一种基于 LDAP 的属性加密模型

麻付强[1,2],徐　峥[1],苏振宇[1],亓开元[1]
(1. 浪潮(北京)电子信息产业有限公司,北京 100085;
2. 浪潮集团,山东 济南 250101)

摘　要:现有的基于属性加密方案通常采用属性权威来进行属性认证和密钥管理,一旦属性权威不可信或者受到攻击则云计算系统的数据安全将无法得到保证。为了提高基于属性加密系统的整体安全性,提出了一种基于 LDAP(轻型目录访问协议)的属性加密模型。该模型利用 LDAP 和密钥管理模块代替传统属性加密中的属性权威,LDAP 部署在组织内部,与共享数据的云存储模块实现权限分离。组织内部的 LDAP 系统管理用户身份的安全认证和属性管理,密钥管理模块实现属性密钥的生成与存储。同时,密钥管理模块由密钥存储模块和属性判别点组成,用户将属性加解密操作安全的外包给密钥管理模块,且加解密操作在密钥管理模块的可信执行环境中进行。可信执行环境通过采用 Intel SGX 的内存加密来动态保护密钥和加解密过程。云存储模块由存储中心和访问决策点组成,为基于属性加密的密文提供存储。安全性分析表明该方案能够有效保障数据机密性,并有效降低了用户的计算量,实现了密钥的安全存储。

关键词:属性加密;轻型目录访问协议;密钥管理;数据共享;软件防护扩展
中图分类号:TP311　　**文献标识码**:A　　**文章编号**:1673-629X(2023)06-0147-06
doi:10.3969/j.issn.1673-629X.2023.06.022

An Attribute-based Encryption Model with LDAP

MA Fu-qiang[1,2],XU Zheng[1],SU Zhen-yu[1],QI Kai-yuan[1]
(1. Inspur (Beijing) Electronic Information Industry Co.,Ltd.,Beijing 100085,China;
2. Inspur Group Co.,Ltd.,Jinan 250101,China)

Abstract:The existing attribute-based encryption generally uses the authority to manage the attributes and keys. Once the authority is not trusted or attacked,the data security of cloud computing cannot be guaranteed. In order to improve the overall security of the attribute-based encryption,an attribute-based encryption model with LDAP (ABE-LDAP) is proposed. The authority in traditional ABE is replaced with the LDAP and key management module. LDAP is deployed within the organization and separated from the cloud storage module. The LDAP can implement the security authentication and attribute management of user's identity,and key management module can realize the generation and storage of attribute keys. At the same time,key management module consists of the key storage module and attribute discrimination points which can outsource the encryption and decryption of attributes and can perform encryption and decryption operations in the trusted execution environment (TEE). The TEE uses memory encryption of Intel SGX to dynamically protect keys and cryptography processes. The cloud storage module consists of the storage center and access decision point which provide the storage for ciphertext. The security analysis shows that the scheme can effectively guarantee the confidentiality of data, reduce the computational complexity of users,and realize the secure storage of keys.

Key words:attribute-based encryption;lightweight directory access protocol (LDAP);key management;data sharing;software guard extensions

0　引　言

随着互联网、5G 和云计算技术的快速发展,越来越多的用户和企业将数据存储在云计算平台上,实现云存储或者云共享,以提高资源利用率,降低开发及运维成本[1-2]。通常情况下,用户数据在云计算平台中并不是以加密的形式进行存储,对数据的访问控制是由云计算完成的。如果云计算平台不可信或者遭受黑客入侵,用户数据将面临信息泄露的威胁,因此在共享之前对数据进行加密是必要的。

传统的加密机制无法实现复杂云计算环境下一对

收稿日期:2022-08-11　　**修回日期**:2022-12-14
基金项目:广东省重点领域研发计划资助(2020B010165002)
作者简介:麻付强(1991-),男,中级工程师,博士,通信作者,研究方向为网络安全、密码协议、云计算安全。

多的细粒度访问控制功能。因此,在不可信的云计算环境中实现信息安全,确保用户数据的合法授权访问成为了科学人员的研究热点。为了最大限度地保护数据的隐私安全,实现更细粒度的访问控制,研究人员提出了基于属性的加密机制。

