



(21) 申请号 202411757652.X

H04L 9/32 (2006.01)

(22) 申请日 2024.12.03

(56) 对比文件

(65) 同一申请的已公布的文献号

CN 112116046 A, 2020.12.22

申请公布号 CN 119232506 A

CN 113255860 A, 2021.08.13

(43) 申请公布日 2024.12.31

审查员 何思佳

(73) 专利权人 成都纳宝科技有限公司

地址 610000 四川省成都市中国(四川)自
由贸易试验区高新区锦城大道666号4
栋24层4号

(72) 发明人 肖轩 李学朋 刘行 杨思同

(74) 专利代理机构 成都精点专利代理事务所

(普通合伙) 51338

专利代理师 王记明

(51) Int. Cl.

H04L 9/40 (2022.01)

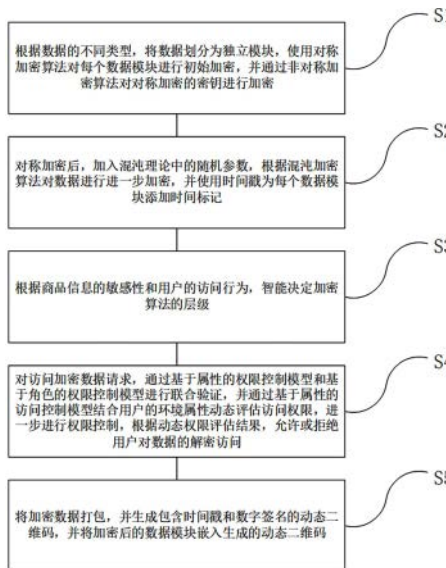
权利要求书3页 说明书10页 附图1页

(54) 发明名称

基于数据安全架构的一物一码多重加密方法
及系统

(57) 摘要

本发明公开了基于数据安全架构的一物一码多重加密方法及系统,涉及一物一码加密方法领域,本发明通过采用对称加密和非对称加密结合的方式进行保护,同时引入混沌理论增强加密强度。系统能够实时监控商品信息的敏感性和用户访问行为,动态调整加密层级。通过多种权限控制模型的协同作用,有效提升访问管理效率,显著降低未授权访问风险。



1. 基于数据安全架构的一物一码多重加密方法,其特征在于,包括以下步骤:

S1. 根据数据的不同类型,将数据划分为独立模块,使用对称加密算法对每个数据模块进行初始加密,并通过非对称加密算法对对称加密的密钥进行加密;

S2. 对称加密后,加入混沌理论中的随机参数,根据混沌加密算法对数据进行进一步加密,并使用时间戳为每个数据模块添加时间标记;

S3. 根据商品信息的敏感性和用户的访问行为,智能决定加密算法的层级;

S4. 对访问加密数据请求,通过基于属性的权限控制模型和基于角色的权限控制模型进行联合验证,并通过基于属性的访问控制模型结合用户的环境属性动态评估访问权限,进一步进行权限控制,根据动态权限评估结果,允许或拒绝用户对数据的解密访问;

S5. 将加密数据打包,并生成包含时间戳和数字签名的动态二维码,并将加密后的数据模块嵌入生成的动态二维码;

其中,所述步骤S2具体包括以下子步骤:

S201. 使用洛伦兹系统生成混沌序列;

S202. 将生成的混沌序列与初始密文通过异或操作进行结合,生成新的加密结果;

S203. 加入时间戳并将其与加密后的数据模块进行绑定;

S204. 使用发送方的私钥对时间戳和混沌加密后的数据模块进行签名;

所述步骤S202中,将生成的混沌序列与密文通过异或操作进行结合的具体流程表示为:

$$C_{chaos} = C_{AES} \oplus S(x_t, y_t, z_t);$$

其中,所述 C_{chaos} 表示生成的混沌序列与初始密文相结合的密文,所述 C_{AES} 表示AES加密后的密文 $E_{K_s}(M)$ 的加密结果,所述 $S(x_t, y_t, z_t)$ 表示通过混沌系统生成的伪随机数序列。

2. 如权利要求1所述的基于数据安全架构的一物一码多重加密方法,其特征在于,所述步骤S1中,使用对称加密算法对每个数据模块进行初始加密,并通过非对称加密算法对对称加密的密钥进行加密具体流程表示为:

$$C_{total} = (E_{K_s}(M), E_{K_{pub}}(K_s));$$

其中,所述 C_{total} 表示结合数据对称加密和秘钥非对称加密的最终加密结果,所述 $E_{K_s}(M)$ 表示AES加密后的密文,代表对数据模块的对称加密,所述 $E_{K_{pub}}(K_s)$ 表示对对称密钥进行的RSA加密,代表非对称加密过程,所述 M 表示数据模块,所述 K_s 表示对称密钥,所述 K_{pub} 表示接收方的RSA公钥。

3. 如权利要求2所述的基于数据安全架构的一物一码多重加密方法,其特征在于,所述AES加密后的密文 $E_{K_s}(M)$ 的加密流程表示为:

$$C_{AES} = E_{K_s}(M) = M \times K_s^T \oplus S(M + K_s);$$

其中,所述 C_{AES} 表示AES加密后的密文 $E_{K_s}(M)$ 的加密结果,即初始密文,所述 K_s^T 表示对称密钥 K_s 的转置,所述 S 表示自定义的多维非线性映射。

