DOI:10.3969/j.issn.1007-9580.2021.06.010

# 基于属性基加密的海洋浮标数据安全管理系统的设计与实现

顾震凯[1,2],张绍华[2],李超[2],戴炳荣[2]
(1 上海海洋大学信息学院,上海 201306;
2 上海计算机软件技术开发中心,上海 201112)

**摘要**:针对海洋浮标数据存在被黑客攻击、窃取的问题,在分析北斗海洋浮标系统工作原理的基础上,设计了基于属性基加密的海洋浮标数据安全管理系统。在该系统中设计了数据加解密、数据管理和密钥管理的子系统,设计了包括数据的存储以及数据的请求两个业务流程,做到了对数据的细化到用户属性的安全管控。在此基础上,基于开源的椭圆曲线配对运算库和主流前后端技术实现了该系统,并对多种加解密方案从加密效率、密钥安全和数据共享等方面进行了对比分析。结果显示:本研究所采用的加密方案具有显著优势,与传统的浮标数据管理系统进行对比,该系统融合了对称加密与属性基加密技术,实现了浮标数据的安全保护与数据的细粒度共享。本研究成果可以为浮标数据的信息安全管理,推动渔业信息化、现代化的发展提供参考。

**关键词**:海洋浮标;海洋渔业;北斗卫星;数据管理;属性基加密;信息安全
**中图分类号**:S973;TP315 **文献标志码**:A **文章编号**:1007-9580(2021)06-0072-08

海洋浮标是海洋观测中的重要手段,具有连续、长期、全天候、全天时、稳定可靠等特点[1],能够实现数据的自动采集、自动发送,其通信方式较为多样[2-3]。近海浮标一般采用移动网络通信,远海浮标通常采用卫星通信、北斗短报文等方式[4-5]。

渔业捕捞中,由于鱼类资源时空变化大[6],需要快速寻找中心渔场以提高捕捞效率[7-8]。近年来,海洋浮标通过携带鱼探设备,成为探测渔场的重要手段[9-10],但是由于海洋浮标数据容易受到黑客的攻击窃取,导致渔业公司花费时间与金钱成本投放的海洋浮标没有得到应有的收益[11-13]。目前的研究中,已经有不少研究人员对海洋浮标的数据管理系统给出了研究方案:任鹏等[14]基于R语言与相关Web框架Shiny构建了一个海洋浮标大数据处理平台;朱明垒[15]提出了海洋资料浮标的数据接收系统,但以上方案只是针对海洋浮标数据存储与管理的需求,未考虑数据传输过程中的安全性;张新文等[16]采用对称加密与非对称加密结合的方式设计了海洋浮标数据的管理系统,通过加密来保护数据传输的安全性,但其数据的共享缺乏灵活性,为实现数据的细粒度共享,本研究引入了属性基加密。

属性基加密(ABE)最初由Sahai等[17]提出,根据访问策略的嵌入位置不同,可分为两种[18]:一种是将访问策略嵌入密钥的密钥策略属性基加密(KP-ABE);另一种是将访问策略嵌入密文的密文策略属性基加密(CP-ABE),将访问策略嵌入密文这意味着数据的拥有者可以通过设定不同的访问策略来决定谁可以访问这份数据密文,可以对数据实现细化到用户属性的访问控制。因此,CP-ABE在数据的细粒度共享方面有着广阔的应用前景。

本研究首先对北斗海洋浮标系统的工作模式进行了分析,根据海洋浮标系统的实际工作情况设计了海洋浮标数据安全管理系统的各层架构与功能模块,并基于对称加密与属性基加密设计了数据存储与数据请求的业务流程。最后对系统进行实现,并将多种加密方案进行了对比测试。

**收稿日期**:2021-07-10
**基金项目**:上海市科委项目"上海市软件技术创新服务平台(20DZ2291700)"
**作者简介**:顾震凯(1996-),男,硕士研究生,研究方向:渔业数据管理以及公钥加密。E-mail:gzk0329@gmail.com
**通信作者**:张绍华(1974-),男,博士,副研究员,研究方向:数据治理、区块链。E-mail:zsh@sscenter.sh.cn