基于属性加密(Attribute-Based Encryption,ABE)是从基于属性的访问控制发展来的[3]。Sahai[4]首次提出了基于属性的加密,并实现了数据隐私保护和细粒度访问控制功能。ABE 利用授权属性集构造一个访问控制结构,实现对消息进行加密和解密。其特点是将属性作为公钥,来保证 ABE 的密文能够被多个不同用户的私钥解密。

ABE 是一种一对多的加密模式,能够对加密后的信息进行细粒度的访问控制。ABE 有两大基本类型,密钥策略 ABE(KP-ABE)和密文策略 ABE(CP-ABE)[5]。KP-ABE 中,密文与属性集合关联,私钥与访问结构关联,用于审计日志,付费电视等。CP-ABE 中,密文与访问结构关联,私钥与属性集合关联,当解密方拥有的属性匹配策略树成功时,才能获得解密密钥,获得对资源的访问权,用于云共享、安全邮件列表等。两种策略都是当且仅当属性集合满足访问结构时,才能正确解密。因此,基于属性的加密方案特别适用于在保证云平台用户隐私的前提下,对数据进行机密性保护。

杨腾飞[6]结合访问控制、基于属性加密、对象存储等技术,提出了一种层次化授权访问控制模型,提高了基于属性加密方案的访问控制策略的灵活性。郑芳[7]将基于属性加密应用到身份认证系统中,利用移动 APP 作为密钥生成中心,以指纹多个特征提取模板与其它特征作为属性,服务器端在不知道用户指纹信息的前提下,根据用户输入的特征解密,以此证明该账号和密码属于用户本人。吴光强[8]针对传统 CP-ABE 方案中存在的密钥泄露等问题,提出了一个多授权机构支持策略更新的 CP-ABE 方案,并将策略更新及密文更新过程交给服务器执行,有效地降低了本地的计算开销和数据传输开销。

上述大多数基于属性加密方案[9-11]均需要属性权威(Attribute Authority,AA)。不同于云服务器,属性权威是基于属性加密系统中唯一可信的第三方。授权中心负责生成系统的公共参数,并生成系统公钥和主密钥。授权中心根据用户具有的属性信息将对应私钥集合发送给用户。系统所有密钥均有属性权威产生并保存,用户没有控制权限。属性权威被恶意攻击时,可利用用户的密钥进行解密,使得用户数据的机密性受到威胁[12]。

针对此问题,Chase[13]提出一个分布式 KP-ABE 方案,利用多个属性权威解决了密钥托管问题,降低了密钥泄露的风险。张星[14]利用密钥生成中心和属性权威协同生成用户密钥,属性权威只有部分用户密钥,使得密钥降低了对属性权威安全性的依赖。Lin[15]采用密钥分发和联合的零秘密共享技术提出了一种无认证中心的多授权机构的 ABE 方案,但是数据拥有者无法指定访问控制策略,无法有效地应用到数据共享系统中。Chen[16]提出了一种多属性权威的 ABE 方案,每个属性权威之间不需要交换信息来产生公共参数,且能够保证常数级密文长度。王于丁[17]提出了一种包含访问权限的 ABE 模型,通过设置权限控制密钥加密云中数据。

因此,云计算系统中可信的权威机构增加了云计算系统的复杂度。其次,随着属性集合的增加,用户解密的计算量会线性增长。为了解决上述问题,该文提出了一种基于 LDAP 的属性加密模型。LDAP 是轻量级目录访问协议(Light Directory Access Protocol)[18],目录是一个以一定规则排列的对象的属性集合,是一个存储着关于对象各种属性的特殊数据库,可以用于实现账号管理、安全策略管理等。因此,利用 LDAP 和密钥管理模块代替传统属性加密中的授权机构方案,利用组织内部的 LDAP 系统实现用户身份的安全认证和属性管理。