4. 如权利要求2所述的基于数据安全架构的一物一码多重加密方法,其特征在于,所述

对对称密钥进行的RSA加密 $E_{K_{pub}}(K_s)$ 的加密流程具体表示为:

$$C_{RSA} = E_{K_{pub}}(K_s) = (K_s^e) \bmod n;$$

其中,所述对称密钥进行的RSA加密的加密流程表示,所述 e 表示公钥指数,所述 n 表示模数。

5.如权利要求1所述的基于数据安全架构的一物一码多重加密方法,其特征在于,所述步骤S3具体包括以下子步骤:

S301.对商品信息进行敏感性分类,基于商品信息的敏感性等级赋予其相应的加密策略,所述敏感性等级包括高、中、低;

S302.实时监控用户的访问信息,所述访问信息包括访问频率、位置、设备信息和登录时间,通过对这些信息进行多维特征提取,计算用户行为特征值;

S303.根据商品信息的敏感性系数和用户行为特征值通过智能加密算法触发条件公式定义加密层次。

6.如权利要求5所述的基于数据安全架构的一物一码多重加密方法,其特征在于,所述步骤S303中,智能加密算法触发条件公式具体表示为:

$$\text{if}(W_s \cdot W_u > T_{threshold}) \text{ then } L_c = L_{base} + 1;$$

其中,所述 W_s 表示商品信息的敏感性,所述 W_u 表示用户行为特征值,所述 $T_{threshold}$ 表示设定的阈值,所述 L_c 表示加密层级。

7.如权利要求6所述的基于数据安全架构的一物一码多重加密方法,其特征在于,所述步骤S303中,通过智能加密算法触发条件公式定义加密层次具体包括:

当计算结果小于等于所设阈值,则不触发进一步加密需求;

当计算结果大于所设阈值,则出发进一步加密需求,对已经加密的数据模块,添加ECC或HMAC层级。

8.如权利要求1所述的基于数据安全架构的一物一码多重加密方法,其特征在于,所述步骤S4具体包括以下子步骤:

S401.对于访问请求,系统通过基于角色的权限控制模型对用户进行初步验证,其中每个用户关联一个或多个角色,系统根据用户的角色决定其初步访问权限;

S402.通过基于属性的权限控制模型对用户的属性进行验证;

S403.结合用户的环境属性进行动态评估,所述环境属性包括时间、地理位置和设备类型;

S404.通过联合权限验证模型,将角色权限、属性权限和环境属性进行综合评估,根据动态权限评估结果,允许或拒绝用户对数据的解密访问。

9.基于数据安全架构的一物一码多重加密系统,该系统基于权利要求1-8任一项所述的基于数据安全架构的一物一码多重加密方法所实现,其特征在于,包括:

初始加密模块,用于根据数据的不同类型,将数据划分为独立模块,使用对称加密算法对每个数据模块进行初始加密,并通过非对称加密算法对对称加密的密钥进行加密;

混沌加密模块,用于在对称加密后,加入混沌理论中的随机参数,根据混沌加密算法对数据进行进一步加密,并使用时间戳为每个数据模块添加时间标记;

层级加密模块,用于根据商品信息的敏感性和用户的访问行为,智能决定加密算法的

层级;

访问请求解密判断模块,用于对访问加密数据请求,通过基于属性的权限控制模型和基于角色的权限控制模型进行联合验证,并通过基于属性的访问控制模型结合用户的环境属性动态评估访问权限,进一步进行权限控制,根据动态权限评估结果,允许或拒绝用户对数据的解密访问;

一物一码生成模块,用于将加密数据打包,并生成包含时间戳和数字签名的动态二维码,并将加密后的数据模块嵌入生成的动态二维码。

基于数据安全架构的一物一码多重加密方法及系统

技术领域

[0001] 本发明涉及一物一码加密方法领域,具体是基于数据安全架构的一物一码多重加密方法及系统。

背景技术

[0002] 在当今信息技术飞速发展的时代,数据安全问题愈发突出,尤其是在一物一码系统中,数据的安全防护显得尤为重要。一物一码系统为每个商品或对象分配唯一的识别码,通过二维码或RFID等技术,实现信息的实时追踪与管理。该系统涉及的数据信息包括商品数据信息、营销活动数据信息、渠道数据信息及用户信息等,这些数据的安全性直接关系到整个供应链的有效运作。现有技术主要集中在数据加密、身份验证等方面,普遍采用对称加密和非对称加密的组合来保护数据传输与存储。然而,尽管对数据进行了加密处理,仍然存在潜在的风险,特别是在面对复杂的用户访问需求和动态环境时,现有技术往往无法提供有效的解决方案。

[0003] 现有一物一码系统的数据安全防护主要依赖于静态的安全措施,如对称加密算法(如AES)和非对称加密算法(如RSA)等。这些方法在一定程度上能够保护数据不被未授权访问,但却面临着多项不足。首先,现有技术在数据管理上往往缺乏对数据类型的细致划分,未能根据不同数据的敏感性采取相应的保护措施。导致高敏感性数据与低敏感性数据混合存储,增加了数据泄露的风险。其次,传统的权限控制模型虽然提供了基础的访问安全保障,但在处理动态访问请求时显得不够灵活。用户的访问行为、地理位置、设备信息等变化未能及时反映在权限控制中,造成访问权限滞后。最后,随着数据泄露事件频发,现有的静态加密方案在面对日益复杂的攻击手段时,显得无能为力,亟需更加灵活和智能的防护机制。