## 1　北斗海洋浮标系统介绍

北斗海洋浮标是一种基于北斗卫星的定位与短报文传输进行通信的浮标,除了可以监测洋流的速度以及方向外,还可通过搭载多种传感器为航海、渔业、港工以及海洋开发提供服务[19-20]。北斗海洋浮标以浮球作为浮标体,浮标体上搭载太阳能电池板为整个浮标系统进行供电[21-22],浮标上的数据采集系统将各传感器采集到的数据通过通信系统发送到北斗卫星。岸上的数据中心从北斗卫星接收数据,对数据进行转码[23]和预处理后将数据存储在数据库中,并对数据进行管理。

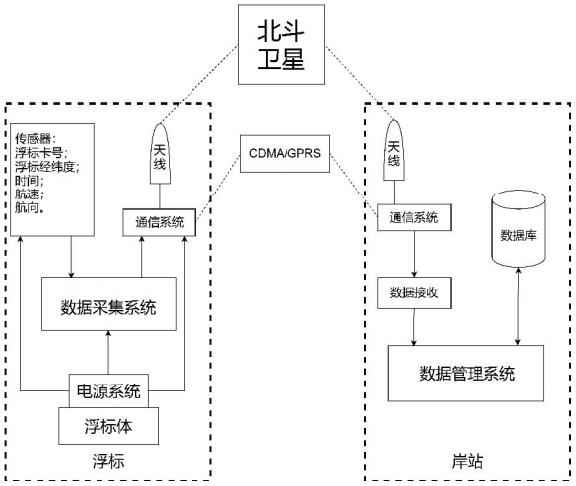


**图 1　海洋浮标与岸基数据接收系统结构**

Fig. 1　The structure of ocean buoy and shore-based data receiving system

## 2　系统设计

### 2.1　系统模块设计

基于可操作性、安全性、可扩展性的原则设计了 3 个子系统,分别为数据加解密子系统、数据管理子系统和密钥管理子系统,具体的功能模块如图 2 所示。其中,数据加解密子系统包括 AES 加解密的实现,CP-ABE 加解密的实现和访问策略的构建等;数据管理子系统包括海洋浮标数据管理,海洋水文数据管理,渔业信息数据管理等;密钥管理子系统负责管理系统中使用的密钥,如 AES 对称密钥,CP-ABE 加解密中的系统公钥 $\delta_{PK}$,系统主密钥 $\delta_{MK}$ 以及用户的私钥 $\delta_{SK}$ 等。

### 2.2　系统总体架构

根据浮标数据管理系统运行的实际需求[24],本系统采用多层分布式框架结构[25]。系统的具体架构如图 3 所示。

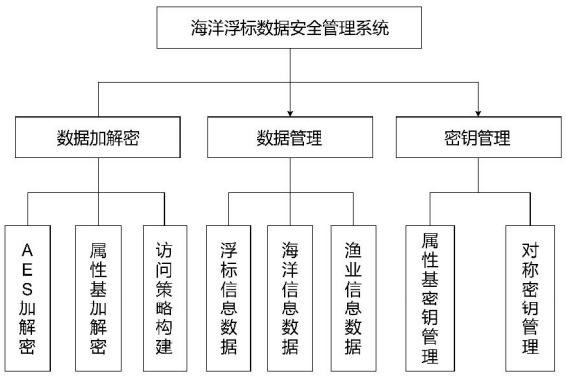


**图 2　海洋浮标数据安全管理系统模块**

Fig. 2　The modules of ocean buoy data security management system

其中,数据层是整个系统的基石,使用 MySQL 数据库对各类海洋浮标数据进行维护管理,使用 Redis 数据库对用户的登录凭证进行有时间限制的存储;逻辑层为系统的具体功能实现,其中数据加解密子系统是对 AES 加解密和属性基加解密以及访问策略的实现,密钥管理子系统是对系统中生成与使用的密钥,如 AES 密钥,属性基加密中的系统公钥 $\delta_{PK}$ 和系统主密钥 $\delta_{MK}$ 以及用户私钥 $\delta_{SK}$ 等的安全保存与管理;表现层为本系统的用户操作界面以及数据呈现界面的实现;用户层为系统的具体使用者,大致可分为渔业的从业人员、渔业领域科研人员和本系统的管理人员等。本研究中使用的相关符号的含义如表 1 所示。