同时,用户将属性解密操作安全的外包给密钥管理模块,且在密钥管理模块的可信执行环境中进行加解密操作[19-21],保证密钥始终处于密钥管理模块的根密钥保护下。Intel SGX(Software Guard Extensions)是一种通用的可信执行环境,在应用程序的地址空间中划分出一块被保护的区域,为容器内的代码和数据提供机密性和完整性的保护,免受拥有特殊权限的恶意软件的破坏。Intel SGX 具有较小的可信计算基础并能实现物理隔离。通过将密钥使用和基于属性加密的关键代码运行在 Intel SGX 提供的安全加密内存中,保证程序运行过程中,攻击者无法窥探内存。有效地降低了用户计算负载,并提高了系统的安全性。

1 理论基础

设 q 是一个大素数,G 和 G_T 均是阶为 q 的循环群。$g \in G$ 是 G 的生成元,则双线性映射 $e: G \times G \rightarrow G_T$ 为一个双线性对。对于 $\forall g \in G$,任意 $a, b \in Z_p$(Z_p 为素数 C_1 阶循环群)满足以下特征:

双线性:有 $e(g^a, g^b) = e(g,g)^{ab}$;

非退化性:满足 $e(g,g) \neq 1$;

可计算性:对于任意的 $g \in G$,存在一个给定安全常数相关的多项式时间算法,可以高效地计算 $e(g,h)$。

2　一种基于 LDAP 的属性基加密模型

该文采用 LDAP 与密钥管理模块代替属性权威,同时属性解密操作由密钥管理中的 SGX 模块[19]执行,降低了用户计算负载,并提高了系统的安全性。

2.1　方案模型

一种基于 LDAP 的属性加密模型包括:多个组织和一个云计算平台,实现每个组织内部的云存储以及云共享。其中每个组织包含多个数据使用者、多个数据拥有者、一个 LDAP 身份提供模块;云计算平台包含统一的云存储模块、多个密钥管理模块。其中每个密钥管理模块对应一个组织,实现组织的安全密钥管理。云存储模块由存储中心和访问决策点组成;密钥管理模块由密钥存储模块和属性判别点组成。在每个组织内部,用户通过安全通道与云计算平台通信,模型如图 1 所示。

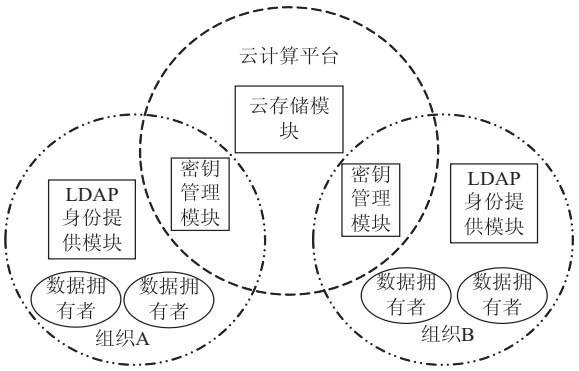

图 1　基于属性加密的系统模型

2.1.1　数据拥有者功能

向 LDAP 身份提供模块进行注册,成为合法用户,并获得对应的属性集合;制定共享数据的授权属性集合,建立相应的访问控制策略,形成基于属性的访问控制矩阵;请求密钥管理模块生成授权属性集合对应的密钥;将数据根据访问控制矩阵进行加密;将基于属性加密的密文上传到云存储模块;根据基于属性加密的对称密钥解密加密数据获得明文数据。

2.1.2　数据使用者功能

向 LDAP 身份提供模块进行注册,成为合法用户,并获得对应的属性集合;根据基于属性加密的对称密钥解密加密数据获得明文数据。

2.1.3　LDAP 身份提供模块功能

为用户提供身份注册功能;验证用户的属性合法性;验证用户登录系统的合法性。

2.1.4　云储存模块功能

为基于属性加密的密文提供存储;访问决策点根据访问控制矩阵验证用户属性集合的合法性。

2.1.5　密钥管理模块功能

为数据拥有者生成基于属性加密的系统公共参数,为组织内所有用户提供公共参数;根据文件标识、属性生成非对称密钥,非对称密钥包括对应的公钥和私钥;在可信执行环境中为数据文件生成对称加密密钥,并通过数据拥有者的公钥加密并发送给数据拥有者;属性判别点从 LDAP 获得用户的属性集合,并验证属性对应的密钥访问权限;在可信执行环境中实现对基于属性加密的对称密钥进行解密,并将解密后的对称密钥通过数据使用者的公钥加密并发送给数据使用者。所有加解密操作均在 intel 的 SGX 中操作,加密安全存储相应的非对称密钥和对称密钥,保证系统安全。

