新的规则。

**欺诈监控，检测和案例管理操作（数据流5、6、7、9和10）**

欺诈检测系统在用户登录后从各种资料（即，网络，服务项目/系统，和验证）中收集数据。欺诈检测系统从欺诈监控组成部件中分析并收集数据。例如，如果有任何验证识别的可疑活动，欺诈检测系统把可疑的欺诈信息发送给欺诈检测组成部件。然后，欺诈检测组件发送一个数据查询请求给欺诈相关数据库（即，用户行为概况数据，欺诈类型数据和欺诈规则数据），以便分析关联性。基于源于欺诈检测组件对欺诈案例的优先级进行排序，并利用高风险评分值提供一个完整的与那些交互相关联的风险图像。在高风险等级的欺诈案例中，欺诈案例管理组件要求对登录用户加强验证。案例的解析情况应该反馈回数据库，以便创建一个自学循环，为了改善未来的性能。

**管理和报告操作（数据流8）**

管理和报告组件应对机构更好地理解和控制欺诈检测系统是有用的。组件使用户能更早地分析和回报系统性能，识别评分或访问不一致以及需要改善的区域，并且跟踪系统用户的行为和性能。此外，报告工具为高级管理和欺诈分析师提供了一个更简单的方式来提交详细的性能信息。

## 7.2 体系结构方面的考虑

对信息通信技术（ICT）应用实施欺诈检测系统可被认为是通过以下三种体系结构中的一种来实现的：置于应用服务器（如万维网）中的欺诈检测模块、监听与/或监控在线应用、至遗留应用的编程接口。对应用的有效性而言，业务规则和流程更是决定性因素。

**置于应用程序服务器内的欺诈检测模块**

在交易启用应用程序之前，过滤器将企业维护的规则运用于任何超文本传输协议（HTTP）请求（例如，登录或支付）。通过执行模块欺诈规则，交易可以实时地被停止与/或被重定向到一个交易验证例行程序。几个供应商都提供了至应用服务器的插件，可直接嵌入至预处理器中。

**监听与/或监控信息通信技术（ICT）应用（监听模式）**

在这个模式中，应用程序监听或“嗅探”输入文件或HTTP网络通信量（例如，登录），或用安装于每个服务器中的应用程序服务插件读取数据。实时读取数据（网络“嗅探器”方法）或近实时读取数据（应用服务器“监听器”方法），以及要么置于另一个欺诈管理应用中，要么重构为一种可运用欺诈规则的格式。对后一种情况，对可疑交易进行排队，以便后续欺诈分析师跟进。可对定制的应用编程接口（API）进行集成，以便将交易重定向至怀疑/响应验证。

**至遗留应用的编程接口（内嵌集成模式）**

在这种情况下，在处理一个交易前，利用API，通过欺诈检测系统来传递所有的交易。对交易流进行控制，如果检测到可疑的交易，那么可以实时怀疑某个用户。业务规则的变化需要改变核心应用。API主要基于万维网服务。此外，API使之更难以切换供应商特定的解决方案。

一般来说，利用API来进行欺诈检测使企业/组织直接控制交易流变得可能，但需要大量的集成工作，并且当核心应用发生变化时，必须不断地做出更新。在用户交易中不需要实时干预的应用服务器将倾向于第二种方法，这种方法对退出和替换而言是最简单的。

# 8 欺诈检测和响应的技术能力

## 8.1 监控能力

监控能力创建早期攻击和漏洞检测所需的用户和数据环境并且使数据访问和活动监控成为可能。特权用户和敏感数据访问监控对合格报告来说也是普遍要求。

欺诈检测系统需要实现安全信息和事件管理能力，来获得用户活动和网络资源访问，系统，数据库和应用程序的大范围监控。欺诈检测系统还需要增加与用户、资产、威胁和漏洞等背景资料有关的事件数据，以便为漏洞检测提高安全监控效力。此外，它也需要选择性地增强一般安全监控能力和额外功能，例如先进的威胁监控，这基于风险等级和有效地实施和操作欺诈检测和响应系统的能力。

欺诈检测系统还可以以快速分析的方式来手机近乎实时的数据。实时监控对威胁管理是重要的，以便追踪和分析跨组件和系统攻击的进展，对用户活动监控也是重要的，来跟踪和分析用户跨应用程序的活动，或者追踪和分析一些列相关的交易或数据访问时间。最后，在实时收集不实用或不被需要的情况下，实时监控能力应支持批次数据收集。