**表 1　相关符号的定义**

Tab. 1　Definition of related symbols

| 符号 | 含义 | 符号 | 含义 |
|---|---|---|---|
| $\delta_{PK}$ | 属性基加密中的系统公钥 | $T_{plain}$ | 数据明文,在具体浮标系统中指未加密的浮标数据 |
| $\delta_{MK}$ | 属性基加密中的系统主密钥 | $T_{enc}$ | 数据密文,在具体浮标系统中指加密后的浮标数据 |
| $\delta_{SK}$ | 属性基加密中的用户私钥 | $\alpha_{KEY}$ | AES 密钥明文 |
| $\delta_{AP}$ | 属性基加密中的访问策略 | $\alpha_{CK}$ | AES 密钥密文 |
| $A$ | 属性基加密中用户的属性集 | $\lambda$ | 在生成 $\delta_{PK}$ 与 $\delta_{MK}$ 时输入的安全参数 |

## 3 系统实现的关键技术

### 3.1 密文策略的属性基加密 CP-ABE 的实现

密文策略的属性基加密(CP-ABE)是将密文与访问策略相关联,用户私钥与属性相关联,不需要知道用户的身份,当用户的属性与密文的访问策略相匹配时,便能使用其私钥解密密文。CP-ABE 的工作流程分为 4 个步骤[26]:

(1)初始化阶段:($\delta_{PK}$,$\delta_{MK}$) = ABE. SetUp($\lambda$),输入安全参数 $\lambda$,生成系统公钥 $\delta_{PK}$ 和系统主密钥 $\delta_{MK}$。

(2)数据加密阶段:$T_{enc}$ = ABE. Encrypt($\delta_{PK}$, $T_{plain}$,$\delta_{AP}$),使用系统公钥 $\delta_{PK}$ 与数据拥有者设置的访问策略 $\delta_{AP}$ 对数据明文 $T_{plain}$ 进行加密,得到密文 $T_{enc}$。

(3)密钥生成阶段:$\delta_{SK}$ = ABE. KeyGen($\delta_{MK}$, A),使用用户的属性集 A,系统主密钥 $\delta_{MK}$,生成用户私钥 $\delta_{SK}$。

(4)密文解密阶段:$T_{plain}$ = ABE. Decrypt($T_{enc}$, $\delta_{SK}$),使用用户私钥 $\delta_{SK}$ 对数据密文 $T_{enc}$ 进行解密,如果用户的属性集 A 满足设置的访问策略 $\delta_{AP}$,则解密成功,得到数据明文 $T_{plain}$。

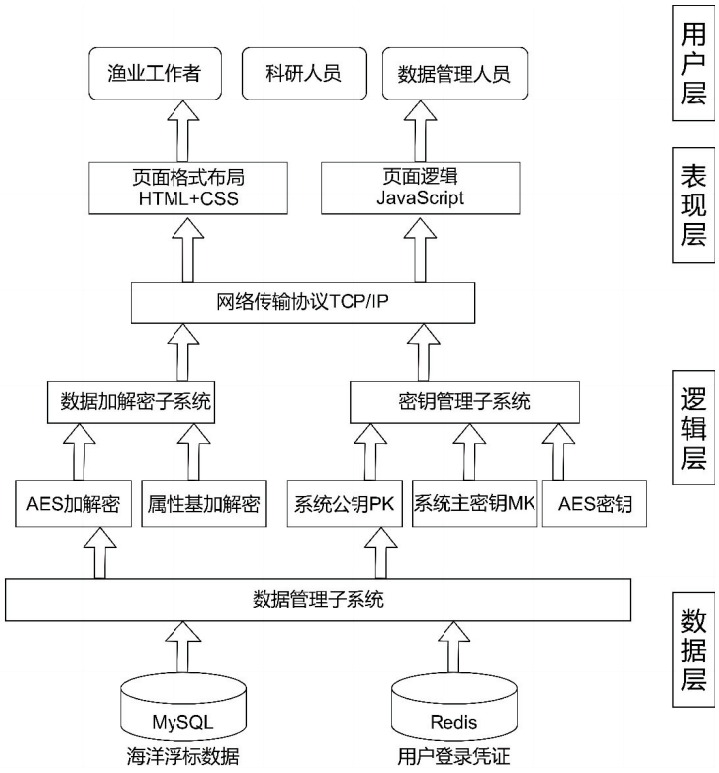


**图 3 系统总体架构**

Fig. 3 The overall architecture of system

### 3.2 数据存储

海洋浮标数据的安全主要体现在存储与分享过程中数据的可靠性、机密性等[27-28]。实现数据安全的核心是加密算法与访问控制[29]。根据海洋浮标数据安全性的实际需求,本系统采用 AES 对称加密与 CP-ABE 加密结合的方法,设计了安全的数据加密与存储的方案。