2.2　方案实施

基于 LDAP 的属性加密模型共 5 个阶段:用户注册阶段、系统参数设置、密钥生成、加密阶段、解密阶段。

2.2.1　用户注册阶段

如图 2 所示,用户(数据拥有者、数据使用者)经过身份认证模块向 LDAP 身份提供模块进行身份注册,包括用户名和密码,同时注册相应的属性集合。LDAP 身份提供模块负责验证用户属性的合法性。用户登录系统时,由 LDAP 身份提供模块验证用户身份的合法性,并返回用户的属性集合。用户根据用户 id ,向密钥管理模块注册一对非对称密钥 pk_u 、sk_u ,并通过安全通道发送给用户。非对称密钥由项目密钥加密,项目密钥由密钥管理模块的根密钥加密,根密钥安全存储在硬件安全模块(HSM)[22]中。

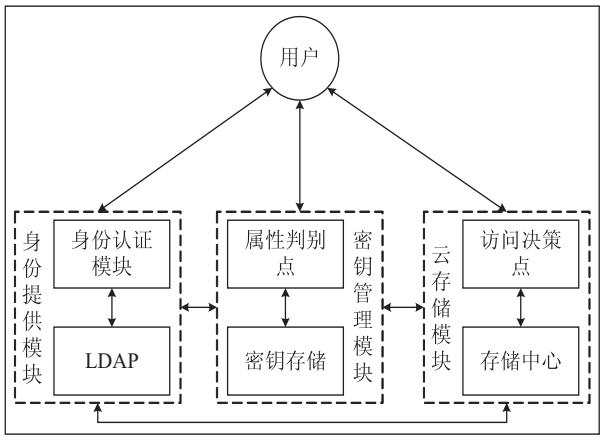

图 2　基于 LDAP 的属性加密示意图

2.2.2　系统参数及密钥生成

数据拥有者请求密钥管理模块生成系统参数。密钥管理模块根据输入的安全参数 λ ,生成全局参数 GP 。

密钥管理模块在可信执行环境中生成一个对称密钥 sk。如表 1 所示,在可信执行环境中,根据文件标识 ID_f 、共享数据的授权属性集合 S 和全局参数 GP ,生成基于属性加密的公钥集合 PK 和私钥集合 SK,并将

公私钥加密存储在密钥管理模块。采用数据拥有者的公钥 pk_u 将对称密钥 sk 和公钥集合 PK 加密发送给数据拥有者。

表 1 密钥管理模块的密钥存储结构

文件标识	全部参数	属性	密钥	
ID_f	GP	属性 1	公钥 1	私钥 1
		属性 2	公钥 2	私钥 2
		属性 3	公钥 3	私钥 3
		属性 4	公钥 4	私钥 4
		…	…	…
		属性 K	公钥 K	私钥 K

2.2.3 加密阶段

数据拥有者根据共享数据的授权属性集合制定相应的访问控制策略,建立基于属性的访问控制矩阵 $\boldsymbol{A}$。采用私钥 sk_u 解密得到对称密钥 sk 和公钥集合 PK。利用对称密钥 sk 加密共享文件 M,形成文件密文 C_1。利用公钥集合 PK 和访问控制矩阵 $\boldsymbol{A}$ 加密对称密钥 sk,形成属性密文 CT = $\{C_2, C_3, C_4, C_5\}$。因此,最终基于属性加密的密文为 $C = \{ID_f, (A, \rho), C_1, CT, sign\}$,其中 sign 表示数字签名。将基于属性加密的密文 C 上传到云存储模块。