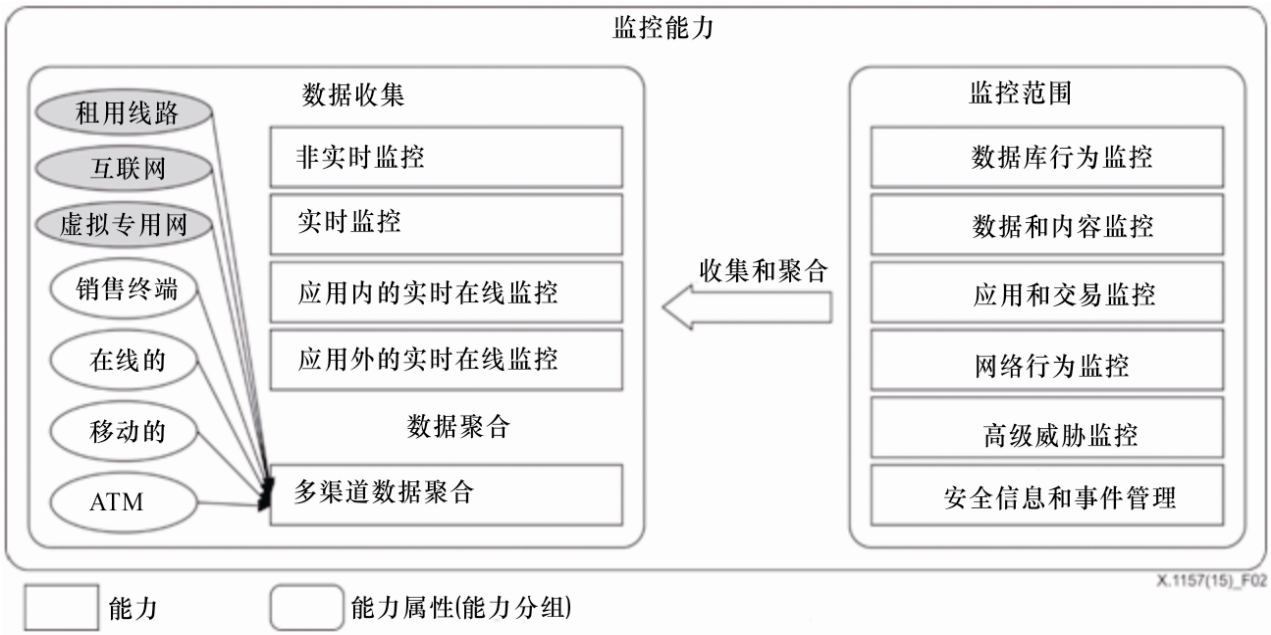


**图2 – 欺诈检测系统的监控能力**

### 8.1.1 数据聚合与收集

大量日志数据资源支持数据聚合与收集，包括网络和安全装置，服务器，数据库和应用程序日志，安全相关应用的输出，例如漏洞评估和数据库活动监控，相关ID输出和访问管理技术，如企业名录，用户配置和访问管理系统。

**非实时监控**

非实时监控要求人工或自动审核日志文件。它能为交易后的分析提供快速部署选项，其中间隙时间较长，并且能解除相关能力以便在完成点停止交易。在实时收集不实用或不被需要的情况下，实时监控能力应支持批次数据收集。

**实时监控**

实时监控利用万维网服务器过滤器实时监控所有的交易（例如HTTP）。该功能可以使用一个低冲击力的万维网服务器过滤器而无需额外的硬件来实施监控。为查看任何实时的交易数据，无需对应用程序做任何改变。

**应用功能内的实时在线监控**

应用功能内的实时在线监控通过内部应用集成实时监控所有HTTP万维网交易。此功能在展开和维护上可能是昂贵和耗时的，因为它需要大量修改应用程序来监控特定交易点。

**应用外实时在线监控**

应用功能外的实时在线监控通过外部应用过滤器来实时监控所有HTTP万维网事物。该功能对有关嗅探器和万维网过滤器方法的应用不会产生任何影响，但外部应用过滤器与应用是匹配的，这可能给应用的可靠性带来风险。为查看任何实时的交易数据，无需对应用程序做任何改变。

**多渠道数据聚合**

多渠道数据聚合意味着其他渠道的交易数据都包含在监控和欺诈检测过程中。另外，多渠道数据聚合寻找可疑用户或账户行为，同时提供了跨渠道和跨产品查看的好处，并关联各用户、账户或实体的警报和活动。多渠道数据聚合使得能够对内部与/或外部实体及其属性（例如，用户、账户、账户属性、机器和机器属性）之间的关系进行分析，以便检测异常活动或滥用。

### 8.1.2 受监控的数据源

欺诈检测系统能在连续的离散时间流中检测到恶意活动，这些离散时间通常与一个经授权的用户相关联，并产生在多种网络，系统和应用源。监控能力包括与多种来源集成来获得可疑和易发事件。

**数据库活动监控**

数据库活动监控维护有特权用户分离责任，有特权用户以监控管理员的活动访问数据库。这项能力通过检测政策违反和不寻常活动来提高数据库安全性。数据库事件聚合，关联性和报告提供了数据库审计功能而无需启用本土审计功能。

该能力支持发现数据库内容和结构的改变以及特权用户通过本地货远程登录访问的数据。因为它在数据库和文件层运行，它缺乏任何未绑定至数据库或相关文件的信息访问和导航的背景知识。网络监控组件（内嵌或之外的）能够用来监控结构化查询语言查询和来自网络的管理访问。

**数据和内容监控**

利用功能支持内容监控，过滤器和数据丢失防护（DLP）,数据和内容监控能力经常用来限制信息泄露，如信用卡号码，个人身份信息和基于文本或基于数据库知识产权。此能力的目的是能够使企业监控它的内部内容来检测可疑活动。内容监控和过滤器用来保护运转中（通过网络监控或或滤器），休息时（通过存储扫描）和使用中（通过端点代理）的内容。大多数功能还包括因政策违规扫描网络上存储内容的能力（如，未经批准的服务器上的一个信用卡号码）和发现内容和数据的合理使用上企业策略的违反情况。

通过使用内容检查和语境分析技术，DLP工具可以发现、监控和主动锁定敏感数据的流动或访问情况，以便在使用时运用一个或多个策略。DLP受限于组织定义敏感内容、其结构或其他识别特征的能力。

尽管这些功能在限制意外泄露或者由不好的业务流程造成的泄露方面非常有用，但恶意攻击者或内部人（如拍照手机，语音信箱，纸或笔）仍会利用非监控活动来规避内容感知解决方案。

**应用程序和交易监控**

应用程序和交易监控能力包括应用程序监控，因为有针对性的攻击经常利用应用程序的弱点，并且异常应用程序活动可能是欺诈活动或一个成功突破的唯一信号。从打包的应用程序中解析活动流的能力使在应用层面对那些组件监控成为可能，此外，为定制应用定义和解析活动流的能力使在应用层面对内部开发的应用程序实施监控成为可能。

监控能力也能在给定渠道内（例如，万维网，手机，本人或跨应用程序和访问渠道）应用程序中提防可疑用户活动或甚至是组织，黑名单IP地址在这些组织间共享。此范围可从检测异常访问（如，通过一台设备同时访问两个不同的地理位置）到检测可疑交易序列（如，改变地址，后跟一个高额转账）。默认情况下，它还可以发现未经授权的员工活动，如果这些活动是在受欺诈检测应用程序监控的应用程序中完成的。

**网络行为监控**

网络行为监控能力提供在系统间信息流量基础上网络操作的可视性，包括来源，目的地，端口，协议，交换的数据量和用户身份。该能力适用于安全和运营相关的分析。另外，此能力利用签名和异常检测的结合来提供网络状态的可视性并且从基线识别偏差，这可指出异常或可疑行为。该能力的目的在于便于公司监控内部网络行为来检测可疑活动。

安全使用案例包括监控，来检测蠕虫的传播，未经授权应用程序的安装和可疑系统访问活动。操作使用案例包括容量规划和信息流量分析，包括将用户ID绑到通信流量上的能力，或者处理审核要求的能力来追踪用户对关键系统的访问。第三层之外的能力几乎没有可视性，所以它不能直接检测系统，数据库，内容，文件系统或其他访问问题。