发明内容

[0004] 本发明提出了基于数据安全架构的一物一码多重加密方法及系统,该方法通过多重加密与动态权限控制的结合,提升了一物一码系统的数据安全性。

[0005] 其中,基于数据安全架构的一物一码多重加密方法,包括以下步骤:

[0006] S1. 根据数据的不同类型,将数据划分为独立模块,使用对称加密算法对每个数据模块进行初始加密,并通过非对称加密算法对对称加密的密钥进行加密;

[0007] S2. 对称加密后,加入混沌理论中的随机参数,根据混沌加密算法对数据进行进一步加密,并使用时间戳为每个数据模块添加时间标记;

[0008] S3. 根据商品信息的敏感性和用户的访问行为,智能决定加密算法的层级;

[0009] S4. 对访问加密数据请求,通过基于属性的权限控制模型和基于角色的权限控制模型进行联合验证,并通过基于属性的访问控制模型结合用户的环境属性动态评估访问权限,进一步进行权限控制,根据动态权限评估结果,允许或拒绝用户对数据的解密访问;

[0010] S5. 将加密数据打包,并生成包含时间戳和数字签名的动态二维码,并将加密后

的数据模块嵌入生成的动态二维码。

[0011] 进一步的,所述步骤S1中,使用对称加密算法对每个数据模块进行初始加密,并通过非对称加密算法对对称加密的密钥进行加密具体流程表示为:

$$[0012] \quad C_{total} = (E_{K_s}(M), E_{K_{pub}}(K_s));$$

[0013] 其中,所述 C_{total} 表示结合数据对称加密和密钥非对称加密的最终加密结果,所述 $E_{K_s}(M)$ 表示AES加密后的密文,代表对数据模块的对称加密,所述 $E_{K_{pub}}(K_s)$ 表示对对称密钥进行的RSA加密,代表非对称加密过程,所述 M 表示数据模块,所述 K_s 表示对称密钥,所述 K_{pub} 表示接收方的RSA公钥。

[0014] 进一步的,所述AES加密后的密文 $E_{K_s}(M)$ 的加密流程表示为:

$$[0015] \quad C_{AES} = E_{K_s}(M) = M \times K_s^T \oplus S(M + K_s);$$

[0016] 其中,所述 C_{AES} 表示AES加密后的密文 $E_{K_s}(M)$ 的加密结果,即初始密文,所述 K_s^T 表示对称密钥 K_s 的转置,所述 S 表示自定义的多维非线性映射。

[0017] 进一步的,所述对对称密钥进行的RSA加密 $E_{K_{pub}}(K_s)$ 的加密流程具体表示为:

$$[0018] \quad C_{RSA} = E_{K_{pub}}(K_s) = (K_s^e) \bmod n;$$

[0019] 其中,所述对称密钥进行的RSA加密的加密流程表示,所述 e 表示公钥指数,所述 n 表示模数。

[0020] 进一步的,所述步骤S2具体包括以下子步骤:

[0021] S201. 使用洛伦兹系统生成混沌序列;

[0022] S202. 将生成的混沌序列与初始密文通过异或操作进行结合,生成新的加密结果;

[0023] S203. 加入时间戳并将其与加密后的数据模块进行绑定;

[0024] S204. 使用发送方的私钥对时间戳和混沌加密后的数据模块进行签名。

[0025] 进一步的,所述步骤S202中,将生成的混沌序列与密文通过异或操作进行结合的具体流程表示为:

$$[0026] \quad C_{chaos} = C_{AES} \oplus S(x_t, y_t, z_t);$$

[0027] 其中,所述 C_{chaos} 表示生成的混沌序列与初始密文相结合的密文,所述 C_{AES} 表示AES加密后的密文 $E_{K_s}(M)$ 的加密结果,所述 $S(x_t, y_t, z_t)$ 表示通过混沌系统生成的伪随机数序列。

[0028] 进一步的,所述步骤S3具体包括以下子步骤:

[0029] S301. 对商品信息进行敏感性分类,基于商品信息的敏感性等级赋予其相应的加密策略,所述敏感性等级包括高、中、低;

[0030] S302. 实时监控用户的访问信息,所述访问信息包括访问频率、位置、设备信息和登录时间,通过对这些信息进行多维特征提取,计算用户行为特征值;

[0031] S303. 根据商品信息的敏感性系数和用户行为特征值通过智能加密算法触发条件公式定义加密层次。

[0032] 进一步的,所述步骤S303中,智能加密算法触发条件公式具体表示为:

[0033] $if(W_s \cdot W_u > T_{threshold}) then L_c = L_{base} + 1;$

[0034] 其中,所述 W_s 表示商品信息的敏感性,所述 W_u 表示用户行为特征值,所述 $T_{threshold}$ 表示设定的阈值,所述 L_c 表示加密层级。

[0035] 进一步的,所述步骤S303中,通过智能加密算法触发条件公式定义加密层次具体包括:

[0036] 当计算结果小于等于所设阈值,则不触发进一步加密需求;

[0037] 当计算结果大于所设阈值,则触发进一步加密需求,对已经加密的数据模块,添加ECC或HMAC层级。

[0038] 进一步的,所述步骤S4具体包括以下子步骤:

[0039] S401. 对于访问请求,系统通过基于角色的权限控制模型对用户进行初步验证,其中每个用户关联一个或多个角色,系统根据用户的角色决定其初步访问权限;

[0040] S402. 通过基于属性的权限控制模型对用户的属性进行验证;

[0041] S403. 结合用户的环境属性进行动态评估,所述环境属性包括时间、地理位置和设备类型;