数据加密并存储的过程如图 4 所示,主要步骤如下。

首先是浮标数据的采集与解码。海洋浮标的各类传感器收集数据,通过北斗卫星短报文的通信形式传输到岸基的数据中心。根据海洋实时数据处理规范,岸基数据中心将接收到的数据进行解码,解码后获得浮标数据 $T_{plain}$。

其次在浮标数据管理中心接收到数据 $T_{plain}$ 后,系统进行初始化工作,密钥管理子系统随机生成一个 AES 密钥 $\alpha_{KEY}$,长度固定为 128 位,并根

据预先设定的安全参数 λ 生成系统公钥 $\delta_{PK}$,系统主密钥 $\delta_{MK}$。接着使用 AES 密钥对 $T_{plain}$ 进行加密,加密后的密文为 $T_{enc}$,根据所加密的浮标数据的类型设置相应的访问策略 $\delta_{AP}$,使用系统公钥 $\delta_{PK}$ 与访问策略 $\delta_{AP}$ 对 $\alpha_{KEY}$ 进行 CP-ABE 加密,生成密钥密文 $\alpha_{CK}$。

最后是数据存储。系统将加密后的浮标数据 $T_{enc}$ 和密钥密文 $\alpha_{CK}$ 存储到数据库中。

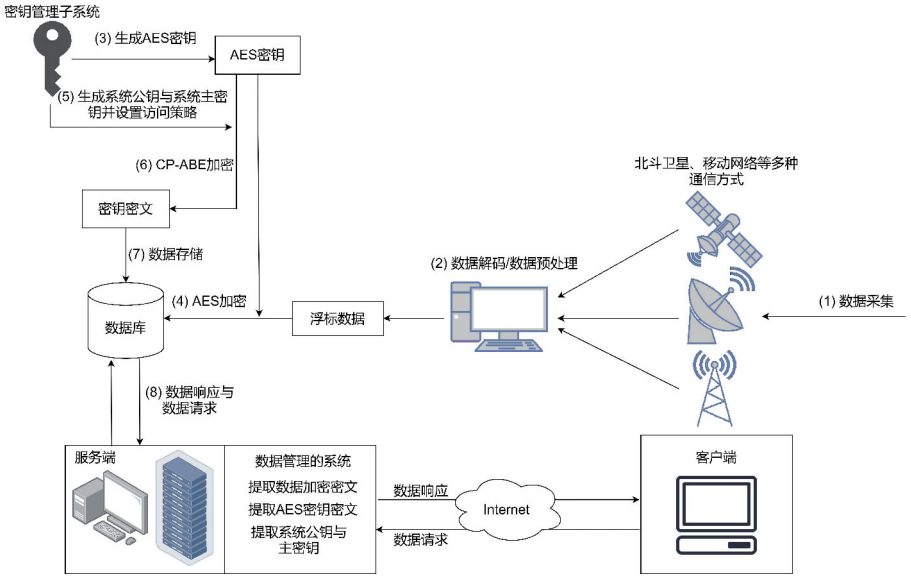


**图 4　海洋浮标数据存储的过程**

Fig. 4　The process of ocean buoy data storage

在浮标数据存储的过程中,通过 AES 密钥对浮标数据进行加密,再使用 CP-ABE 对 AES 密钥进行加密,数据与密钥在传输的过程中均为密文状态,保障了数据的机密性。数据的获取依赖于 AES 密钥的获取,而 AES 密钥则通过 CP-ABE 进行加密,只有属性满足设定访问策略的用户才能够对 AES 密钥进行 CP-ABE 解密,实现了数据的细粒度的访问控制。