**高级威胁监控**

针对性恶意软件绕过当代网络互联网服务提供商（IPSs），网络防火墙和万维网安全网关技术。一些小型，专业厂商利用基于网络型产品来检测高级威胁。这些工具通常通过分析可执行程序、通过监控自和至已知或可疑之僵尸网络指控中心的通信（包括域名系统（DNS）查询）或者通过这两种技术的结合，来对恶意的功能（通常使用虚拟环境）进行检测。该能力可以快速地识别出一个潜在的危害（例如，高级的持续威胁），但许多相同的能力正被添加到下一代防火墙、入侵防护系统（IPS）万维网安全网关中。

其他功能专门检测在外部环境中对一个企业的威胁，包括多人在线聊天渠道，聊天室，社交网络等的“黑网”。这些功能能够通过针对一个域，一组IP地址或者关键字的检测来进行。

**安全信息和事件管理**

安全信息和事件管理能力是宽泛的事件收集能力，以及将不同信息源的事件进行关联的能力，以便实现早期破坏检测。通过实时收集和分析来自众多不同数据源的安全事件，该能力将改进威胁管理和安全事件响应。这些来源包括网络和安全设备、服务器、数据库和应用日志、安全相关应用程序的输出（如安全管理和数据库活动监控），以及相关身份和访问管理技术的输出（如企业目录、用户配置和访问管理系统）。此外，通过对来自这些渠道的历史数据进行分析和报告，该能力还为安全策略合规性监控和事件调查提供支持。

为实施欺诈检测，该能力对由设备、系统和应用程序产生的事件数据进行聚合和分析。主要数据来源是日志数据，但该能力还可处理其他形式的数据。要对数据进行归一化处理，这样，可依据为特定目的而设计的规则集，对来自不同渠道的事件进行关联和分析，如网络安全事件监控或用户活动监控，原因是监控和分析完全依赖于由其他渠道产生的事件数据。未具体化至活动日志或作为一个外部事件的活动，对该能力而言是不可见的。

## 8.2 检测能力

欺诈检测使用后台基于服务器的过程 – 对用户来说是透明的 – 检查用户访问和行为。然后它将该信息与预期的和认为“正常的”概况进行比较。它同时对各风险因素组合进行评估，以使实际的欺诈浮出水面，并保持低的虚测率。实时地对可疑的用户交易进行重新验证，以评估其合法性，或者暂停之，直至欺诈分析师有时间对其合法性做出研究。

由于欺诈检测在应用背景下操作，因此它不能检测应用之外的、行为异常的和潜在的欺诈性流程。欺诈检测无法检测未在其引擎中定义的可疑行为，原因是规则不知道活动样式，模型未经足够的学习来将其区分出来，或者应用集成未给欺诈风险评估引擎提供足够的相关数据。为使检测有效，对特定的用例，分析需要嵌入式知识，或者客户需要以定制的关联规则和报告的形式提供此类知识。因此，欺诈检测系统需要以下能力，如欺诈样式更新、预定义规则库支持、实时规则处理等。

在应用程序完全发挥功能之前，大多数能力需要进行广泛的模型调优、配置调优或者检测规则开发。这些能力包括监控所有交易、自动分析风险和评定风险等级、配置和学习用户行为、应用服务特定的和智能的欺诈确定、跨渠道的风险评估等。

### 交易捕获

交易捕获指的是从交易中匹配和提取关键属性的能力，这要求在第一次接入时自动、详细地对每个用户的行为状况做出分析。

### 事件归一化和分类

需要对事件数据做归一化处理，从而可以依据为特定目的（如网络安全事件监控或用户活动监控）而设计的规则集，对来自不同数据源的事件进行关联和分析。这是一种从异构数据源信息到公共事件分类方案的映射。分类有助于模式识别，它还可提高关联规则的范围和稳定性。当来自异构数据源的事件得到归一化后，就可以用较少的关联规则对其进行分析，从而减少部署和支持的工作量。此外，在撰写报告和设计仪表板时，经过归一化的事件更易于处理。