[0042] S404. 通过联合权限验证模型,将角色权限、属性权限和环境属性进行综合评估,根据动态权限评估结果,允许或拒绝用户对数据的解密访问。

[0043] 进一步的,基于数据安全架构的一物一码多重加密系统,该系统基于上述任一项所述的基于数据安全架构的一物一码多重加密方法所实现,包括:

[0044] 初始加密模块,用于根据数据的不同类型,将数据划分为独立模块,使用对称加密算法对每个数据模块进行初始加密,并通过非对称加密算法对对称加密的密钥进行加密;

[0045] 混沌加密模块,用于在对称加密后,加入混沌理论中的随机参数,根据混沌加密算法对数据进行进一步加密,并使用时间戳为每个数据模块添加时间标记;

[0046] 层级加密模块,用于根据商品信息的敏感性和用户的访问行为,智能决定加密算法的层级;

[0047] 访问请求解密判断模块,用于对访问加密数据请求,通过基于属性的权限控制模型和基于角色的权限控制模型进行联合验证,并通过基于属性的访问控制模型结合用户的环境属性动态评估访问权限,进一步进行权限控制,根据动态权限评估结果,允许或拒绝用户对数据的解密访问;

[0048] 一物一码生成模块,用于将加密数据打包,并生成包含时间戳和数字签名的动态二维码,并将加密后的数据模块嵌入生成的动态二维码。

[0049] 发明的有益效果是:

[0050] 本发明通过采用对称加密和非对称加密结合的方式进行保护,同时引入混沌理论增强加密强度。系统能够实时监控商品信息的敏感性和用户访问行为,动态调整加密层级。通过多种权限控制模型的协同作用,有效提升访问管理效率,显著降低未授权访问风险。

附图说明

[0051] 图1为本发明实施例提供的基于数据安全架构的一物一码多重加密方法的方法流程图。

具体实施方式

[0052] 下面结合附图进一步详细描述本发明的技术方案,但本发明的保护范围不局限于以下所述。

[0053] 为了使本发明的目的,技术方案及优点更加清楚明白,结合附图及实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅用以解释本发明,并不用于限定本发明,即所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。通常在此处附图中描述和示出的本发明实施例的组件可以以各种不同的配置来布置和设计。

[0054] 因此,以下对在附图中提供的本发明的实施例的详细描述并非旨在限制要求保护的本发明的范围,而是仅仅表示本发明的选定实施例。基于本发明的实施例,本领域技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例,都属于本发明保护的范围。需要说明的是,术语“第一”和“第二”等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。

[0055] 而且,术语“包括”,“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程,方法,物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程,方法,物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程,方法,物品或者设备中还存在另外的相同要素。

[0056] 以下结合实施例对本发明的特征和性能作进一步的详细描述。

[0057] 其中,如图1,基于数据安全架构的一物一码多重加密方法,包括以下步骤:

[0058] S1. 根据数据的不同类型,将数据划分为独立模块,使用对称加密算法对每个数据模块进行初始加密,并通过非对称加密算法对对称加密的密钥进行加密;具体的,根据数据的不同类型,将数据划分为独立模块,以便进行更加灵活和高效的加密。使用对称加密算法(如AES)对每个数据模块进行初步加密,并通过非对称加密算法(如RSA)对对称密钥进行加密,确保密钥的安全存储和传输。通过这种方式,能够实现数据的初步保护,增强数据安全性,同时确保密钥不会被泄露。

[0059] S2. 对称加密后,加入混沌理论中的随机参数,根据混沌加密算法对数据进行进一步加密,并使用时间戳为每个数据模块添加时间标记;具体的,在对称加密后,通过引入混沌理论,利用洛伦兹系统生成的混沌序列,提高数据的复杂性和安全性。生成的混沌序列与初始密文进行异或操作,得到新的加密结果。随后为每个数据模块添加时间戳,确保数据的时效性。最后,使用发送方的私钥对混沌加密后的数据模块和时间戳进行签名,保证数据的完整性。这样可以增强加密强度,确保数据在传输过程中的安全性与完整性,有效防止数据伪造和重放攻击。

[0060] S3. 根据商品信息的敏感性和用户的访问行为,智能决定加密算法的层级;具体的,通过评估商品信息的敏感性和用户的访问行为,动态调整加密层级,以实现智能化数据保护。商品信息根据敏感性被分类为高、中、低级别。实时收集用户的访问行为数据,分析访问频率、位置等信息,并计算用户行为特征值。根据商品的敏感性系数和用户行为特征值,通过智能加密算法触发条件公式定义加密层次,从而实现对不同数据类型的智能化保护,使数据安全措施更具针对性和灵活性。

[0061] S4. 对访问加密数据请求,通过基于属性的权限控制模型和基于角色的权限控制模型进行联合验证,并通过基于属性的访问控制模型结合用户的环境属性动态评估访问权限,进一步进行权限控制,根据动态权限评估结果,允许或拒绝用户对数据的解密访问;具体的,通过结合多种权限控制模型,对用户进行全面的身份验证和权限评估,以确保只有授权用户能够访问特定数据。对于访问请求,系统利用基于角色的访问控制模型对用户进行初步验证,决定初步访问权限。随后,通过基于属性的权限控制模型验证用户属性,并结合用户的环境属性(如时间、地理位置和设备类型)进行动态评估。最终,通过联合验证模型,将角色权限、属性权限和环境属性进行综合评估,从而提升访问控制的安全性,确保只有符合条件的用户能够访问敏感数据,有效降低数据泄露的风险。