### 3.3　数据请求

根据海洋浮标数据安全性的要求,本系统设计了浮标数据请求的方案,支持基于用户属性的细粒度的数据访问控制。

用户请求浮标数据的过程如图 5 所示。

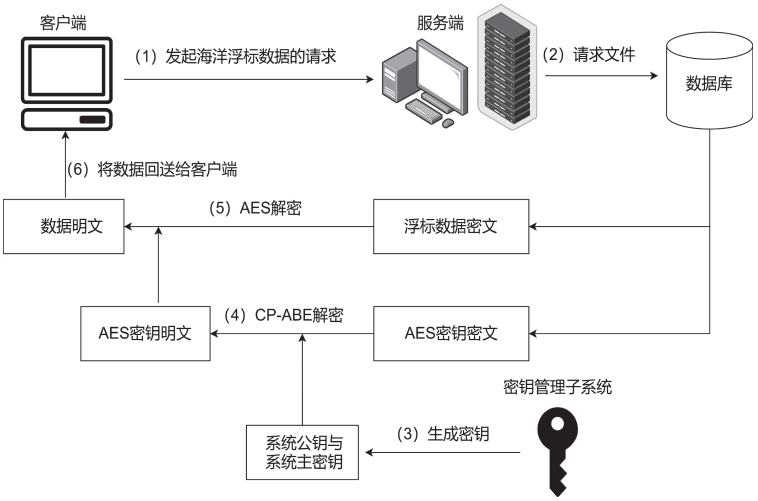


**图 5　海洋浮标数据请求的过程**

Fig. 5　The process of ocean buoy data request

主要步骤如下：

首先客户端用户发起海洋浮标数据的请求。用户在海洋浮标数据管理系统中注册，并登录后，将其请求海洋浮标的编号和自身属性集 A 发送给海洋浮标数据管理系统的服务端。

其次服务端通过接收到的海洋浮标编号在数据库中检索相应浮标的加密数据 $T_{enc}$ 以及相关 AES 密钥的密文 $\alpha_{CK}$。服务端中密钥子系统给出系统主密钥 $\delta_{MK}$、系统公钥 $\delta_{PK}$。

服务端使用系统主密钥 $\delta_{MK}$ 和用户属性集 A 生成用户私钥 $\delta_{SK}$，并使用私钥 $\delta_{SK}$ 对接收到的 AES 密钥的密文 $\alpha_{CK}$ 进行 CP-ABE 解密，如果用户的属性集 A 符合预先设定的访问策略 $\delta_{AP}$，则可成功解密，否则无法解密。CP-ABE 解密完成后得到 AES 密钥 $\alpha_{KEY}$，对接收到的浮标数据密文 $T_{enc}$ 进行 AES 解密，解密后可得到请求的海洋浮标数据的明文 $T_{plain}$。

最后服务端将浮标数据 $T_{plain}$ 回送给用户，用户退出系统，断开连接。至此数据请求的工作完成。

## 4 系统实现

### 4.1 系统实现过程

本系统的实现中，使用 Java 基于 SpringBoot 框架来进行服务端业务模块的开发，Java 版本使用 JDK8，数据库采用 MySQL 数据库与 Redis 数据库，操作系统为 Windows10，PC 机硬件为 AMD Ryzen5 5600U 处理器，16 GB RAM。后台在阿里云服务器进行部署，服务器系统为 CentOS。系统架构采用客户端/服务端(C/S)架构，具体的双端实现如下。

在系统的服务端的实现上，本研究基于 JPBC 密码库使用 Java 实现了加解密模块，包括 AES 密钥的生成，AES 加解密功能的实现，CP-ABE 中访问策略的构造，CP-ABE 加解密功能的实现，其中 AES 密钥固定为 128 位，大小为 16 B。在数据库方面，本研究通过 MyBatis 框架实现对 MySQL 数据库中数据的维护管理，通过 Redis 数据来实现用户登录凭证的有过期机制的存储。浮标数据在系统开发中均以 Json 形式传输与显示。

在系统的客户端的实现上，本研究基于 Vue.js 框架设计了系统的操作与管理页面，通过 TCP 协议与服务端建立连接，并进行数据的传输。

### 4.2 系统测试

本系统采用 AES 对称密钥加密浮标数据，采用 CP-ABE 加密 AES 密钥，浮标数据与密钥均以密文的形式传递，保障了数据的机密性与安全性，但在系统工作的过程中，对数据的处理操作将增加系统的性能开销。本研究从加密效率、安全性等方面对多种加解密方案进行了对比，并对属性个数不同的情况下，CP-ABE 加解密所需要的时间进行了测试对比。