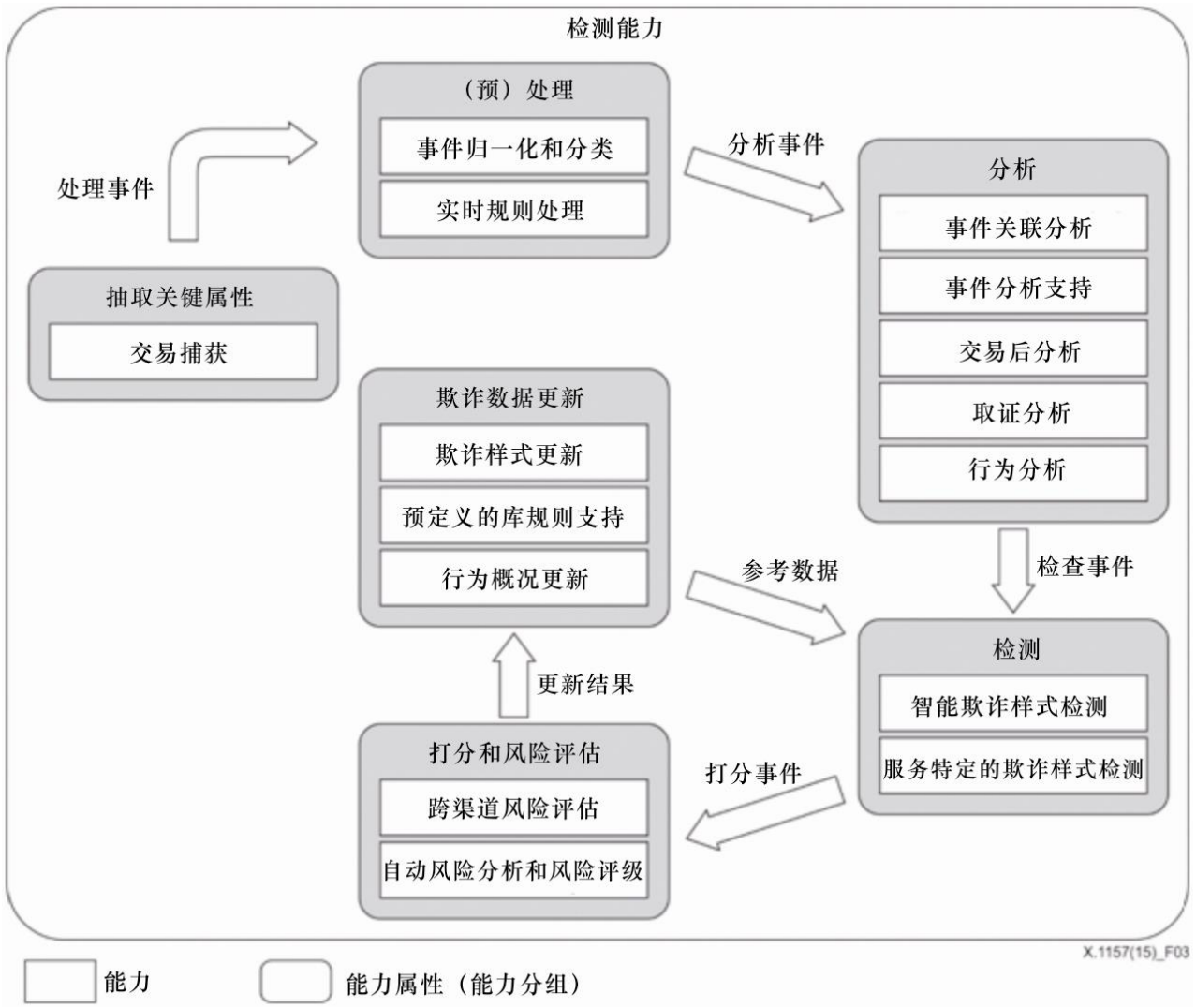


**图 3 – 欺诈检测系统的检测能力**

**欺诈样式更新**

这意味着从网络自动更新欺诈事件数据。欺诈事件数据包括按地理位置分布的IP数据，以对交易来源进行位置分析，包括城市、国家和互联网服务提供商（ISP）等数据，主机声誉数据，用于识别来自已知可疑来源的交易，以及来自试图隐藏起源点者的交易匿名数据。欺诈样式更新应有能力将欺诈检测系统用于整个企业中的其他欺诈用例，并对其进行定制，以满足特定的企业业务需求。例如，欺诈检测系统可集成来自外部欺诈检测的结果、信用评分以及共享的情报系统，如黑名单。

为部署应用欺诈样式更新，有关当前威胁环境的情况存在于各种各样的来源中，包括开放源代码清单、在安全厂商内由安全研究团队开发和维护的威胁和声誉目录，以及所管之安全和其他服务提供商开发的数据等。威胁情报数据可以以观测清单、关联规则和查询的形式，以提高早期破坏检测成功率的方式，集成在一个欺诈检测系统中。

关于威胁和攻击样式的最新信息可以帮助一个组织识别异常活动。例如，至一个外部IP地址的、少量的外向活动可能显示正常，并很易被忽视。如果有一个威胁情报系统，用于指明目的地与僵尸网络控制是关联的，那么一切都将发生变化。该信息可以与预期行为的机器学习算法进行比较，或者与更一般的规则进行比较，指明什么是“正常的”行为，以便对欺诈进行检测。

**预定义的库规则支持**

预定义库规则意味着欺诈检测系统支持可用的已得到证明的规则来应对欺诈。通常，欺诈检测系统的该功能包括部署一系列已得到证明的规则，也应该包括可方便地创建/修改新的规则。此外，该功能可包括与其他组织共享规则的能力。该功能使欺诈检测系统能够快速更新和测试规则以及新的欺诈场景，并轻松地查看和分析数据与欺诈检测结果。它还可以使一组特定的规则可用于管理客户层面、客户群层面或任何其他用户层面的欺诈或滥用。

大多数信用卡欺诈检测系统使企业能够实现对业务规则的管理，使每一笔交易都依据规则进行，这样，企业可以检测特别针对其状况的欺诈行为样式。

该库规则可以基于安全性和背景信息来定义一组规则：

- 用户背景：用户的业务角色；
- 资产背景：所有权、相关的应用或业务流程；
- 信息安全背景：出现在操作系统（OS）、应用程序、万维网或数据库层以及配置状态的薄弱环节；
- 外部威胁背景：已知的坏角色和攻击样式；
- 数据背景：业务重要性或者法律和法规的合规性要求。
- 应用背景：应用程序的商业使用和正常数据访问的边界。

**事件关联分析**

事件关联建立消息或事件之间的关系，这些消息或事件由设备、系统或应用程序产生，基于如来源、目标、协议或事件类型等特性。还应有一个预定义关联规则的库，以及便于定

制这些规则的能力。通过事件关联分析，一个安全事件控制台应提供实时的安全事故和事件陈述。

**事件分析支持**

事件分析通过实时事件关联以及通过基于查询的历史事件分析来实现。安全事件分析由仪表板视图、报告和特别的查询功能组成，用于支持对用户活动和资源访问的调查，以确定威胁、违犯或访问权的滥用情况。当可疑活动因安全监控或活动报告而浮出水面时，重要的是要能够对用户和资源访问情况做出分析。该过程可以通过使用迭代方法来实现，首先需要广泛查询事件的来源、用户或目标，然后开始越来越关注查询，以确定问题的根源。事件分析使用行为分析功能来增强基于规则的关联。

**实时规则处理**

这指的是依据事务流，实时处理欺诈规则的能力，以产生用户/会话风险评分以及详细的事件警报。该功能需要考虑异常的用户行为、常见的欺诈样式、黑名单/白名单以及欺诈事件数据。该功能可以支持规则语法，如带有宽限期限、客户端设备ID、常见欺诈样式、黑名单/白名单、地理IP数据、主机声誉数据等的异常用户行为。此外，欺诈检测系统可以为每个会话执行风险评分和以及为每个用户执行累计风险评分；它还可以使认证系统具有基于风险的认证功能（可实时地为用户和会话提供风险评分功能），以确定是否需要额外的认证。