[0062] S5. 将加密数据打包,并生成包含时间戳和数字签名的动态二维码,并将加密后的数据模块嵌入生成的动态二维码;具体的,通过将加密数据与时间戳和数字签名结合,生成动态二维码,以便于数据的安全传输和验证。将所有加密数据模块进行打包,准备生成二维码。随后创建动态二维码,嵌入加密后的数据模块,同时附上时间戳和数字签名。二维码可以通过多种渠道发布,用户扫描后获取对应的安全数据。通过这种方式,提供了一种安全、便捷的数据传输方式,有效防止二维码的伪造和重复使用,确保数据在流通过程中的安全性。

[0063] 其中,上述实施例用于一物一码系统中的数据安全防护,特别是通过多重加密机制和数据安全架构,确保一物一码和码包数据信息、商品数据信息、营销活动数据信息、厂家数据信息、渠道数据信息以及用户信息数据的安全性。进一步的,上述实施例采用模块化设计方案,每个系统功能划分为独立的模块,确保高内聚性和低耦合性,提升功能模块的可维护性和可重用性;系统设计遵循单一职责原则(SRP)和开闭原则(OCP),提高功能模块的可维护性和增量开发能力,对于数据传输与加密机制,系统采用多层加密机制,运用AES、RSA等多种加密算法,确保每个数据传输和存储的安全,结合混合加密和混沌理论加密模式,增强数据的安全性和可靠性。另外,通过系统内置动态生成算法,配合时间戳和数字签名技术,生成可用作于产品一物一码管理的唯一动态二维码。

[0064] 进一步的,本实施例引入RBAC(基于角色的访问控制模型)、ABAC(基于属性的访问控制模型)、ACL(访问控制列表模型)、PBAC(基于策略的访问控制模型)等多种权限模型,实现独立的身份和权限管理服务,集中处理认证和授权,确保安全性和一致性;同时使用策略引擎来定义和管理访问控制策略,根据不同角色和属性动态调整访问权限;通过内容分发网络(CDN),优化内容分发,根据地理位置和角色提供个性化内容展示。系统采用OAuth 2.0和OpenID Connect进行安全的认证,并利用JWT技术在服务间安全传输数据信息。核心的权限管理服务集成了RBAC、ABAC、ACL和PBAC等多种访问控制模型,由策略引擎动态评估并执行访问控制策略,保障不同角色的权限一致性和安全性。

[0065] 需要说明的是,所述动态二维码可根据实际需求进行替换,其形式包括但不限于二维码、条形码、数字ID等。

[0066] 进一步的,所述步骤S1中,使用对称加密算法对每个数据模块进行初始加密,并通过非对称加密算法对对称加密的密钥进行加密具体流程表示为:

[0067] $C_{total} = (E_{K_s}(M), E_{K_{pub}}(K_s));$

[0068] 其中,所述 C_{total} 表示结合数据对称加密和密钥非对称加密的最终加密结果,所述

$E_{K_s}(M)$ 表示AES加密后的密文,代表对数据模块的对称加密,所述 $E_{K_{pub}}(K_s)$ 表示对对称密钥进行的RSA加密,代表非对称加密过程,所述 M 表示数据模块,所述 K_s 表示对称密钥,所述 K_{pub} 表示接收方的RSA公钥。

[0069] 进一步的,所述AES加密后的密文 $E_{K_s}(M)$ 的加密流程表示为:

$$[0070] \quad C_{AES} = E_{K_s}(M) = M \times K_s^T \oplus S(M + K_s);$$

[0071] 其中,所述 C_{AES} 表示AES加密后的密文 $E_{K_s}(M)$ 的加密结果,即初始密文,所述 K_s^T 表示对称密钥 K_s 的转置,所述 S 表示自定义的多维非线性映射。

[0072] 进一步的,所述对对称密钥进行的RSA加密 $E_{K_{pub}}(K_s)$ 的加密流程具体表示为:

$$[0073] \quad C_{RSA} = E_{K_{pub}}(K_s) = (K_s^e) \bmod n;$$

[0074] 其中,所述对称密钥进行的RSA加密的加密流程表示,所述 e 表示公钥指数,所述 n 表示模数。

[0075] 进一步的,所述步骤S2具体包括以下子步骤:

[0076] S201. 使用洛伦兹系统生成混沌序列;具体的,利用洛伦兹系统的动力学特性,生成一个高维的混沌序列。洛伦兹系统通过非线性微分方程产生复杂的动态行为,确保生成的序列具有高度的不确定性和不可预测性,为后续的加密提供了随机性基础。

[0077] S202. 将生成的混沌序列与初始密文通过异或操作进行结合,生成新的加密结果;具体的,将生成的混沌序列与初始的对称加密密文进行异或操作。此步骤通过将混沌序列的随机性引入到密文中,进一步增强了加密强度,使得攻击者难以通过已知的密文信息进行有效的破解。

[0078] S203. 加入时间戳并将其与加密后的数据模块进行绑定;具体的,为每个加密后的数据模块添加一个时间戳。这一时间戳不仅标记数据生成的时间,还在后续验证中起到重要作用,确保数据的时效性和唯一性,从而防止重放攻击。

[0079] S204. 使用发送方的私钥对时间戳和混沌加密后的数据模块进行签名;具体的,利用发送方的私钥对时间戳和混沌加密后的数据模块进行数字签名。此步骤确保了数据的完整性和真实性,使得接收方能够验证数据是否在传输过程中被篡改或伪造,从而进一步保障数据的安全性。