2.2.4 密钥生成阶段

密钥管理模块根据数据使用者的属性集合、全局参数 GP、私钥集合 SK 生成相应的私钥集合 K_{id}。

2.2.5 解密阶段

数据使用者从云存储模块请求基于属性加密的密文 C。云存储模块中的访问决策点基于数据使用者 id 从 LDAP 系统中获得数据使用者对应的属性集合。根据基于属性加密的密文 C 中的访问控制矩阵 $\boldsymbol{A}$ 判定数据使用者对应的属性集合的访问合法性。如果数据使用者具有访问权限,将基于属性加密的密文 C 返还给数据使用者。数据使用者利用属性密文 CT 访问密钥管理模块。密钥管理模块中的属性判别点基于数据使用者 id 从 LDAP 系统中获得数据使用者对应的属性集合。根据数据使用者对应的属性集合和文件标识 ID_f 确定属性集合对应的私钥集合。将私钥集合、属性密文 CT、用户公钥 pk_u 发送到密钥管理模块中的可信执行环境中。由可信执行环境对对称密钥 sk 进行解密,并用数据使用者 pk_u 加密发送给数据使用者。数据使用者采用私钥 sk_u 解密得到对称密钥 sk,并用对称密钥 sk 解密文件密文 C_1,获得共享文件 M。

3 算法设计

在基于 LDAP 的属性加密模型中,访问控制矩阵被嵌入到密文中,而密钥被绑定到一组属性中。

3.1 系统参数及密钥生成

首先,密钥管理模块根据数据拥有者的请求进行全局参数设置,函数为:Global Setup(λ) → GP。

一个双线性群 G 的阶为 q,$g_1 \in G$。一个 Hash 函数具有映射功能 H:$\{0,1\}^* \rightarrow G$。全局参数为:GP = $\{g_1, G, G_T, Z_p, q, p, H\}$。

根据文件标识 ID_f、共享数据的授权属性集合 S、全局参数 GP、数据拥有者的公钥 pk_u 向密钥管理模块请求生成一个对称密钥和共享数据的授权属性集合对应的非对称密钥。函数为:GKeyGen(ID_f, S, GP, pk_u) → PK, SK, sk。

选择两个随机数 $\alpha_i, y_i \in Z_p$,其中 i 是访问控制矩阵中的第 i 属性,共有 K 个属性。对应的公钥为 PK = $\{e(g_1, g_1)^{\alpha_i}, g_1^{y_i}\}$,其私钥为 SK = $\{\alpha_i, y_i\}$,$i \in \{1, 2, \cdots, K\}$。

3.2 加密阶段

数据拥有者对文件进行基于属性加密,函数为:Encrypt(M, (A, ρ), GP, {PK}, sk) → C。

加密消息为 M,访问控制矩阵为 $K \times L$ 的矩阵 $\boldsymbol{A}$,其中 K 是矩阵 $\boldsymbol{A}$ 的行数,L 是矩阵 $\boldsymbol{A}$ 的列数。ρ 是一个属性映射函数,将属性与访问控制矩阵的行联系起来。选择一个随机秘密 $s \in Z_p$,一个随机向量 $\boldsymbol{v} \in Z_p^L$,其中 v 的第一个元素为 s,其他为随机数。$\lambda_i = \boldsymbol{A}_i \boldsymbol{v}$,$i \in \{1, 2, \cdots, K\}$ 为第 i 个属性,A_i 为 $\boldsymbol{A}$ 的第 i 行。同时对于矩阵 $\boldsymbol{A}$ 的每一行 A_i 选择一个随机数 $r_i \in Z_p$。

数据拥有者利用对称密钥 sk 加密文件,形成文件密文 C_1。

$$C_1 = Enc_{sk}(M) \tag{1}$$

数据拥有者根据访问控制结构和公钥集合对对称密钥 sk 进行基于属性加密,将这些访问控制矩阵封装到密文中,形成属性密文 CT = $\{C_2, C_3, C_4, C_5\}$。因此,基于属性加密的密文为 $C = \{ID_f, (A, \rho), C_1, CT, sign\}$,其中 sign 表示数字签名。