**管理工具支持**

该功能支持对大信息量的、高效费比的存储和分析，包括收集、索引和存储来自每个渠道的所有日志和事件数据，以及搜索和报告数据的能力。报告能力还应包括预定义的报告，以及能够定义特别报告或使用第三方报告工具的能力。管理工具功能一般包括预定义的和可修改的、有关用户活动的报告，出于特定的和周期性的管理目的而生成的资源访问和模型报告。典型地，管理工具通过万维网支持案例指派和工作流即可用，包括用户特定的视图，如已知的欺诈事件状态、当前的活动和新的标记项、可配置的报警机制，包括电子邮件和万维网服务通知等。

**交易后分析**

这指的是捕获和存储所有数据元素以供未来分析之用的能力。后来，数据仓库包含一个完整的、有关一段时期内所有用户的交易历史。该功能需要进行复杂的数据捕获和格式化，以便实时存储以及快速检索和评估。为进行交易后分析，欺诈检测系统需要使用有关每个单独用户的行为概况，可以按会话、用户和时间戳来分类和存储交易，以便进行检索和分析。

**取证分析**

该功能旨在搜索、过滤和探究交易数据仓库的细节。该能力包括过滤、搜索以及详细分析交易和访问样式的能力。它支持对新兴欺诈样式进行识别，其价值和优势体现在实时的检测规则上。

### 行为分析

欺诈检测系统需要带有所有用户行为概要文件的交易，支持更加复杂的系统，以跟踪个人用户的行为。它为正常活动构建一个概要文件，并通过行为分析功能对偏差发出警报。行为概要文件利用一个学习阶段，来为通过监控功能收集的离散事件源，构建关于正常活动的概要文件。

欺诈检测系统自动从系统第一次监控用户就开始构建用户的概要文件。系统而后可以建立一个关于用户“正常”行为的概要文件，然后在“异常”行为发生时对其进行检查。在检测阶段，当出现偏离正常行为时，发出警报。当对异常条件做了良好定义后，有可能定义关联规则，用于查找一组特定的条件。该能力必须能够自动检测、跟踪、翻译和理解可能有害的样式与异常，避免中断合法的客户体验。最后，行为分析可以基于与正常行为的偏离情况来做出风险决策。

初步建立概要文件后，系统需要更多的时间来学习是什么导致了异常行为，或者让企业来实施正确的规则，以检测异常行为或会话。这种方法可以提高发现有针对性攻击的能力，但仍需领域专家广泛的调优，以便控制虚警率。

### 智能欺诈样式检测

并非所有的欺诈行为都能通过网络、应用日志和离散数据字段来发现。必须纳入非结构化的数据分析，方法是通过使用各种各样的数据挖掘逻辑，评估输入信息的适宜性。

企业应该寻求可利用最小的数据来自己完成学习的数据挖掘逻辑，使系统可以轻松而快速地针对已知的或新发现的欺诈参数来对规则进行更新。它可以依据由身份评分服务供应商直接提供的身份评分服务，来检查新的在线用户身份。这些评分用于确定某个在线用户是否是一个欺诈者的可能性。

### 服务特定的欺诈样式检测

欺诈检测系统需要具备定义规则的能力，以寻找与已知的欺诈样式和服务特定的欺诈样式相对应的交易样式。换句话说，系统依据应用服务中的业务/工作逻辑，寻找某个特定的、可疑的交易和条件序列。根据特定的应用服务，这种样式可以在单个会话中完成，或者跨多个会话和多个用户。

最后，如果不能适当地调整服务，那么欺诈检测系统可能产生太多的虚警。在如电子交易等环境中，实时执行是必要的，虚警太高显然是无法接受的。

### 跨渠道风险评估

欺诈检测系统只运行于给定的应用程序和给定的渠道中，并不跨渠道进行检查（例如，电话、万维网或亲自进行）或者账户类型（例如，存款或信贷）。此外，欺诈检测系统不知道应用程序之外的欺诈活动，它们不集成在知道此类活动的系统中（例如，基于网络的和基于系统的欺诈检测）。因此，它们不能检测应用之外的、恶意的和潜在的欺诈性流程。

因此，欺诈检测需要观察给定访问渠道内应用程序中可疑的用户活动（例如，万维网、电话或亲自进行），或者跨应用程序、访问渠道或甚至组织（例如，当中，在各组织间共享

“黑名单”IP地址）。该范围可从检测异常访问（例如，通过一个设备同时访问两个不同的地理位置）到可疑交易序列（例如，改变地址，后跟一个高额的资金转账）。

为能检测到更多欺诈，欺诈检测系统需要将从欺诈检测模块得到的评分集成进跨渠道的风险评分模块中，后者跨用户渠道进行查看（例如，呼叫中心或自动取款机）。

**自动风险分析和风险评级**

这需要具备自动评价、评估和评级安全风险的能力。检测欺诈和评分交易风险由模型或规则驱动，或者二者的结合。为从各种各样收集到的数据中发现可疑活动，它可使用各种各样建模技术，如贝叶斯、神经网络和其他数据挖掘技术，这需要数据来计算欺诈概率。

可以很好用于目前信用卡空间的神经网络，不能很好用于互联网空间，原因是它们需要大量的数据来检测欺诈样式。因此，对基于万维网的交易，欺诈检测系统将使用替代建模技术，如贝叶斯，这需要较少的数据来计算欺诈概率或者仅仅基于规则来检测。欺诈检测模型生成风险评分，可以输入应用程序的规则集，然后由企业/组织来维护和更新。

## 8.3 响应能力

欺诈检测系统需要自动触发欺诈警报、账户锁定以及为某个特定的交易进行加速的申请者验证（该交易已被标记为可疑的事件响应）。所有的在线账户应用或高风险的匿名交易都应通过一组初始的筛选程序，从作为初始身份证明程序结果的验证事件开始，到应用程序使用和应用程序日志。最初的筛选程序包括基本的欺诈检测，如客户端设备基本身份数据的识别和验证，如姓名、电子邮件地址、地理位置分析，电话号码验证、信用卡欺诈检测、信用局报告验证与/或身份评分。

未通过初始身份证明步骤的可疑交易应被路由至欺诈调查小组，对之进行排队，以便人工或自动进行额外的筛查。而后，如果提示可疑的用户和高风险的交易需要进行额外的筛查，那么欺诈检测系统可使用一个基于风险的和分层的身份证明方法来加速进行身份审核。