[0080] 进一步的,所述步骤S202中,将生成的混沌序列与密文通过异或操作进行结合的具体流程表示为:

$$[0081] \quad C_{chaos} = C_{AES} \oplus S(x_t, y_t, z_t);$$

[0082] 其中,所述 C_{chaos} 表示生成的混沌序列与初始密文相结合的密文,所述 C_{AES} 表示AES加密后的密文 $E_{K_s}(M)$ 的加密结果,所述 $S(x_t, y_t, z_t)$ 表示通过混沌系统生成的伪随机数序列。

[0083] 具体的,本实施例采用多层加密机制的加密标准,运用AES、RSA、ECC等多种加密算法,集成混合加密和混沌理论加密模式,确保每个数据传输和存储安全。作为优选的,还可结合Reed-Solomon错误纠正算法,即便在部分损坏的情况下也能可靠读取,保障了数据的完整性和准确性。系统内置的动态生成算法可创建独一无二的二维码,配合时间戳和数字

签名技术,有效防止二维码的伪造和重复使用。

[0084] 进一步的,所述步骤S3具体包括以下子步骤:

[0085] S301. 对商品信息进行敏感性分类,基于商品信息的敏感性等级赋予其相应的加密策略,所述敏感性等级包括高、中、低;具体的,根据商品的信息和相关标准,将其分类为高、中、低三个敏感性等级。这一分类过程确保系统能够识别哪些数据需要更高的保护级别,以便为不同等级的数据应用相应的加密策略。

[0086] S302. 实时监控用户的访问信息,所述访问信息包括访问频率、位置、设备信息和登录时间,通过对这些信息进行多维特征提取,计算用户行为特征值;具体的,系统实时监控用户的访问行为,收集并分析访问频率、地理位置、设备信息和登录时间等数据。通过对这些信息的多维特征提取,系统能够形成用户的行为特征值,为后续的动态加密决策提供依据。

[0087] S303. 根据商品信息的敏感性系数和用户行为特征值通过智能加密算法触发条件公式定义加密层次;具体的,结合商品信息的敏感性系数和用户的行为特征值,应用智能加密算法触发条件公式,以确定加密的层级。通过这一过程,系统能够智能调整加密策略,确保敏感数据在不同场景下的安全性。

[0088] 进一步的,所述步骤S303中,智能加密算法触发条件公式具体表示为:

[0089] $\text{if}(W_s \cdot W_u > T_{\text{threshold}}) \text{ then } L_c = L_{\text{base}} + 1;$

[0090] 其中,所述 W_s 表示商品信息的敏感性,所述 W_u 表示用户行为特征值,所述 $T_{\text{threshold}}$ 表示设定的阈值,所述 L_c 表示加密层级。具体的,用户行为特征在动态加密策略中用于识别访问数据的用户带来的安全风险,从而实现更具情境敏感的加密策略。示例性的,设置用户行为特征包括:访问时间:如在非常规时间(深夜或非工作时间)进行的数据请求;访问位置:基于地理位置,检测访问是否来自于可信位置(如公司内部网络)还是未知或高风险位置;设备类型:检测设备是否为常用或可信设备(如工作电脑)或陌生设备;访问频率:高频次或不寻常的访问请求可能代表数据滥用风险,尤其是敏感数据的重复读取;设备安全等级:判断设备是否具备最新的安全更新、反病毒软件等安全保护。再示例性的,对于非常敏感的数据信息(如机密文件),如果检测到高风险用户行为特征(如共享公共网络、非授权设备登录),系统可以优先考虑加入高强度加密算法的层级。

[0091] 进一步的,所述步骤S303中,通过智能加密算法触发条件公式定义加密层次具体包括:

[0092] 当计算结果小于等于所设阈值,则不触发进一步加密需求;

[0093] 当计算结果大于所设阈值,则触发进一步加密需求,对已经加密的数据模块,添加ECC或HMAC层级。

[0094] 进一步的,所述步骤S4具体包括以下子步骤:

[0095] S401. 对于访问请求,系统通过基于角色的权限控制模型对用户进行初步验证,其中每个用户关联一个或多个角色,系统根据用户的角色决定其初步访问权限;具体的,对访问请求进行处理,系统使用基于角色的访问控制(RBAC)模型对用户进行初步验证。每个用户被分配一个或多个角色,根据角色来初步决定其访问权限,从而过滤掉不具备基本访问权限的请求。

[0096] S402. 通过基于属性的权限控制模型对用户的属性进行验证;具体的,系统利用基于属性的访问控制(ABAC)模型,对用户的属性进行进一步验证。这包括用户的身份信息、角色信息等,以确保只有符合条件的用户才能进入下一步验证。

[0097] S403. 结合用户的环境属性进行动态评估,所述环境属性包括时间、地理位置和设备类型;具体的,结合用户的环境属性(如访问时间、地理位置和设备类型),系统进行动态评估。这一步骤确保在不同环境下,用户的访问权限能够灵活调整,提高了安全性。

[0098] S404. 通过联合权限验证模型,将角色权限、属性权限和环境属性进行综合评估,根据动态权限评估结果,允许或拒绝用户对数据的解密访问;具体的,通过联合权限验证模型,综合评估用户的角色权限、属性权限和环境属性。根据综合评估结果,系统决定是否允许用户对数据的解密访问,从而实现全面的访问控制,降低数据泄露风险。