(1)不同加解密方案的对比

基于海洋浮标数据管理[30-31]的实际需求，本系统在选择加密算法时对比了多种加密算法，其中有中国国家密码局发布的对称加密 SM4 算法，开源的对称加密 AES 算法和基于密文策略的属性基加密 CP-ABE，表 2 是多种加密算法在加密效率、密钥安全、数据共享等方面的对比结果。从表中可以看出，在加解密效率方面，AES 算法相比于 SM4 算法稍有优势，同时 CP-ABE 相比于 SM4 和 AES 算法在密钥管理安全与数据的细粒度共享方面有着显著的优势，但是 CP-ABE 的加解密效率相比于 SM4 和 AES 较低，因此本研究采用了先对海洋浮标数据使用 AES 加密再对 AES 密钥使用 CP-ABE 加密的方案，由于 AES 密钥长度较短，大小在本系统中固定为 16 B，使用 CP-ABE 对其加密会比较迅速，可以有效地解决 CP-ABE 加解密效率略低的问题，同时对 AES 密钥加密也解决了对称加密中存在的密钥泄漏问题，因此，本研究采用的加密方案在加密效率、密钥安全、细粒度数据共享等方面均具有一定的优越性。

**表 2 多种加密算法的对比**

Tab. 2 Comparison of different encryption algorithms

| 加密算法 | 类别 | 加解密效率 | 是否存在密钥泄漏问题 | 是否支持细粒度的访问控制 |
|---|---|---|---|---|
| CP-ABE | 属性基加密 | 较低 | 不存在 | 支持 |
| SM4 | 对称加密 | 中 | 存在 | 不支持 |
| AES | 对称加密 | 较高 | 存在 | 不支持 |

(2)不同属性个数 CP-ABE 加解密所需时间对比

固定浮标数据大小为 500 KB，通过改变属性

的个数,计算 CP-ABE 加解密所需的时间。图 6 表示 CP-ABE 在不同属性个数下加解密所需时间的变化,由图 6 可以看出,随着属性个数的增加,CP-ABE 加解密所需的时间也呈线性增长的趋势。因此,CP-ABE 中访问策略设置的越复杂,属性设置越多,细粒度访问控制的程度越高,则消耗的计算资源也会越多。

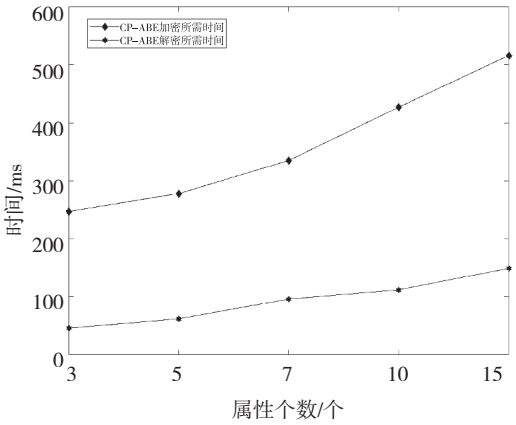


**图 6　在不同属性个数下 CP-ABE 加解密所需时间变化**

Fig. 6　The time spent for CP-ABE with different attributes

### 4.3　与其他方案的对比分析

本节中,将任鹏[14]与朱明垒[15]提出的传统海洋浮标数据管理系统,以及张新文等[16]提出的基于混合加密的浮标数据管理系统与本文方案分别从数据的加密方式,是否支持内容加密密钥的安全保管,是否支持访问控制等 3 个方面进行对比分析。对比的结果如表 3 所示,任鹏等[14]与朱明垒[15]提出的传统海洋浮标数据管理系统,未考虑浮标数据的安全问题,仅实现了浮标数据的采集存储与查询等;张新文等[16]提出的基于混合加密的浮标数据管理系统,采用了对称加密与非对称加密混合的方式对浮标数据进行加密保护,其通过非对称加密解决了对称加密的密钥保管安全问题,但其数据的共享依赖于非对称加密的公钥与私钥,公钥与私钥一一对应,在多个用户访问数据的情况下,需要使用每位用户的公钥分别为对称密钥进行加密,增加计算资源的消耗,不利于数据的共享;本研究为解决以上的问题,实现浮标数据的安全管理,首先使用 AES 算法加密浮标数据,解决浮标数据的安全问题,其次为解决 AES 密钥的安全管理问题,使用 CP-ABE 对 AES 密钥进行加密,在 CP-ABE 加密的过程中将访问策略嵌入了 AES 密钥的密文中,用户在请求数据的时候只需提交其属性集,系统为其生成私钥,并进行 CP-ABE 解密,如果用户属性符合访问策略,则解密成功。在多用户访问数据的情况下,此方案中只需要对 AES 密钥加密一次,便可实现细化到用户属性的访问控制,大大减少了计算资源的消耗,有利于数据的共享。综上所述,本研究方案在浮标数据安全,密钥安全,数据共享等领域具有显著优势。