**加速申请人验证**

欺诈检测系统可以集成验证机制，这样，欺诈系统产生的风险评分将确定进行用户验证的强度或者进行用户交易验证的强度。它提出了可用于清除可疑交易或其他高风险交易的步骤，这些交易需要进行身份证明。为了尽可能降低成本和尽可能方便客户，企业可以采用一种基于风险的方法，当中，身份证明解决方案的强度与交易风险相称。为此，欺诈检测系统可以结合使用多个身份证明应用程序，这在[b-ITU-T X.1154]中予以描述。

一般来说，市场上没有单一的、包罗万象的身份证明应用程序可用。然而，存在诸多商用的身份证明机制，可将之组合起来，来提供一种有效的、对欺诈者构成威慑的力量。

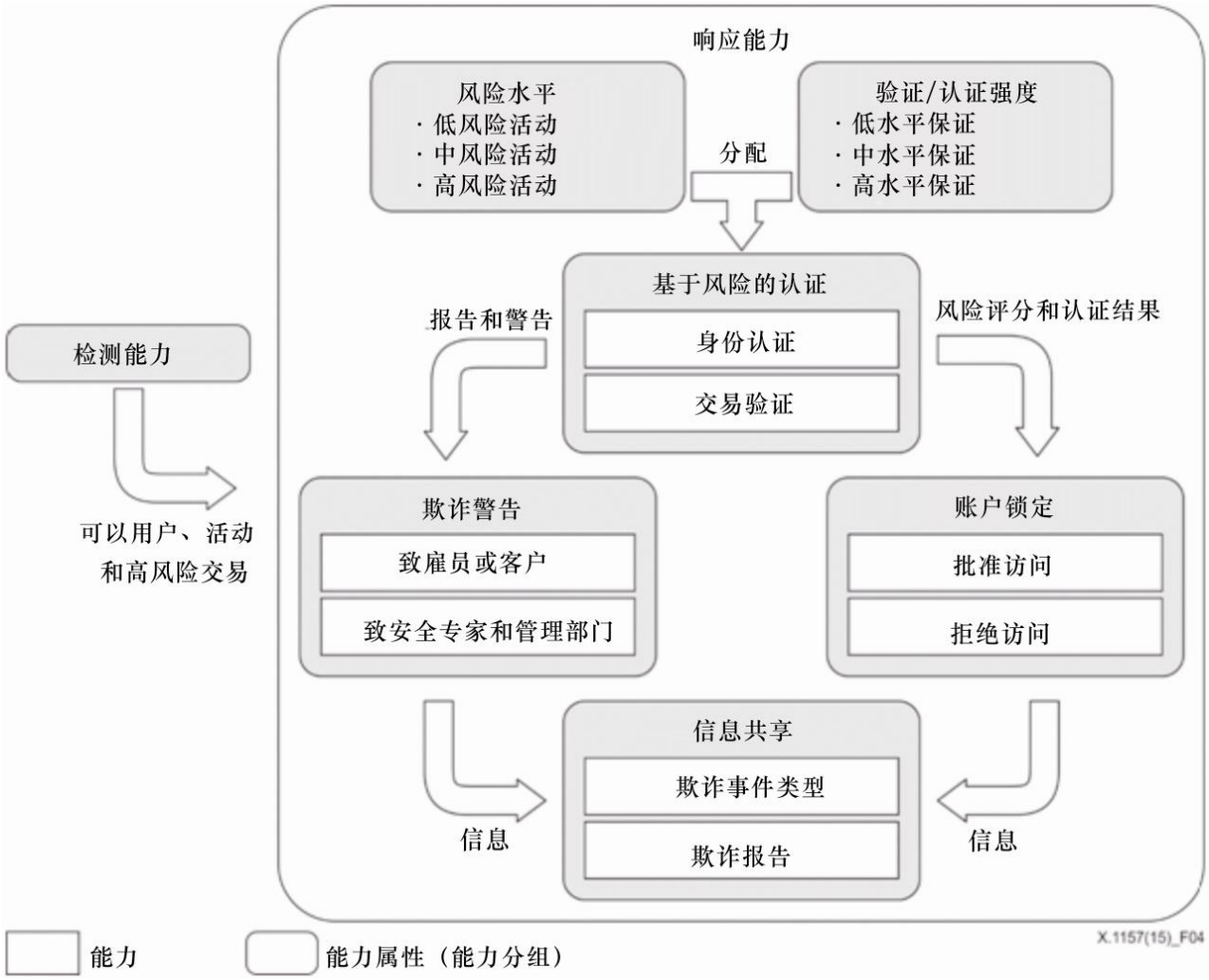


**图 4 – 欺诈检测系统的响应能力**

### 基于风险的认证

经确定，例如，通过欺诈检测系统，风险越高，对客户而言，要求的身份证明措施就越昂贵和越不方便。有若干方法可用，为此需要更强的身份验证，例如：

- 设置初始账户访问，以便低风险活动成为可能，如只读访问公共信息、需要非常基本的身份证明。例如，身份证明机制可以检查针对次要来源的用户姓名和邮件地址。
- 推迟高风险活动，如更新邮件地址，直至采取更强的身份证明（参见[b-ITU-T X.1254]）以及欺诈检测。这包括提供更高保证水平的认证。
  - 依据公共源数据库，使用基于知识的验证，身份证明机制可以对个人信息进行验证。该验证结合了公开可用的信息，如人口统计数据、驾照记录以及信用局数据。
  - 身份证明机制可要求用户对一个或多个有怀疑的问题做出响应，问题要么已经预先做了回答，要么已经存储在用户概述文件中，或者基于真正的账户持有者应知道的信息。
  - 身份证明机制可以使用替代渠道身份验证方法，如蜂窝电话或电子邮件，来联系账户持有者。身份证明机制可以通过向一个已记录在企业的电话号码或已由用户

输入新账户应用程序或支付页面的电话号码发起语音呼叫或发送SMS短信，来向一个新的在线用户传送一个一次性的密码。

- 风险最高的活动将被禁止，如向一个相连的外部银行账户转账，直至用户可以联系到并进行验证；然而，由于许多交易以批处理模式进行执行（而非实时地执行），因此这种方法可能不会改变交易执行的时序。