$$C_2 = sk \cdot e(g_1, g_1)^s \tag{2}$$

$$C_{3,i} = e(g_1, g_1)^{\lambda_i} e(g_1, g_1)^{\alpha_{\rho(i)} r_i} \tag{3}$$

$$C_{4,i} = g_1^{r_i} \tag{4}$$

$$C_{5,i} = g_1^{y_{\rho(i)} r_i} \tag{5}$$

基于属性加密的密文 $C = \{ID_f, (A, \rho), C_1, CT, sign\}$ 上传到云存储模块。

3.3 密钥生成阶段

密钥管理模块根据数据使用者的属性集合、全局参数 GP、私钥集合 SK 生成相应的私钥集合 K_{id},函数为 KeyGen(id, x, S, GP, SK) → $K_{x,id}$。

$$K_{x,id} = g_1^{\alpha_x} H(id)^{y_x} \tag{6}$$

$x \in \{1, 2, \cdots, K\}$ 为第 x 个属性,数据使用者的属

性集合为共享数据的授权属性集合 S 的子集。

3.4　解密阶段

解密的时候,用户只有自身属性集合对应的私钥集合,只要符合访问控制矩阵的都可以解密。解密函数为: $\mathrm{Decrypt}(C,K_{\mathrm{id}},\mathrm{GP})\rightarrow \mathrm{sk}$, $\mathrm{Dec}_{\mathrm{sk}}(C_1)\rightarrow M$ 。

根据用户拥有的属性集合,从 $C_{3,\rho(x)}$, $C_{4,\rho(x)}$, $C_{5,\rho(x)}$ 中获取对应的数据。其中, $\rho(x)$ 将数据使用者的属性 x 映射到基于属性的访问控制矩阵 $\boldsymbol{A}$ 的第 $\rho(x)$ 行。

$$C_{3,\rho(x)}e(H(\mathrm{id}),C_{5,\rho(x)})/e(K_{x,id},C_{4,\rho(x)})=e(g_1,g_1)^{\lambda_{\rho(x)}} \tag{7}$$

计算常量 $c_x\in\mathbb{Z}_N$,使得 $\sum_x c_xA_{\rho(x)}=(1,0,\cdots,0)$ 。计算 $e(g_1,g_1)^s$,其中 $\lambda_{\rho(x)}=A_{\rho(x)}v$, $v\cdot(1,0,\cdots,0)=s$ 。

$$\prod_x\left(e(g_1,g_1)^{\lambda_{\rho(x)}}\right)^{c_x}=e(g_1,g_1)^s \tag{8}$$

对对称密钥进行解密,获得对称密钥 sk:

$$\mathrm{sk}=C_2/e(g_1,g_1)^s \tag{9}$$

利用对称密钥 sk 解密文件密文 C_1 ,获得明文数据。

$$M=\mathrm{Dec}_{\mathrm{sk}}(C_1) \tag{10}$$

4　安全性分析

4.1　机密性

数据机密性既保证数据为授权者所有而不会泄露给未经授权者。在 ABE-LDAP 中,仅当用户属性集合满足基于属性的访问控制矩阵,才能从云存储模块获取加密数据,未经授权的用户因无法满足系统的访问控制结构,所以保证了数据的机密性。

基于属性加密的密钥始终存在密钥管理模块中,未授权用户不能获取属性集合对应的密钥,保证了密钥的机密性。

仅当用户属性集合满足基于属性的访问控制矩阵,密钥管理模块才执行对称密钥的解密过程,未授权用户无法获得加密数据的对称密钥,保证了数据的机密性。

同时密钥管理模块所有加解密操作均在可信执行环境中执行,保证了密钥的安全性。

4.2　抗合谋攻击

抗合谋是 ABE 系统要求的重要安全特性之一。合谋攻击是指即使每个用户不能单独解密密文,他们可以通过组合他们的属性来解密密文。在 ABE-LDAP 中,由于用户的属性密钥与用户身份标识结合,因而阻止了多个用户之间的合谋攻击。

5　性能分析

该文使用了 CPU 型号为 Intel(R) Xeon(R) Gold 6326 CPU@ 2. 90 GHz,内存为 256 G,操作系统为 Ubuntu20. 04 的支持 SGX 平台,部署安装了基于 LDAP 的属性加密模型。本节从 ABE-LDAP 复杂度、SGX 的机密性及 ABE-LDAP 的加解密时间进行性能分析。