**表 3　多种海洋浮标数据关系系统的对比分析**

Tab. 3　Comparison of different ocean buoy data management schemes

| 方案 | 时间 | 数据加密方式 | 是否支持内容加密密钥安全保管 | 是否支持细粒度的访问控制 |
|---|---|---|---|---|
| 文献[14] | 2012 年 | — | — | 不支持 |
| 文献[15] | 2018 年 | — | — | 不支持 |
| 文献[16] | 2020 年 | 对称加密与非对称加密 | 部分支持 | 不支持 |
| 本研究方案 | 2021 年 | 对称加密与属性基加密 | 支持 | 支持 |

## 5　结论

本研究将对称加密与属性基加密结合,构建了海洋浮标数据的安全管理系统。系统的测试结果表明,系统运行稳定,能够以较低的时间开销实现数据的安全存储以及细粒度访问控制,对浮标数据被攻击窃取问题的解决有着突出优势。本研究是加密技术的延伸,属性基加密的引入使得浮标数据的管理更具有灵活性,有助于传统的数据请求流程的优化,省去烦琐的权限申请,对于提高海洋浮标数据管理的安全性与灵活性的理论研究与实用价值明显,但在数据的加解密效率方面仍然存在一定的不足,下一步的研究中,会在对称加密的加解密效率与系统内通信的网络性能等方面进一步研究优化。　□

### 参考文献

[1] 王春晓,王旭,刘长华,等. 一种用于海洋综合观测浮标的多种通信方式集成系统[J]. 海洋科学,2020,44(1):142-147.

[2] 张胜茂,戴 阳,杨胜龙,等. 北斗海洋浮标数据接收与控制终端软件[J]. 渔业现代化,2021,48(1):80-86.