**欺诈警报**

这意味着当检测到可疑活动时将自动/手动地发出警报。典型地，欺诈警报是结合了风险评分以及针对该评分之若干行动规则的结果。详细的警报包括交易属性和行为描述，可通过电子邮件、可通过规则配置的寻呼机，来通知管理用户其严重程度。根据度量得到的风险水平，欺诈警报可被送往安全专家或者客户/用户。安全专家而后可对感知到的风险做更详细的研究，而送往客户/用户的欺诈警报可用来向潜在的放款者发出警报，其身份可能已被盗走。

**账户锁定**

当检测到可疑活动时，可锁定用户的账户。基于指派的评分和机构的容忍限度，可批准或拒绝用户访问。对评分不足以保证完全访问的用户，可允许之进行有限的访问，或者要求之提供更强的身份验证，以便能够进行完全访问或者允许执行某些高风险的交易。如果用户无法满足这些要求，那么他们可以重新启动加速的验证过程或者立即予以锁定。

**信息共享**

欺诈检测系统应确保系统可有效协调其事件响应活动的各组成部分与组织适当的合作伙伴联合开展行动。

关于事件响应协调，最重要的问题是信息共享，即不同组织相互分享威胁、攻击、漏洞等信息，从而每个组织的知识都能使彼此受益。同样，信息可以直接在企业与客户之间进行共享，或者在组织与员工之间进行共享，原因是同样的威胁和攻击常常同时影响到多个组织或服务。信息共享的目的是使任何发现欺诈的任何组织能够分享该信息，不论是在组织内部共享还是与其他潜在的受害者组织共享。

接收组织可使用该信息，例如，来对由可疑之IP地址发起的交易进行人工检查。欺诈报告可描述一个特定的交易，交易被知或被认为是欺诈交易，或者欺诈报告可描述行为的样式，行为被认为具有欺诈性质。

# 附录 I

# 敏感的信息通信技术应用服务

（本附录不是本建议书的组成部分）

## I.1 电子金融服务

### I.1.1 电子银行和安全问题

在线银行（或互联网银行或电子银行）允许金融机构的客户在一个由金融机构运营的安全网站上进行金融交易，可以是一个零售银行或虚拟银行、信用社或建筑协会。为了访问一个金融机构的在线银行功能，具有个人互联网接入功能的客户必须就相关服务向金融机构进行注册，并设置一个密码（以不同的名称），以便进行客户验证。为了访问在线银行，客户需要上到金融机构的网站上，并使用客户编号和密码进入在线银行设施。一些金融机构已经设立针对此类访问的、额外的安全措施，但没有采取一致的方法。

尽管仍在使用单密码的身份验证，但在一些国家，对在线银行而言，这不被认为具备足够的安全。基本上，在线银行在用两种不同的安全方法。

- 个人身份号/交易号（PIN/TAN）系统，当中PIN代表一个密码，用于登录；TAN代表用于验证交易的一次性密码。TAN可以用不同的方式来分发；最受欢迎的一种方式是通过邮政信件向在线银行用户发送一个TAN清单。使用TAN的最安全方式是根据需要使用一个安全令牌来生成TAN。这些用令牌生成的TAN取决于时间以及一个存储于安全令牌中的唯一密码（双要素身份验证）。带PIN/TAN的在线银行通常通过一个万维网浏览器来实现，浏览器使用一个安全套接层（SSL）来保证连接的安全，因此无需额外进行加密。
- 向在线银行用户提供TAN的另一种方式是通过短信服务（SMS），将当前银行交易的TAN发送给用户的全球移动通信系统（GSM）移动电话。SMS文本通常引用交易数量 和细节；TAN只在一段很短的时间内有效。在许多国家的许多银行中都已采用这种“SMS TAN”服务，尤其在德国、奥地利和荷兰，原因是认为这种方式非常安全。
- 基于签名的在线银行要求所有交易都经数字签名和加密。签名生成和加密的密钥可以存储在智能卡或某种存储介质中，这取决于具体的实现方案。

### I.1.2 电子支付和安全问题

电子支付是指通过基于计算机的系统，在一个金融机构内或跨多个金融机构进行电子交换，或者将资金从一个账户转到另一个。

一个不安全的电子支付系统无法获得其用户的信任。为确保得到用户的接受，信任是非常重要的。电子支付应用面临安全挑战，原因是它们高度依赖于关键的信息通信技术系统，这些ICT系统在金融机构、企业中产生薄弱环节，对客户构成潜在危害。一个安全的电子金融交易必须满足以下要求：

- 完整性和授权：完整性定义为依据业务价值和期望的信息准确性、完全性和有效性。支付系统的完整性意味着，除非支付经过用户授权，否则不会从用户处取走任何资金。此外，用户还可以要求金融机构，如果没有金融机构的明确同意，将不接受任何来自金融机构的付款。

- 机密性：机密性定义为保护敏感或私人信息免遭未经授权的披露。一些相关方可能希望保守交易机密。本文中的机密性意味着限制知晓与交易相关的方方面面信息，如付款者/收款者的身份、购买内容、数量等。在大多数情况下，涉及的参与者想确保通信是私密的。
- 可用性和可靠性：可用性旨在确保信息系统和数据在需要时随时可用。这通常表示为系统可用于有效工作之时间的百分比。所有各方都需要在必要时能够随时完成付款或收款的能力。

## I.2 电子医疗服务

旨在无纸化管理大型医疗机构内所有活动的电子医疗（e-healthcare），承诺加快消除医疗中心和医院中存在的、典型的官僚主义现象。然而，正确实施电子医疗面对的现实是将要涉及诸多安全问题。为了医院能够广泛采用电子医疗，有必要对安全问题做一详细的评估，以便为各种各样组成部件实现标准化设定阶段和步骤，从而正确实施电子医疗。一个典型的电子医疗系统可以包含许多组成部件和子系统，如预约和调度；入院、出院和转院；处方订单输入；饮食规划；常规临床笔记；实验室和放射学订单；图片存档和智能卡登记。每一个子系统都易受到安全威胁的攻击。