[0099] 进一步的,所述步骤S401-S404具体的流程公式表示如下:

[0100] 系统通过基于角色的权限控制模型对用户进行初步验证。每个用户都关联一个或多个角色,系统根据用户的角色决定其初步访问权限:

$$[0101] \quad P_r(U) = f(U_r);$$

[0102] 其中,所述 $P_r(U)$ 表示用户 U 的访问权限,所述 U_r 表示用户的角色,所述 $f(U_r)$ 表示角色到权限的映射函数;对于用户 U ,当其角色 U_r 拥有访问权限 P_r 时,则通过初步验证;

[0103] 系统对用户的属性进行验证,采用基于属性的权限控制模型(ABAC),确保用户不仅有角色权限,还具有合适的属性来访问数据:

$$[0104] \quad P_a(U) = g(U_a);$$

[0105] 其中,所述 U_a 表示用户的属性集合,所述 $g(U_a)$ 表示属性到权限的映射函数,所述 $P_a(U)$ 表示基于用户 U 的属性的访问权限;根据用户的属性 U_a ,系统确定用户是否符合访问加密数据的要求;

[0106] 系统结合用户的环境属性进行动态评估。环境属性可以包括时间、地理位置、设备类型等外部因素。根据环境属性进行动态评估可以使系统在不同场景下做出更合适的权限判断:

$$[0107] \quad P_{env}(U, E_a) = h(E_a);$$

[0108] 其中,所述 E_a 表示环境属性集合,所述 $h(E_a)$ 表示环境属性到权限评估的函数,所述 $P_{env}(U, E_a)$ 表示结合用户 U 的环境属性 E_a 的访问权限;当在满足环境属性要求的情况下,系统授予用户最终的访问权限;

[0109] 通过联合权限验证模型,将角色权限、属性权限和环境属性进行综合评估,确保最终的权限判定是根据多重条件来决定的。具体联合验证规则通过以下公式表示:

$$[0110] \quad P_{final}(U) = P_r(U) \wedge P_a(U) \wedge P_{env}(U, E_a);$$

[0111] 其中,所述 $P_{final}(U)$ 表示用户 U 的最终权限判定,只有当角色、属性和环境权限均满足条件时,用户才能通过验证,获得对加密数据的访问权限。

[0112] 进一步的,上述实施例的权限评估流程为:

[0113] 用户发起访问加密数据请求,提供身份信息、角色信息、属性信息和环境信息;

- [0114] 系统根据用户的角色信息进行初步权限验证,判断 $P_r(U)$ 是否为真;
- [0115] 系统进一步验证用户的属性信息 U_a ,判断 $P_a(U)$ 是否为真;
- [0116] 系统对用户的环境信息 E_a 进行动态评估,判断 $P_{env}(U, E_a)$ 是否为真;
- [0117] 通过联合权限验证,综合角色、属性和环境评估结果,判断用户是否具备访问权限,若果 $P_{final}(U) = true$,则允许用户解密访问加密数据;否则,拒绝访问。
- [0118] 进一步的,作为上述实施例优选的实施方案,提出一种基于数据安全架构的一物一码多重加密系统,包括:
- [0119] 初始加密模块,用于根据数据的不同类型,将数据划分为独立模块,使用对称加密算法对每个数据模块进行初始加密,并通过非对称加密算法对对称加密的密钥进行加密;
- [0120] 混沌加密模块,用于在对称加密后,加入混沌理论中的随机参数,根据混沌加密算法对数据进行进一步加密,并使用时间戳为每个数据模块添加时间标记;
- [0121] 层级加密模块,用于根据商品信息的敏感性和用户的访问行为,智能决定加密算法的层级;
- [0122] 访问请求解密判断模块,用于对访问加密数据请求,通过基于属性的权限控制模型和基于角色的权限控制模型进行联合验证,并通过基于属性的访问控制模型结合用户的环境属性动态评估访问权限,进一步进行权限控制,根据动态权限评估结果,允许或拒绝用户对数据的解密访问;
- [0123] 一物一码生成模块,用于将加密数据打包,并生成包含时间戳和数字签名的动态二维码,并将加密后的数据模块嵌入生成的动态二维码。
- [0124] 所述混沌加密模块具体包括:
- [0125] 混沌序列生成单元,用于使用洛伦兹系统生成混沌序列;
- [0126] 密文混沌加密单元,用于将生成的混沌序列与初始密文通过异或操作进行结合,生成新的加密结果;
- [0127] 时间戳单元,用于加入时间戳并将其与加密后的数据模块进行绑定;
- [0128] 数字签名单元,用于使用发送方的私钥对时间戳和混沌加密后的数据模块进行签名。
- [0129] 所述层级加密模块具体:
- [0130] 商品信息敏感性分类单元,用于对商品信息进行敏感性分类,基于商品信息的敏感性等级赋予其相应的加密策略,所述敏感性等级包括高、中、低;
- [0131] 访问信息特征值计算单元,用于实时监控用户的访问信息,所述访问信息包括访问频率、位置、设备信息和登录时间,通过对这些信息进行多维特征提取,计算用户行为特征值;
- [0132] 智能加密算法触发单元,用于根据商品信息的敏感性系数和用户行为特征值通过智能加密算法触发条件公式定义加密层次。
- [0133] 所述访问请求解密判断模块具体包括:
- [0134] RBAC访问判定单元,用于对于访问请求,系统通过基于角色的权限控制模型对用户进行初步验证,其中每个用户关联一个或多个角色,系统根据用户的角色决定其初步访问权限;