5.1　ABE-LDAP 算法复杂度

下面将文中模型与 Chen 方案[16]、DACPCC 方案[17]进行对比分析,如表 2 所示。设 $|s_1|$ 为群 G 的元素长度, $|s_2|$ 为群 G_T 的元素长度, $|s_3|$ 为群 Z_p 的元素长度 , $|M|$ 是选取的数据明文的空间大小, n_a 为考虑范围内的所有属性数量, n_u 为某个用户具有的属性数量, E 为群 G 的幂运算复杂度, E_T 为群 G_T 的幂运算复杂度, P 为群 G 的双线性运算复杂度。

通过理论分析可知,文中方案在加密、解密开销上与 Chen 方案和 DACPCC 方案类似。但是文中方案的属性解密执行是在云端的密钥管理模块中,显著降低了用户的计算开销,提高了系统性能。在密文长度方面,文中方案采用层次加密方案,密文长度相对较大,但是安全性相对更高。

表 2　ABE-LDAP 性能分析

指标	Chen	DACPCC	ABE-LDAP
公钥长度	$n_a\lvert s_1\rvert+n_a\lvert s_2\rvert$	$n_a\lvert s_1\rvert+n_a\lvert s_2\rvert+\lvert s_2\rvert$	$n_a\lvert s_1\rvert+n_a\lvert s_2\rvert$
私钥长度	$2n_a\lvert s_3\rvert+\lvert s_3\rvert$	$2n_a\lvert s_3\rvert+\lvert s_3\rvert$	$2n_a\lvert s_3\rvert$
密文长度	$n_a\lvert s_1\rvert+n_a\lvert s_2\rvert+\lvert s_1\rvert$	$n_a\lvert s_1\rvert+n_a\lvert s_2\rvert+3\lvert s_1\rvert+\lvert M\rvert$	$n_a\lvert s_1\rvert+2n_a\lvert s_2\rvert+\lvert s_2\rvert+\lvert M\rvert$
加密开销	$O(n_aE+n_aE_T)$	$O(n_aE+n_aE_T)$	$O(n_aE+n_aE_T)$
解密开销	$O(n_uP)$	$O(n_uP)$	$O(n_uP)$

5.2　ABE-LDAP 的机密性测试

分别在采用 SGX 和不采用 SGX 技术的情况下,验证密钥管理模块的机密性,以验证密钥信息和加解密过程是否存在泄露风险。在密钥管理模块中添加机密性测试字符串“0123456789abcdef0a1b2c3d4e5f0123456789abcdef”,来验证字符串是否明文出现在

内存中。利用 RFSD、rfdk-gui、winhex 等工具进行内存抓取。

如图 3 所示,密钥管理模块没有运行在 SGX 中,可以从内存中显示出测试字符串信息。如图 4 所示,密钥管理模块运行在 SGX 中,无法从内存中获取测试字符串信息。因为密钥管理模块属于 SGX 的保护范围,除了 SGX 的 Enclave 结构外,外界无法获取其中任何数据及代码信息。实现了密钥管理模块中密钥和加解密运算过程的机密性。

图 3 未采用 SGX 的密钥管理模块机密性

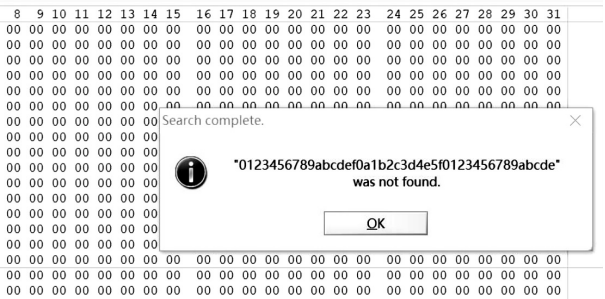

图 4 采用 SGX 的密钥管理模块机密性

5.3 ABE-LDAP 的加解密测试

本节对 ABE-LDAP 的加解密性能分别进行了测试。所有属性数量 n_a 设置为 6,某个用户具有的属性数量 n_u 设置为 4。密钥管理模块分别采用 SGX 技术和不采用 SGX 技术。对基于属性加解密过程进行了 5 次实验。通过图 5 和表 3 可以得出,采用 SGX 保护密钥管理模块会降低整个系统的性能,但是性能开销相对较小,在系统可以接受的范围内。同时,密钥管理模块可以安全的部署在云平台上,实现密钥和解密运算的机密性。