[3] 马凤强,吕婷婷,张浩. 应用于智能浮标的北斗铱星双模通信系统设计[J]. 传感器与微系统,2021,40(5):107-110.
[4] 饶浩. 应用于海上浮标的卫星通信终端关键技术研究[D]. 北京:中国科学院大学,2020.
[5] 王世明,李晴. 基于北斗卫星导航系统的海洋监测浮标通信系统设计与应用[J]. 全球定位系统,2016,41(4):102-105.
[6] 张春琳,莫旭冬,曹兵,等. 试论海洋观测数据传输网通讯方式的选择[J]. 气象水文海洋仪器,2015,32(4):92-95.
[7] 陈锦辉,王学昉,田思泉,等. 长江口及邻近水域渔业资源监测现状分析[J]. 长江流域资源与环境,2021,30(1):122-136.
[8] 张魁,廖宝超,许友伟,等. 基于渔业统计数据的南海区渔业资源可捕量评估[J]. 海洋学报,2017,39(8):25-33.
[9] 徐皓,陈家勇,方辉,等. 中国海洋渔业转型与深蓝渔业战略性新兴产业[J]. 渔业现代化,2020,47(3):1-9.
[10] 宗艳梅,魏珂,李国栋,等. 海洋渔业声学装备关键技术研究进展[J]. 渔业现代化,2021,48(3):28-35.
[11] 张慧杰,危起伟,杨德国. 回声探测仪的发展趋势及渔业应用[J]. 水利渔业,2008(1):9-13.
[12] 王小宁. 我国远洋海业企业海外发展研究[D]. 青岛:中国海洋大学,2012.
[13] 岳冬冬,王鲁民,方辉,等. 我国近海捕捞渔业发展现状、问题与对策研究[J]. 渔业信息与战略,2015,30(4):239-245.
[14] 任鹏,王廷伟,Christos Grecos. 基于 Shiny 框架的海洋浮标大数据处理实验平台[J]. 实验室研究与探索,2018,37(8):46-49.
[15] 朱明垒. 小型海洋资料浮标数据采集系统的设计[D]. 青岛:中国海洋大学,2012.
[16] 张新文,刘愉强,刘同木,等. 基于混合加密的浮标数据安全管理系统研究[J]. 热带海洋学报,2020,39(5):117-123.
[17] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]. ICTAC 2005: International Conference on Theory and Applications of Cryptographic Techniques. Denmark, Springer Verlag,2005:457-473.
[18] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]. Proceedings of IEEE Symposium on Security and Privacy. Berkeley, USA, IEEE, 2007:321-334.
[19] LI Y F, GUO Q Y, HUANG M J, et al. Study of an Electromagnetic Ocean Wave Energy Harvester Driven by an Efficient Swing Body Toward the Self-Powered Ocean Buoy Application[J]. IEEE Access, 2019(7):129758-129769.
[20] 解静,常江,孙家文,等. 海洋水文观测实时共享技术与应用研究[J]. 海洋环境科学,2020,39(2):302-308.
[21] 王世明,田园,田卡. 北斗卫星导航系统在波浪能自供电海洋浮标中的应用[J]. 全球定位系统,2018,43(4):126-130.
[22] 吴明东,盛松伟,张亚群,等. 海洋波浪能浮标发展现状及前景[J]. 新能源进展,2021,9(1):42-47.
[23] 滕骏华,吴彬锋,田杰,等. 海洋渔业志愿船观测数据可用性评估[J]. 海洋预报,2020,37(4):21-29.
[24] XI F B, PANG Y K, LIU G X, et al. Self-powered intelligent buoy system by water wave energy for sustainable and autonomous wireless sensing and data transmission[J]. Nano Energy, 2019(61):1-9.
[25] 贾相忠. 基于多层分布式架构的现场营销支持系统研究和实现[D]. 长沙:湖南大学,2014.
[26] 陈家豪,殷新春. 基于云雾计算的可追踪可撤销密文策略属性基加密方案[J]. 计算机应用,2021,41(6):1611-1620.
[27] 冯登国,张敏,李昊. 大数据安全与隐私保护[J]. 计算机学报,2014,37(1):246-258.
[28] 陈兴蜀,杨露,罗永刚. 大数据安全保护技术[J]. 工程科学与技术,2017,49(5):1-12.
[29] 李昊,张敏,冯登国,等. 大数据访问控制研究[J]. 计算机学报,2017,40(1):72-91.
[30] 李晴. 多参数海洋浮标监测系统研究[D]. 上海:上海海洋大学,2017.
[31] 党超群,张锁平,齐占辉,等. 基于北斗卫星系统的深远海 GPS 波浪浮标数据传输研究[J]. 传感器与微系统,2016,35(1):46-48.

# Design and realization of an ocean buoy data security management system based on attribute-based encryption

GU Zhenkai[1,2], ZHANG Shaohua[2], LI Chao[2], DAI Binrong[2]

(1 *College of Information Technology, Shanghai Ocean University, Shanghai* 201306, *China*;
2 *Shanghai Computer Software Technology Development Center, Shanghai* 201112, *China*)

**Abstract**: Targeting the problem of ocean buoys data being attacked and stolen by hackers, and based on analyzing the operating mechanism of Beidou ocean buoy system, an attribute-based encryption ocean buoy data security management system was designed and proposed in this paper. In order to achieve fine-grained access control of ocean buoy data, this system contained three subsystems including data encryption and decryption, data management and key management, meanwhile, the process of data storage and data request were designed to manage the transfer of buoy data between data requester and data owner. Furthermore, the system was implemented based on the open source JPBC cryptographic library and popular front-end and back-end technologies, and compared with multiple encryption schemes. The results showed that the encryption scheme used in this paper had significant advantages in encryption efficiency and fine-grained buoy data sharing. Compared with the traditional buoy data management system, this system combined symmetric encryption and attribute-based encryption technologies to realize the security protection of buoy data and the fine-grained sharing of data. The research results provided references for buoy data security management, and promoting fishery informatization and modernization development.

**Key words**: ocean buoy; ocean fishing; Beidou satellite; data management; attribute-based encryption; information security