[0135] ABAC访问判定单元,用于通过基于属性的权限控制模型对用户的属性进行验证;

[0136] 环境属性判断单元,用于结合用户的环境属性进行动态评估,所述环境属性包括时间、地理位置和设备类型;

[0137] 联合验证单元,用于通过联合权限验证模型,将角色权限、属性权限和环境属性进行综合评估。

[0138] 进一步的,作为本实施例优选的实施方案,上述系统提供开放API接口、集成模式、数据导入三种方式,与第三方平台无缝数据交换,实现数据的即时同步和更新;数据集成过程中,系统采用高效的数据映射和转换工具,智能地将第三方数据转换为系统可识别和处理的格式,确保数据的一致性和准确性;利用OAuth 2.0授权机制,系统确保第三方平台接入的安全性,防止未授权访问和数据泄露;采用SSL/TLS协议的使用,保障与第三方平台之间的数据传输过程安全加密,抵御了潜在的网络攻击和数据截取风险;另外,通过错误处理机制和日志记录系统,能够实时监控并记录数据对接过程中的任何异常,确保及时发现并响应安全威胁。

[0139] 以上所述仅是本发明的优选实施方式,应当理解本发明并非局限于本文所披露的形式,不应看作是对其他实施例的排除,而可用于各种其他组合、修改和环境,并能够在本文所述构想范围内,通过上述教导或相关领域的技术或知识进行改动。而本领域人员所进行的改动和变化不脱离本发明的精神和范围,则都应在本发明所附权利要求的保护范围内。

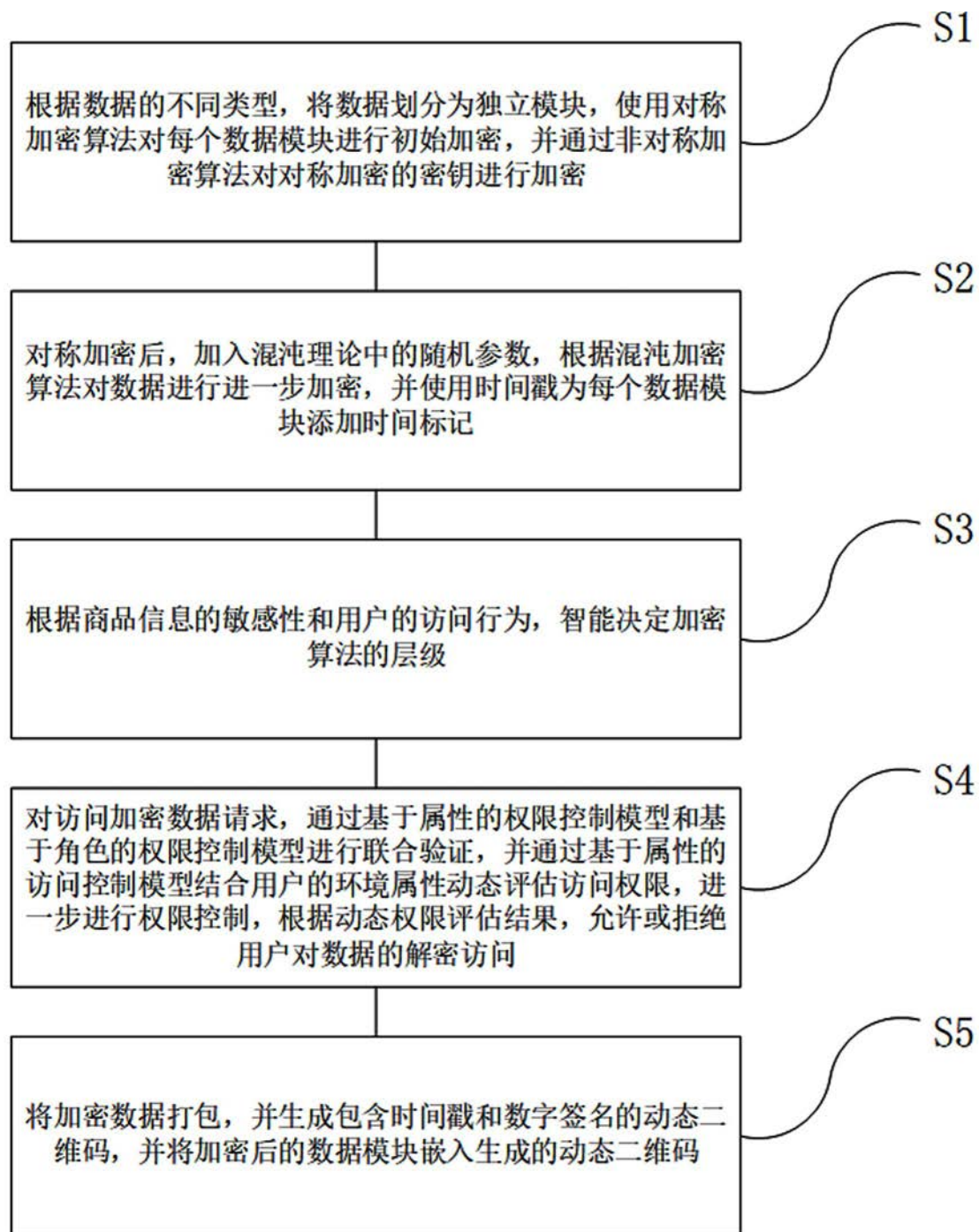


图1