### I.2.1 电子医疗服务中的安全问题

- 信息隐私和安全方面的威胁：现有的信息安全风险知识库识别健康信息隐私和安全可能面临的不同类型威胁。然而，当前这种单独的特别分类可能不适用于实践。
- 医疗消费者隐私方面的顾虑：越来越多地依赖于基于万维网的健康信息管理系统以及个人健康银行的部署应用，医疗消费者的隐私问题已逐步成为人们关注的焦点。
- 数据互操作性和信息安全方面的问题：数据互操作的基本前提是为了实现组织内或组织间准确、无缝的数据交换，以支持及时的医疗保健。
- 电子医疗的信息安全问题：医疗部门在移动设备应用和基于万维网的应用方面经历了大幅增长。同时，信息安全问题研究集中于开发框架和协议，以解决电子医疗中存在的安全问题。

## I.3 企业远程接入服务

许多组织的员工和承包商使用企业远程接入技术来从外部站点开展工作。大多数远程工作者使用企业远程接入技术来实现与组织非公开之计算资源的接口。企业远程接入技术的本质—允许从外部网络以及常常是从外部主机访问受保护的资源 – 相比只从组织内部进行访问，通常这会将之置于更高的风险下；此外，允许远程工作者通过企业远程接入技术访问内部资源，也将增加内部资源的风险。

### I.3.1 企业远程接入中的安全问题

企业远程接入技术最常见的安全目标如下所述：

- 机密性：确保远程接入通信和所存用户数据无法被未经授权方读取；
- 完整性：检测在远程接入通信传输过程中出现的、任何有意或无意的变化；
- 可用性：确保当需要时用户随时可以通过远程接入访问资源。

为了实现这些目标，对企业远程接入解决方案的所有组成部件都应做好安全防护，包括客户端设备、远程接入服务器、通过远程接入访问的内部服务器，以应对各种各样的安全威胁。企业远程接入技术通常需要额外的保护，原因是其性质决定了，相比仅从组织内部访问的技术，通常它们更易暴露于外部威胁之下。

企业远程接入的主要安全问题如下所述：

- 缺乏物理安全控制：在各种各样组织控制范围之外的地点来使用企业远程接入客户端设备，如员工的住家、咖啡店、宾馆和会议室。这些设备的移动特性使之可能丢失或被盗，从而将设备中的数据置于可能造成危害的高风险中。即使一个客户端设备总是在其主人手中，也还存在其他形式的物理安全风险，如攻击者在咖啡店“偷窥”企业远程接入工作者、查看客户端设备屏幕上的敏感数据等。
- 不安全的网络：由于几乎所有的企业远程接入都通过互联网进行，因此组织通常无法控制客户使用之外部网络的安全。用于企业远程接入的通信系统包括电话和数字用户线（DSL）调制解调器、如电缆形式的宽带网络和[b-IEEE 802.11]形式的无线机制、全球微波接入互操作性（WiMAX）以及蜂窝网络等。这些通信系统易被窃听，这将把在企业远程接入过程中传输的敏感信息置于可能造成危害的高风险中。也可实施中间人（MITM）攻击，来拦截和篡改通信。因使用不安全的网络而造成的风险是可以减轻的，但不能完全消除，方法是使用加密技术来保护通信的机密性和完整性，以及使用相互身份认证机制来验证两个端点的身份。
- 内部网络中受感染的设备：客户端设备，尤其是笔记本电脑，常常使用外部网络，然后进入组织并直接连接至组织的内部网络。物理接入客户端设备的攻击者可在设备上安装恶意软件，来从其连接的客户端设备、网络和系统上收集数据。如果一个客户端设备感染了恶意软件，那么一旦客户端设备连接至内部网络，该恶意软件可能蔓延至整个组织。除了从组织的安全配置基线使用恰当的反恶意软件技术之外，如客户端设备上的反恶意软件等，组织应考虑使用网络访问控制（NAC）解决方案，以便在允许客户端设备使用内部网络之前，对客户端设备的安全状况进行验证。组织也应考虑为远程工作者的客户端设备启用一个单独的网络，而不是允许其直接连接至内部网络。

- 外部访问内部资源：企业远程接入为外部主机访问内部资源提供了可能，如服务器。如果之前无法从外部网络访问这些内部资源，那么通过远程接入使之可以访问，将使之暴露于新的威胁下，尤其是来自不信任客户端设备和网络的威胁，这将大幅增加其遭受危害的可能性。每种可用于访问内部资源的企业远程接入形式，都会增加资源遭受破坏的风险。

# 参考资料


[b-ITU-T X.1141] ITU-T X.1141 (2006)建议书，安全断言标记语言 *(SAML 2.0)*。

[b-ITU-T X.1154] ITU-T X.1154 (2013)建议书，多重身份服务提供商环境联合认证的一般框架。

[b-ITU-T X.1252] ITU-T X.1252 (2010)建议书，基线的身份管理的术语和定义。

[b-ITU-T X.1254] ITU-T X.1254 (2012)建议书，实体认证保证框架。

[b-IEEE 802.11] IEEE 802.11, *IEEE Standard for Information technology – Telecommunications and information exchange between systems, Local and metropolitan area network – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.*

# ITU-T 系列建议书

| | |
|---|---|
| 系列 A | ITU-T 工作安排 |
| 系列 D | 一般关税原则 |
| 系列 E | 整体网络运营、电话业务、服务运营和人为因素 |
| 系列 F | 非电话电信服务 |
| 系列 G | 传输系统和媒体、数字系统和网络 |
| 系列 H | 视听和多媒体系统 |
| 系列 I | 综合服务数字网络 |
| 系列 J | 有线电视网络和电视的传播，合理的计划和其他多媒体信号 |
| 系列 K | 干扰防护 |
| 系列 L | 环境和信息通信技术、气候变化、电子垃圾、能源效率；结构、安装和电缆保护以及外部设备的其他因素 |
| 系列 M | 电信管理、包括电信管理网和网络维护 |
| 系列 N | 维护：国际广播节目和电视传输电路 |
| 系列 O | 测量设备说明书 |
| 系列 P | 终端和主观及客观的评价方法 |
| 系列 Q | 交换和信令 |
| 系列 R | 电报传输 |
| 系列 S | 终端服务终端设备 |
| 系列 T | 远程信息处理服务终端 |
| 系列 U | 电报交换 |
| 系列 V | 电话网络之上的数据通信 |
| **系列 X** | **数据网络、开放系统通信和安全** |
| 系列 Y | 全球信息基础设施,网络协议方面和下一代网络 |
| 系列 Z | 电信系统的语言和通用软件方面 |

瑞士印刷
2016年，日内瓦