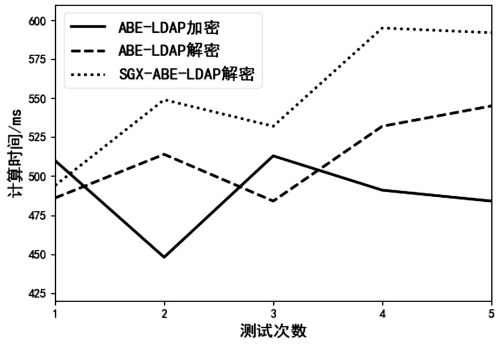

图 5 ABE-LDAP 的加解密性能

表 3 ABE-LDAP 的平均加解密时间

算法	平均时间/ms
ABE-LDAP 加密	494
ABE-LDAP 解密	512
SGX-ABE-LDAP 解密	552

6 结束语

该文利用 LDAP 和密钥管理模块代替传统属性加密中的授权机构,利用组织内部的 LDAP 系统实现用户身份的安全认证和属性管理,利用密钥管理模块实现属性密钥的生成与存储。同时,用户将属性解密操作安全的外包给密钥管理模块,且在密钥管理模块的可信执行环境中进行加解密操作。安全性分析表明,该方案能够有效保障数据机密性,实现安全高效和细粒度数据访问控制,并有效降低了用户的计算量,实现了密钥的安全存储。

参考文献:

[1] ZHANG Y, DENG R H, XU S, et al. Attribute-based encryption for cloud computing access control: a survey[J]. ACM Computing Surveys, 2020, 53(4): 1-41.

[2] SUN P J. Security and privacy protection in cloud com-puting: discussions and challenges[J]. Journal of Network and Computer Applications, 2020, 160: 102642.

[3] RASORI M, PERAZZO P, DINI G. A lightweight and scalable attribute-based encryption system for smart cities [J]. Computer Communications, 2020, 149: 78-89.

[4] SAHAI A, WATERS B. Fuzzy identity-based encryption [C]//Annual international conference on the theory and applications of cryptographic techniques. Aarhus: Springer, 2005: 457-473.

[5] ZHANG J, XIN Y, GAO Y, et al. Secure ABE scheme for access management in blockchain-based IoT[J]. IEEE Access, 2021, 9: 54840-54849.

[6] 杨腾飞,申培松,田 雪,等. 对象云存储中分类分级数据的访问控制方法[J]. 软件学报,2017,28(9):2334-2353.

[7] 郑 芳,冯丽萍,李平珍,等. 一种利用属性加密进行身份认证的隐私保护方案[J]. 网络安全技术与应用,2020(2):33-36.

[8] 吴光强. 适合云存储的访问策略可更新多中心 CP-ABE 方案[J]. 计算机研究与发展,2016,53(10):2393-2399.

[9] 王光波,刘海涛,王晨露,等. 云存储环境下可撤销属性加密[J]. 计算机研究与发展,2018,55(6):1190-1200.

[10] LI J, YAO W, HAN J, et al. User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage[J]. IEEE Systems Journal, 2017, 12(2): 1767-1777.

[11] 齐 芳,李艳梅,汤 哲. 可撤销和可追踪的密钥策略属性基加密方案[J]. 通信学报,2018,39(11):63-69.

[12] 孙 磊,赵志远,王建华,等. 云存储环境下支持属性撤销的属性基加密方案[J]. 通信学报,2019,40(5):47-56.

[13] CHASE M, CHOW S S M. Improving privacy and security in multi-authority attribute-based encryption[C]//Proceedings of the 16th ACM conference on computer and communications security. New York: ACM, 2009: 121-130.

[14] 张 星,文子龙,沈晴霓,等. 可追责并解决密钥托管问题

(下转第 159 页)